

UNITED STATES ARMY SPECIAL OPERATIONS COMMAND



AY21-22 Priority Research Topics



**UNITED STATES ARMY
SPECIAL OPERATIONS COMMAND**

AY21-22 Priority Research Topics

12 JAN 21



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY
SPECIAL OPERATIONS COMMAND
2929 DESERT STORM DRIVE
FORT BRAGG, NORTH CAROLINA 28310-9110

AOSO

12 January 2021

MEMORANDUM FOR Record

SUBJECT: USASOC AY21-22 Priority Research Topics

1. This memorandum serves to approve the USASOC AY21-22 Priority Research Topics List. These topics inform future force development related analysis such as USASOC led Capabilities-Based Assessments, graduate student thesis topic selection, RAND studies, etc.
2. Topics reflect ARSOF high priority issues, in particular those best suited for academic discovery and are developed via an assessment of strategic guidance, the contemporary and future operating environment, current and projected knowledge shortfalls, and current or projected capability shortfalls.
3. The (16) enclosed priorities are aligned to (4) categories (Information Warfare, Multi-Domain Operations, Technology, and Title 10 Functions) and each includes a broad description of the problem set or hypothesis as well as a list of potential research questions.
4. The USASOC Priority Research Topics are published biennially by the USASOC DCS G9 and are posted on the USAJFKSWCS Graduate Research Management Office portal located at: [USASOC AY21-21 Priority Research Topics List](#).
5. Point of Contact this action is Mr. Larry Deel, USASOC DCS G9 at COMM 910-396-0476, or email larry.deel@socom.mil.

LOCK.JOSEPH.GUY
.1045577178

Digitally signed by
LOCK.JOSEPH.GUY.1045577178
Date: 2021.01.12 16:42:56 -05'00'

Encl
AY21-22 Priority Research Topics

JOSEPH G. LOCK
Colonel, SF
Chief, USASOC Force Modernization Center

Table of Contents

<u>Forward</u>	1
<u>Summary</u>	2
<u>Information Warfare</u>	4
Influence Operations	4
Electronic Warfare	5
SOF-Space-CEMA Nexus	5
Adversary Information Warfare	6
Civil Resistance in the Future Information Environment	7
21st Century Maneuver Space	7
Optimizing for Information Warfare	8
<u>Multi-Domain Operations</u>	9
Great-Power Competition	9
Maneuver in the Deep Fire Areas in support of MDO	10
Strategic Blind Spots in Large Scale Combat Operations.....	10
Sensitive Activities	11
<u>Technology</u>	11
Optimizing the ARSOF Soldier for the Future Operating Environment	11
Artificial Intelligence/ Machine Learning	11
Robotics and Autonomous Systems	12
<u>Title 10 Functions</u>	12
Dynamic Force Management.....	12
Dynamic Talent Management.....	13
ARSOF Accessions	13
<u>Appendix</u> : Acronym List.....	15

Forward

The following research topics reflect Commanding General, US Army Special Operations Command (USASOC) priority issues, in particular those best suited for academic study. These topics support the FY21 USASOC Campaign of Learning and were developed via an assessment of strategic guidance, the contemporary and future operating environment (FOE), current and projected knowledge shortfalls, current and projected capability shortfalls, and input from USASOC Headquarters (HQ) staff and Component Subordinate Commands/ Units (CSC/Us).

The research topics are updated biennially and inform USASOC internal analyses as well as nominations for RAND Studies, the US Army War College Key Strategic Issues List (KSIL), Joint Professional Military Education (JPME) Topics, Joint Special Operations University (JSOU) Special Operations Research Topics list, Army Special Operations Forces (ARSOF) graduate student thesis topic selection, and other academic research.

Results of the research are spiraled into the USASOC Strategic Planning Process as appropriate to inform strategic resourcing and/or future force development decisions, or sometimes simply add to the enterprise-wide body of knowledge in support of the Campaign of Learning.

Comments about this publication are invited and should be forwarded to the study coordinators listed below.

This publication can be found online at: [USASOC AY21-21 Priority Research Topics List](#)

For additional information on any of the topics, please contact the USASOC DCS G9 study coordinators, Mr. John (Brooke) Tannehill at 910-432-2328/john.tannehill1@socom.mil or Mr. Damon Cussen at 910-396-0493/damon.cussen@socom.mil.

