SOF Paradigm in Great Power Competition

Invited Perspective Series
Strategic Multilayer Assessment (SMA)
Future of Global Competition & Conflict Effort

OCTOBER 17

STRATEGIC MULTILAYER ASSESSMENT
Editor: Dr. Spencer Meredith III
National Defense University
Series Editor: Sarah Canna, NSI Inc.

Dr. John DeRosa, Special Operations Command - Europe

Dr. John DeRosa is a Strategist at Special Operations Command - Europe (SOCEUR). Prior to SOCEUR, Dr. DeRosa worked on the Joint Staff (J-8) and the Army Staff (HQDA, G-35). He is a graduate of the National War College as the U.S. European Command Scholar. He holds a Ph.D. and M.S. from George Mason University and a M.A. and B.A. from California State University - San Bernardino. He is an Army veteran of the Iraq and Kosovo campaigns.

MAJ Thomas Doherty, USASOC

MAJ Thomas Doherty has a Master of Arts in Military History and a Project Management Graduate Certificate. His military experience includes time served in the enlisted and officer ranks of both the National Guard and active duty Army. He received his first commission through the Arkansas National Guard OCS program. He was later re-commissioned via a direct commission. He has served in multiple military occupational specialties spanning the aviation, medical, Infantry and SOF fields. His enlisted time includes service in the Massachusetts and Arkansas National Guards, 3rd Ranger Battalion, and 7th Special Forces Group (Airborne). His commissioned service time includes Platoon Leader of both anti-armor and long range surveillance (LRS) platoons, OC/T at JRTC, MFF ODA Commander, ARSOF CCC Instructor Team Lead, along with other staff positions. He has deployed to Colombia, Afghanistan, Iraq, Tajikistan, Botswana, and Germany. He is currently serving as a Special Forces officer.

CW4 Jeffrey Elwell, Special Forces, USASOC

Chief Warrant Officer 4 Jeffrey A. Elwell is a Special Forces Warrant Officer with twenty-six years of active duty experience, including two decades in Special Forces. He has multiple combat and operational deployments to Europe, the Middle East, and Africa. His previous assignment was as the Battalion Operations Warrant Officer for 1st Battalion, 10th Special Forces Group (Airborne) stationed in Stuttgart, Germany. He is a graduate of the National Defense University with a Master of Arts degree in Strategic Security Studies. He currently serves as the director of Special Operations Warrant Officer Intermediate-Level Education at the USAJFKSWCS Warrant Officer Institute at Fort Bragg, North Carolina.

Dr. Otto Fiala, Special Operations Command - Europe

Dr. Otto Fiala is the author of the Resistance Operating Concept at SOCEUR. He also served as a Senior Counterintelligence Analyst at USEUCOM and as USAFRICOM's Joint Doctrine Coordinator. Dr. Fiala commanded in the ranks of Captain through Colonel, retiring as an Army Reserve Civil Affairs Officer with operational deployments to Iraq and Georgia and missions in Bosnia-Herzegovina and Kosovo while assigned to SHAPE as a NATO officer. He holds a Ph.D. in International Relations from the University of Reading, UK,a J.D. from Brooklyn Law School, NY, and a B.A. in Political Science and Economics from St. John's University, NY. He remains admitted to the bar in the Commonwealth of Virginia and the State of New York. He is married to Christine Anne N. Fiala, also COL, USAR (R).

LTC Mike P. Maloney, USASOC

Lieutenant Colonel Mike P. Maloney currently serves at the United States Army Special Operations Command, culminating two decades working within the Special Operations community. His experience areas include counter-terrorism, transnational criminal activity, and international affairs in Europe, the

Middle East, and Latin America. He is currently focusing research on the contemporary and emerging global security environment and the United States' return to the great power competition space and the role of Special Operations Forces within that arena.