Summary

Information Warfare

- Influence Operations. ARSOF support to Influence Operations in Great-Power Competition (GPC).
- Electronic Warfare (EW). ARSOF's ability to conduct full spectrum characterization of the Electromagnetic Environment (EME) to geo-locate and disrupt adversary systems across the conflict continuum.
- Special Operations Forces (SOF)-Space-Cyber Electromagnetic Activity (CEMA) Nexus. Leveraging the global synergy of ARSOF's persistent forward presence, Space based capabilities, and CEMA to see, sense, and strike deep against peer adversaries across the conflict continuum.
- Adversary Information Warfare. How peer adversary's' holistic exploitation of the Information Environment (IE) to manipulate, coerce, and control populations could provide a "best practices" template for US consideration.
- Civil Resistance in the future IE. How globally dispersed individuals, groups, and ideas can challenge the narrative (and sovereignty) of the State in an increasingly interconnected and globally scaled IE.
- 21st Century Maneuver Space. Irregular ("Proxy") Warfare and Information Warfare as the only (feasible) maneuver space against modern, technology enabled, hyper-lethal, nuclear armed peer adversaries.
- Optimizing for Information Warfare. Rethinking organizational structure and associated 'Information' framework (taxonomy and lexicon) to optimize for operations in the IE.

Multi-Domain Operations (MDO)

- GPC. Operationalizing ARSOF's role in GPC to impose costs, improve the US strategic position, and/or set conditions for transition to conflict.
- Maneuver in the Deep Fires Area in support of MDO. ARSOF's ability to maneuver in the operational and strategic deep fires areas to enable the Joint Force (JF) to prevail in MDO across the conflict continuum.
- Strategic Blind spots in Large Scale Combat Operations (LSCO). Critical examination of (AR)SOF's strategic thinking, and associated assumptions in high end conflict with a peer adversary.
- Sensitive Activities. (For additional details, contact the G9 study coordinator).

Technology

- Optimizing the ARSOF Soldier for the FOE. Enhancements in competency, cognition, performance, and total health to successfully navigate the changing human and technology landscapes.

- Artificial Intelligence (AI)/ Machine Learning (ML). Harnessing AI/ML to maintain a competitive edge in data-intensive tasks such sentiment analysis, disinformation analysis, etc., while reducing cognitive load on the Soldier.
- Robotics and Autonomous Systems (RAS). Harnessing future manned and unmanned robotic systems in the Future Operating Environment (FOE).

Title 10 Functions

- Dynamic Force Management. Modifying (AR)SOF's strategic resourcing, acquisition, sustainment, and divestiture processes to more rapidly respond to anticipated and emergent operational needs.
- Dynamic Talent Management. Enterprise-wide total career lifecycle management based on individual knowledge, skills, behaviors, and preferences.
- ARSOF Accessions. Addressing systemic SF, CA, and PSYOP accessions challenges given dwindling Initial Entry and In-Service recruiting pools.

Information Warfare

1. **Influence Operations.** The 2018 National Defense Strategy (NDS) states that Russia, China, and their proxies have largely chosen to compete with the US “below the threshold likely to provoke a US conventional response”. This, coupled with the increasingly constrained maneuver space of the early to mid-21st Century security environment (as described in the Joint Operating Environment 2035), highlights the role of information, in particular “Influence”, as a primary line of effort to shape the global security environment. The power of the narrative to impact the perceptions, decision making, and/or behavior of adversary, neutral, or foreign target audiences is paramount to achieving an enduring or temporary position of advantage relative to the enemy and population.

- In this environment, given a less than optimal Joint and interagency (Command and Control (C2)) framework for influence Operations, Activities, and Actions (OAAs) Outside of a Declared Theater of Active Armed Conflict (ODTAAC), how does (AR)SOF support whole of government “statecraft” against great power competitors Russia and China?

- How has the (20 year) focus on counter violent extremist organizations, and most recently LSCO, put the US out of position to compete with Russia and China on a global scale?

- How does the internet and social media, as well as the (virtual) assimilation of groups and individuals on a global scale, create entirely new and powerful opportunities for industrial scale influence?

- CONUS Based Operational Support (CBOS) must be considered given the ubiquitous nature of information and means of rapid global dissemination. How should this be integrated into Geographic Combatant Command (GCC) and Theater Special Operations Command (TSOC) Campaign Plans?

- How important is an active, offensive strategy and accompanying narrative relative to a defensive and/or reactive approach that pushes a counter-narrative as a means to achieve US goals and objectives?

- How does PSYOP composition and (global) disposition, in particular Active Component Compo 1, support Influence on the modern battlefield?

- Can (AR)SOF garner any best practices from large commercial enterprises and their associated advertising campaigns? What about Russian and Chinese use of information to coerce, influence, and control? Are there historical examples, US led or otherwise, that could inform contemporary Campaigns?

- How can ARSOF achieve scale against GPC? Is a fundamental change required in the Special Warfare Center and School training pipeline for PSYOP Soldiers? Should greater focus be placed on bilateral influence operations, actions, and activities, i.e. via

partners and surrogates, rather than US unilateral? What must fundamentally change regarding PSYOP doctrine to achieve any recommended changes?

- Can Active Component (AC) and Reserve Component (RC) PSYOP forces potentially achieve greater synergy in competition as well as large scale combat operations through habitual training, improved resourcing, joint deployments (in competition), RC restructuring (to mirror their AC counterparts), and/or changes to RC accessions models?

- What training models should be incorporated in the PSYOP Qualification Course to account for the use of digital modeling, publicly available information, commercially available information, polling, psychometrics, and A/B testing to account for data proliferation and audience segmentation in today's increasing digital environment?

2. **Electronic Warfare.** In an increasingly interconnected and technology saturated IE, the Electromagnetic Spectrum (EMS) is an increasingly relevant aspect of modern warfare. (AR)SOF, and the JF, must have unimpeded access to and use of this Electro-Magnetic Environment (EME), while denying adversary use of the same. This creates opportunities for EW in support of MDO (e.g. electronic exploit, attack), while also highlighting US vulnerabilities and the corresponding need to manage and protect network, devices, and information. In 2015, Russia's use of brigade-level Electronic Warfare (EW) assets in Ukraine, particularly with barrage (noise) jamming of tactical radio nets, cell phone emitters, and satellite downlink targets highlights the relevance of the EMS on the modern battlefield.

- What is ARSOF's role in support of full spectrum characterization of the EME to geo-locate and disrupt adversary systems across the conflict continuum against peer competitors?

- How can (AR)SOF reduce its vulnerability to peer/near-peer adversary use of EW in both competition and conflict?

- What future technology advances (e.g. 5G) may be the next game changer in the EME?

3. **SOF-Space-CEMA Nexus.** In an increasingly complex, ambiguous, and technology-saturated mid-21st Century security environment, highlighting the relevance of transparency and reach, an opportunity presents at the nexus of SOF, Space, and Cyber. From space comes a full view of the planet and global access. From SOF, with its forward posture and agile forward positioning, comes knowledge of the people, cultures, and populations and the ability, if needed, to deliver precision fires. From Cyber comes an understanding of the global pulse through the World Wide Web, social media, etc., as well as the ability to deliver non-kinetic effects via computer networks operations, electronic warfare, information warfare, etc. This nexus allows for hyper-enabled situational awareness across all facets of the operating environment (physical, virtual, and human), to include precision (strategic) indicators and warnings, enabling the JF to operate ahead

of threat intentions across the conflict continuum. The nexus also allows the JF to see, sense, and when necessary, strike deep - with physical, information, and/or virtual power, dictating the terms of the adversary's next move to prevail in the contact layer, and attain overmatch in the blunt and surge layers through increased operational time, speed, precision, range, and lethality.

- How would this fusion of SOF, Space, and CEMA, particularly when enabled by AI, enable the US and Partners to challenge adversaries in new and unique ways? Could this nexus better enable the JF to maneuver (or create effects) in the operational and strategic deep fires areas?

- The National Security Strategy (NSS) of 2017 states that "Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders." How does a SOF, Space, CEMA nexus support a whole of government approach to mitigate this challenge? Does this nexus better posture the JF to proactively campaign (and win), in competition?

- What organic capabilities does ARSOF need and what capabilities are sufficient on demand from USCYBERCOM, US Army Space and Missile Defense Command, the JF, and/or the Interagency, etc.?

- How does ARSOF support Space operations? Correspondingly, how does JF space operations and the emerging Space Force provide support to Special Operations?

4. **Adversary Information Warfare.** China's Three Warfares (public opinion warfare, psychological warfare, and legal warfare), along with Russia's Gerasimov Doctrine, which leverages the state, military, and information power to achieve national objectives, highlight the changing character of modern warfare. These holistic influence campaigns below the threshold of armed conflict target entire populations (governments, societies, and militaries) to achieve desired political outcomes.

- How does Russia's and China's approach to modern political warfare, in particular exploitation of the IE to manipulate, coerce, and control, potentially provide a "best practices" template for US consideration?

- "Mission Command" of these national influence campaigns is difficult to operationalize. How do adversaries "decide, manage, coordinate" operations or take advantage of emergent opportunities?

- What tools and methods are used to coerce and control populations? How can populations be inoculated against these tactics? What impact do these tools and methods have on US influence operations?

- What legal, moral, or ethical considerations constrain, or limit, US adoption?

5. Civil Resistance in the Future Information Environment. In an increasingly complex, interconnected, and globally-scaled IE, dispersed individuals, groups, and ideas can challenge the narrative and hence sovereignty of the state through virtual means, with little to no physical presence or footprint. Social media, sensationalized (or fake) news, and other forms of propaganda (at scale) can impact perceptions, beliefs, attitudes, behaviors, opinions, and correspondingly the decisions of the public as well as government and private officials. Dr. Yaneer Bar Yam, Professor and President of the New England Complex Systems Institute stated several years ago that “one of the biggest challenges we face (to the status quo) is the disaggregation of individuals, groups, communities, etc. into a global collective where people assimilate around a common idea or interest irrespective of their physical location, thereby weakening the tie between the citizen and the state, and correspondingly eroding national identity”. This could impact (AR)SOF core activities in a number of ways, in particular Foreign Internal Defense (FID), Counterinsurgency (COIN), and Unconventional Warfare (UW).

- How would these activities be conducted via virtual means, either in whole or in part? Presumably, the knowledge, skills, and abilities of the ARSOF soldier would need to change to account for the “language and culture” of the virtual world, not to mention the general scheme of maneuver or mission profile where the skills imparted on the partner or proxy to protect their National interest (FID/COIN) or enable a “war of movement” (UW) would be cyber centric, and the training/ advising/ assisting of those skills could be done physically or virtually, or a hybrid therewithin.

- In a general sense, how will this future IE affect ARSOF's ability to develop understanding and wield influence, leverage the indigenous approach, respond to crisis, and/or conduct precision targeting?

- What are some historical examples (e.g. Iran) where a more optimized presence in the virtual space years prior would have led to a tipping point?

- What can SOF learn about the methods or science behind movements’ communications abilities, such as relationship-building, grassroots organizing, strategy, and planning?

6. 21st Century Maneuver Space. In an era characterized by exponential advances in technology and an accelerating rate of change, adversary militaries are modernizing at an alarming rate. Unencumbered by rigid bureaucracies, Russia, China, and others are fielding capabilities that can markedly increase force speed, reach, battlespace surveillance, lethality, etc. Additionally, peer adversaries’ layered standoff continues to limit US force projection options. As this trend continues, many will likely achieve parity with, or surpass that of the US. On the modern battlefield, given near ubiquitous surveillance, it is nearly impossible to hide, and if forces can be seen (across all domains) certainly they can be targeted and eliminated. This hyper-enabled, hyper-lethal adversary likely also possesses nuclear weapons, which suggests that any form of high end, large scale combat would be a very high risk endeavor.

- Is the US, and the rest of the world, moving toward a global stalemate, where conventional forces and capabilities become another means of mutually assured destruction, and therefore function as a deterrent only?
- Does Irregular (“Proxy”) Warfare and Information Warfare become the only (feasible) maneuver space against modern, technology enabled, hyper-lethal, nuclear armed peer adversaries?
- SOF is essentially purpose built for Information Warfare and Irregular Warfare. Should USSOCOM by its very nature not be the service of choice for GPC?
- Is the US not (per se) at war with Russia via proxy in Syria? Is this not a contemporary example of future trends?

7. Optimizing for Information Warfare. The Army and JF are optimized for LSCO. (AR)SOF is certainly a force multiplier in high-end conflict, but not surprisingly, is purpose built for Irregular Warfare, and by extension Information Warfare. The recent NSS 2+3 pivot then correspondingly highlights the relevance of (AR)SOF for the contemporary global security environment which favors a non-kinetic, non-lethal approach to compete with our Nation’s adversaries below the threshold of armed intervention. Conversely, this strategic refocus highlights the JF imbalance with respect to high end competition. The Army and JF are chartered to win the Nation’s wars, and therefore not optimally postured for enduring competition with Russia and China. Certainly, modernizing for LSCO after nearly 2 decades of large scale COIN is a strategic imperative to deter peer adversary aggression, but GPC is not a SOF only responsibility, nor can SOF effectively go it alone. This is evident in the recent NDS Irregular Warfare Annex which directed all the services to build an enduring irregular warfare capability, and by extension Information Warfare capability. As peer adversaries skillfully operate in the seam between peace and war to achieve political objectives, the US and JF are playing catch up, challenged in their ability to think about, and effectively plan and organize for campaigns below the threshold of conflict to deter Chinese expansionism in the South China Sea and Russian aggression in Eastern Europe.

This lack of proficiency in Information Warfare across the Army and Joint community is evidenced, as one example, in the use of something as simple as the term “information”, which takes on a different meaning depending on the context of the discussion, sometimes denoting a ‘form of warfare’, other times a ‘domain of warfare’, or an ‘aspect of the environment’, and even a warfighting function, etc. This is unnecessarily confusing. The (TRADOC) CAC Commander recently asked CG USASOC to assist the Army in devising a framework for how to “professionally think about ‘information.’”

- What is “Information” in context with current operating and functional paradigms? What is a logical taxonomy and lexicon for all information-related capabilities that facilitates accurate and consistent communication and understanding, and ultimately operational effectiveness?

- As a “think piece”, how would the JF organize for, plan, and execute enduring campaigns in the competition space given a favorable political environment and unconstrained resources, and no other major responsibilities or functions? How would the DoD/JF optimize for GPC (irregular warfare and information warfare) in terms of force structure, disposition, and C2? Is this paradigm mutually exclusive with maintaining readiness for LSCO?
- Ambassadors and their staffs control permissions ODTAAC, while US forces frequently rotate in and out of country, or engage only episodically. Is there a more effective approach?

Multi-Domain Operations

1. **Great-Power Competition.** ARSOF campaign in the Contact Layer to buy down risk by setting deterrence conditions early to impose costs, improve the US strategic position, and/or set conditions to transition to conflict if deterrence fails. That said, given the fairly recent transition to GPC, the US is out of position and ill-equipped to deal with modern security challenges posed by Russia and China (ODTAAC), where in most cases the nature of the problem does not easily lend itself to a military only or military-centric solution. In this space, the US must proactively employ all tools across the diplomatic, informational, military, and economic realm to both understand and place at risk those things adversaries value.

- In this environment, given the lack of a comprehensive US strategy and corresponding information assurance mechanism or approach to whole of government “statecraft”, how does (AR)SOF effectively leverage authorities such as 1202 to impact the Russian cost calculus in Eastern Europe or Chinese incursions in the Indo-PACOM area of responsibility?
 - How can ARSOF optimize CBOS to GPC?
 - What are some examples of (AR)SOF support to campaigning and winning in the contact layer, noting that a “win” might be characterized as improving the US strategic position, developing greater understanding and expanding influence, increasing governance, or simply retaining the initiative for follow-on action?
 - How might GCCs better posture to deal with what are increasingly global vice regional threats?
 - How might Component Commands, which are currently Title 10-focused (organize, man, train, equip), vice warfighting HQs, better support the TSOC?
 - Fully integrated, cross-functional, interagency teams are imperative to address challenges in the contact layer. Could a global Memorandum of Agreement better facilitate co-deployment (and employment) of US government agencies?

- How might ARSOF garner a clearer understanding of adversary actions and underlying logic to maneuver them into unfavorable positions in order to set the conditions that dictate the terms of the next move?

2. Maneuver in the Deep Fire Areas in support of MDO. The Army and JF must be capable of conducting operational-level, multi-domain, physical, cognitive, and virtual maneuver across the conflict continuum to gain an advantage over the Nation's adversaries. ARSOF's persistent forward presence (under the anti-access/ area-denial umbrella) enables deep understanding and influence across all facets of the operating environment. This positions ARSOF, in support of the JF and MDO, to penetrate peer adversary systems in the Blunt Layer if deterrence mechanisms fail, and in the Surge Layer, target key adversary systems and mobilize populations to generate indigenous mass, countering adversary influence or opening windows of opportunity for JF Commanders. In particular, in accordance with the Army's MDO Concept, "the operational and strategic deep fires areas are beyond the feasible range of movement for conventional forces, but where the JF can employ joint fires, SOF, information, and virtual capabilities".

- How does ARSOF leverage unilateral, partner, proxy, and/or indigenous resistance capabilities to see, sense, and when necessary strike deep across multiple domains (land, maritime, air, space, cyber, and human) to delay/ disrupt enemy preparations, and support the convergence of joint multi-domain capabilities at the precise location and time in the targeting/ interdiction of high-value systems?
- How does ARSOF leverage physical, virtual, and/or cognitive capabilities across multiple domains to achieve the same?
- In the operational and strategic deep fires areas, in close proximity to a full spectrum of adversary capabilities across multiple domains, how does ARSOF reduce risk to mission and force?

3. Strategic Blind Spots in LSCO. As the Nation shifts focus to align with the priorities of the NSS (and corresponding NDS and National Military Strategy), critical examination of the JF and (AR)SOF's strategic thinking and associated assumptions about high end conflict with peer adversaries is warranted. Any blind spot in the military's approach to Chinese and/or Russian challenges across the conflict continuum could result in serious, or possibly catastrophic consequences. This is particularly so, given an era where quickly advancing technologies enable adversaries to rapidly develop and field robust capabilities, such as ubiquitous sensing, hyper-lethal weapons systems, etc. More to the point, there also exists an opportunity, for those less scrupulous, to potentially field leap-ahead capabilities that could change the nature of the game altogether. These blind spots may result from a lack of knowledge, lack of situational awareness, lack of experience, incomplete information or intelligence, faulty assumptions, poor planning, or in some cases simply flawed strategy.

- Could there be a strategic blind spot in ARSOF's mental frame of the environment, the military challenges it faces, and the corresponding approach(es) to mitigate these challenges?
- What method of (blind spot) analysis could be utilized to uncover obsolete, incomplete, or incorrect facts and/or assumptions?
- Are there historic examples, or lessons learned from recent operations that could provide valuable insights?

4. **Sensitive Activities.** The ability of SOF to conduct clandestine operations is increasingly challenged by peer and near-peer adversaries (e.g., persistent surveillance, big data analytics, data aggregation, and biometrics). These operations require non-standard functions which are critical to success. How can SOF improve its efficiency in operations and the associated enabling functions in order to provide JF Commanders increased optionality across the conflict continuum? (Discussion and research on this topic would need to be classified (up to the S//NF level)). Please contact the USASOC DCS G9 study coordinator for more information.

Technology

1. **Optimizing the ARSOF Soldier for the FOE.** ARSOF requires new operating concepts and associated capabilities to confront a broad range of anticipated future security challenges. In an increasingly complex and globally-scaled operating environment characterized by exponential advances in technology, an accelerating rate of change, hyper-enabled adversaries, etc., the Soldier, the cornerstone of ARSOF's contribution to the Nation, must correspondingly optimize to confront these challenges.

- What enhancements in competency, cognition, performance, and total health increase the ability of the future ARSOF Soldier to successfully navigate changing human terrain and new technology landscapes?
- How will the ARSOF Soldier seamlessly navigate the digital/ technology space while remaining fully proficient in "analog" operations?
- How should regional alignment, language expertise, and cross-cultural agility evolve?
- What legal or ethical challenges are associated with biological, mechanical, or digital enhancements?

2. **Artificial Intelligence/ Machine Learning.** AI will ultimately permeate every aspect of daily life in the not-too-distant future, having a similar impact to that of electricity at the turn of the 20th Century. AI will also quite probably lead to a revolution in military affairs, fueling the rise of robotic and autonomous systems as an example. As well, AI could optimize intelligence/battlespace awareness via seamless control of multiple, spatially-dispersed, networked sensor platforms, autonomously processing voluminous amounts of

full motion video, sensor data, personally available information, etc., improving decision-making at the point of need while lessening the cognitive load on the Soldier. AI will also certainly assist in the execution of complex tasks with much greater speed and accuracy.

- To what extent can ARSOF leverage AI as a force multiplier in the contemporary and FOE, as well as counter the adversary's use of the same?
- What AI/ML application best practices from non-DoD organizations could be incorporated into open source intelligence analysis and production activities as well as operationally-focused open source research?
- How can AI be used to mitigate cognitive overload (e.g., sensor feeds, video/photo/document analysis, data mining, or social media)?
- What is the appropriate level of autonomy for processes such as social science modeling, sentiment analysis, disinformation analysis, event forensics, trend analysis, etc.?

3. Robotics and Autonomous Systems. RAS offers the possibility of a wide range of platforms, to include weapon systems, that could potentially revolutionize the way (AR)SOF and the JF fight, from precision interdiction operations to mundane or dangerous tasks such as resupply, security, route clearance, etc., reducing risk while also increasing overall force efficacy and efficiency. Recent improvements in unmanned aerial and ground systems include increased mobility, miniaturization, software and processing speeds, autonomy, sensor/ weapons payloads, and networking abilities. Currently, the incorporation of RAS into military operations is implemented via Manned-Unmanned Team (MUM-T) which leverages the inherent and complementary strengths of the unmanned system and the Soldier. That said, AI is key to greater autonomy of the robotic system, where the (future) nexus of RAS and AI could even change the nature of warfare itself.

- What specific roles and associated concept of operations/ Tactics, Techniques, and Procedures could be envisaged for RAS capabilities?
- What is the appropriate level of autonomy for RAS? Should these systems ever be fully autonomous, or always include a human in the loop? What are the legal, moral, and/or ethical considerations?

Title 10 Functions

1. Dynamic Force Management. USASOC requires a more responsive and flexible approach to strategic resourcing, acquisition management, program sustainment, and divesture to more rapidly respond to anticipated and emergent operational needs. Competitors are responding, and will increasingly respond, with speed and lethality, enabled by disruptive technologies and unencumbered by rigid bureaucratic systems. Though relatively agile and responsive, USASOC exercises its Title 10 organize, man,

train, and equip responsibilities in a manner that will not be sufficiently nimble to address the rapidly evolving global security environment. For example, allocating resources to broad program categories (e.g. communications, weapons) vice a specific Line Item Number (LIN), could enable a flexible, timely, and effective Commercial-Off-the Shelf (COTS) based approach to acquisition by fielding the most recent and effective technologies and associated systems.

- Presumably, though more effective, this approach may in fact be more expensive, unless costly sustainment and lifecycle replacement tails could be replaced with a throw-away approach. Per capita, what is the associated cost for each of these approaches?

- How can SOF, the Army, and JF in general shed the existing “money in motion is money at risk” paradigm, enabling decentralized divestiture and reprogramming actions by subordinate Commanders?

2. Dynamic Talent Management. Optimized talent management matches individual knowledge, skills, behaviors, and preferences against the needs of an organization, from initial entry through senior leader/ management positions, and includes command, staff, functional, and special assignments. Though manned with the highest quality personnel, ARSOF lacks an effective enterprise-wide career lifecycle management program that deliberately, and strategically, aligns the right individual to the right position, at the right time, throughout his or her career. To develop and maximize human capital for the increasingly complex challenges of the future, SOF must jettison its longstanding “cookie cutter” approach to personnel management, in favor of a 21st century paradigm that considers advanced analytics, (predictive) modeling, trends analysis, etc.

- Could a functional cohort approach for each year group be an effective alternative, one that aligns individuals into command, staff, functional, or ‘special’ categories early in their career, with purpose built education, training, and assignments? What other alternatives could be considered, orthodox or otherwise, that better utilize (or build) requisite talent?

- Given anticipated recruiting and accessions challenges, how can (AR)SOF better manage retention, or extend the career lifecycle through “SOF-for-life” or other options? Could a conditions vice time-based approach to retirement provide an alternative?

- What is the cost of a deliberate, proactive, and dynamic talent management approach in manpower and dollars?

3. ARSOF Accessions. ARSOF faces systemic recruiting and accessions challenges that could lead to increasing manpower shortages across all its formations. Volunteers for Army Special Operations training, from both Initial Entry and In-Service recruiting pools, is dwindling. Contributing factors likely include a smaller Army, a prosperous economy, a general decline in physical fitness levels of young adults, and possibly even a change in the value system of the younger generation(s). Of those that do volunteer, increasing numbers are withdrawing from assessment. Exacerbating the problem, two decades of an

extremely high OPTEMPO, largely in combat, have led to retention issues. These bleak trends have persisted for some time and are not expected to change.

How can USASOC better identify and attract candidates that are both willing and qualified to apply?

Of those candidates that are eligible (on paper), how are current social norms, trends, and/or value systems impacting their desire to apply? What other variables are at play?

Of those (in-service) candidates that are eligible (on paper), how are Soldiers' units or other factors impacting their desire to apply? What other variables are at play?

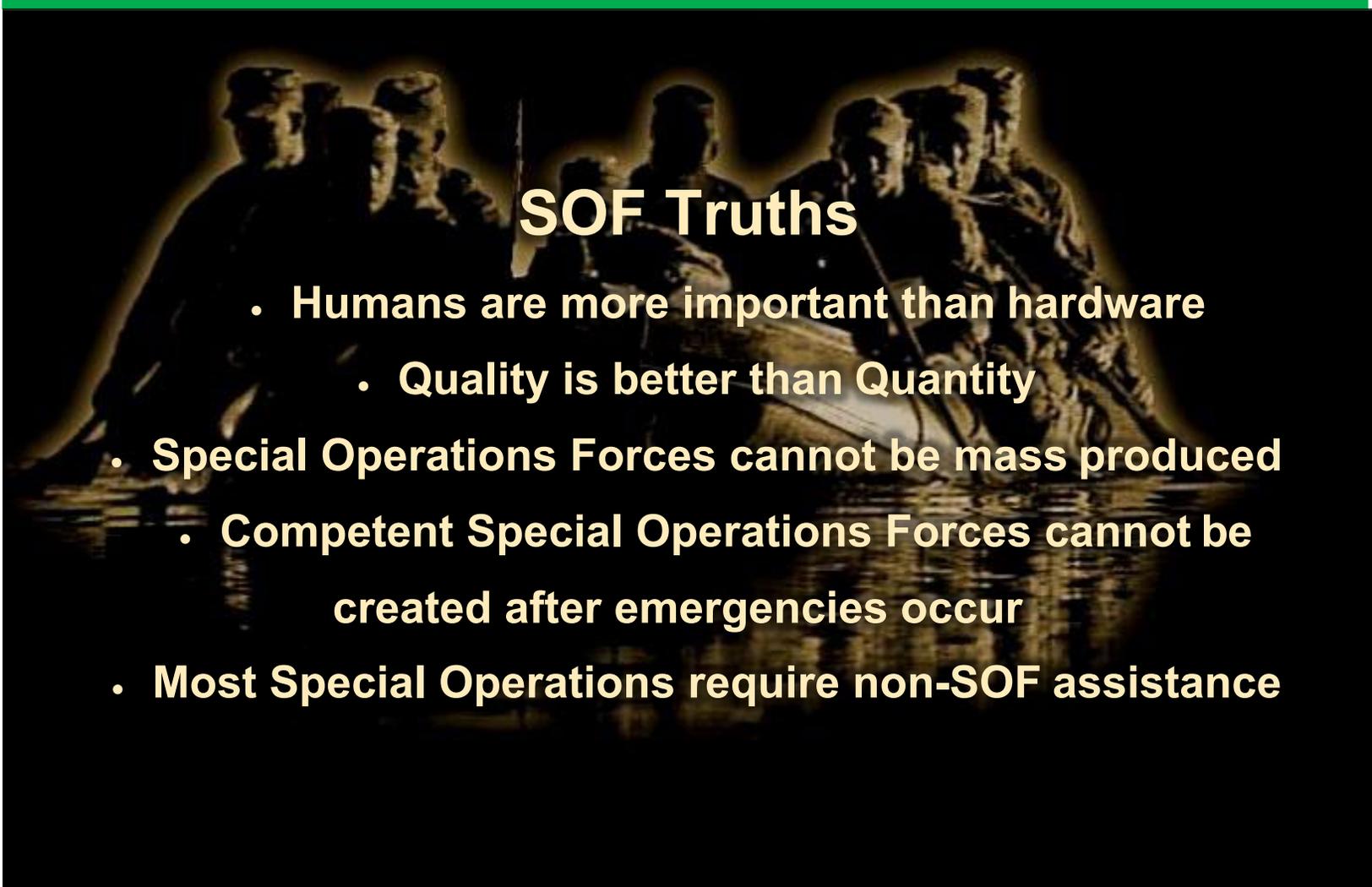
Appendix: Acronym List

AC	Active Component
AI	Artificial Intelligence
ARSOF	Army Special Operations Forces
C2	Command and Control
CBOS	CONUS Based Operational Support
CEMA	Cyber Electromagnetic Activity
COIN	Counterinsurgency
COTS	Commercial-Off-the Shelf
CSC/Us	Component Subordinate Commands/ Units
EME	Electromagnetic Environment
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
FID	Foreign Internal Defense
FOE	Future Operating Environment
GCC	Geographic Combatant Command
GPC	Great-Power Competition
HQ	Headquarters
IE	Information Environment
JF	Joint Force
JPME	Joint Professional Military Education
JSOU	Joint Special Operations University
KSIL	Key Strategic Issues List
LIN	Line Item Number
LSCO	Large Scale Combat Operations
MDO	Multi-Domain Operations
ML	Machine Learning
MUM-T	Manned-Unmanned Team
NDS	National Defense Strategy
NSS	National Security Strategy
OAA	Operations, Activities, and Actions
ODTAAC	Outside of a Declared Theater of Active Armed Conflict

RAS	Robotics and Autonomous Systems
RC	Reserve Component
SOF	Special Operations Forces
TSOC	Theater Special Operations Command
USASOC	US Army Special Operations Command
UW	Unconventional Warfare

The following research topics reflect Commanding General, US Army Special Operations Command (USASOC) priority issues, in particular those best suited for academic study. These topics support the FY21 USASOC Campaign of Learning and were developed via an assessment of strategic guidance, the contemporary and future operating environment, current and projected knowledge shortfalls, current and projected capability shortfalls, and input from USASOC HQ staff and Component Subordinate Commands/ Units (CSC/Us).

USASOC DCS G9
2929 Desert Storm Dr.
Fort Bragg, NC 28310



SOF Truths

- **Humans are more important than hardware**
 - **Quality is better than Quantity**
- **Special Operations Forces cannot be mass produced**
 - **Competent Special Operations Forces cannot be created after emergencies occur**
- **Most Special Operations require non-SOF assistance**