MAJ Robert McBride, USASOC

MAJ Robert (Bobby) McBride is an Aviation Officer with 11 years of SOF experience. Upon commissioning from the University of Notre Dame in 2004, Bobby's first assignment was in Fort Hood, TX in support of the 1st Air Cavalry Brigade, 1st Cavalry Division, where he deployed to Islamabad, Pakistan and Taji, Iraq. Following his Iraq deployment, Bobby assessed favorably for the 160th Special Operations Aviation Regiment (Airborne) and was assigned to 4-160th SOAR(Abn) in JBLM, WA, where he completed two Company Commands and culminated as the Battalion Executive Officer. MAJ McBride's aircraft ratings include the CH-47D and MH-47G Chinook. He has deployed over a dozen times in support of OIF, OEF, RSM/OFS, and the INDOPACOM AOR while supporting Joint SOF on a variety of both surgical strike and special warfare mission sets. MAJ McBride has a keen interest in strategy to include how to influence behavior change from our adversaries in the competition space while at the same time avoiding escalation. He also holds a Master of Science in Adult and Occupational Education from Kansas State University.

Dr. Spencer B. Meredith III, National Defense University

Dr. Spencer B. Meredith III is a professor of national security strategy at the National Defense University (NDU) / College of International Security Affairs (CISA) / Joint Special Operations Master of Arts (JSOMA) program at Fort Bragg. With two decades of research and support to governance and conflict mitigation, his principle areas of expertise include Russian, Eastern European, Eurasian, and Middle Eastern politics, and how those regions factor into emerging Great Power Competition. Dr. Meredith works closely with the Special Operations community, assisting with education and capabilities assessments as part of broader goals to address adversary hybrid warfare activities. He is a Subject Matter Expert for several Geographic Combatant Command, Intelligence Community, and Joint Special Operations efforts. He has briefed at the National Security Council and presented at multiple USG and NATO senior leader events. He supports several Joint Staff Strategic Multilayer Assessments, including leading the "SOF Paradigm in Great Power Competition" project, the subject of his forthcoming book.

Dr. Jason Spitaletta (Maj, USMCR), Johns Hopkins University Applied Physics Laboratory

Jason Spitaletta is a Major in the US Marine Corps Reserve and a psychologist with primary research experience in applied, experimental, political psychology, and cognitive neuroscience as well as operational experience in Psychological Operations (PSYOP)/Military Information Support Operations (MISO) and intelligence assignments in the US Marine Corps as well as Joint and Special Operations communities. He has deployed to the Western Pacific, Iraq, and Uganda. In civilian life, he is a researcher at The Johns Hopkins University-Applied Physics Laboratory as well as an adjunct faculty member at National Intelligence University and The Catholic University of America. He holds a bachelors' degree in biochemistry from Franklin & Marshall College, a master's degree in human factors from Embry-Riddle Aeronautical University, and a master's degree and Ph.D. in applied experimental psychology from The Catholic University of America. He also holds a graduate certificate from Stanford University's Summer Institute for Political Psychology.

MAJ Jeffrey Uherka, USASOC

MAJ Jeff Uherka is a Civil Affairs officer with 17 years of SOF experience. He first served in SOF as a 75th Ranger Platoon Leader and Company XO with multiple deployments to Iraq and Afghanistan. He later served across SOCEUR and SOCCENT as a Special Forces Detachment and Company Commander with the 19th Special Forces Group. As a Civil Affairs officer in the 95th CA BDE he first served as a Company Operations Officer in SOCPAC, then as a Company Commander in SOCAFRICA. Following command, he served as the BN XO for the 91st CA BN. His last CA assignment was the Brigade S3 for the 95th Civil Affairs Brigade. MAJ Uherka's professional goal over the last five years has been to enhance SOF CA's Force design and METL in order to improve CA's cross-functional integration within ARSOF and the interagency. His Masters Degree thesis at the National Defense University was entitled "Civil Warfare: ARSOF Wielding the Political and Economic Operational Variables."

Dr. David Walton, National Defense University

Dr. David Walton is a professor of national security strategy at the National Defense University. As a retired Green Beret officer with extensive operational experience in Latin America and the Middle East, his work and research focuses on operationalizing great strategy for better results.

LTC (R) Gordon James Worrall, Special Operations Command - Europe

LTC (R) Gordon James (Jim) Worrall is a Resistance Planner at SOCEUR. Prior to SOCEUR, Jim was a U.S. Army Special Forces Officer. He is a graduate of the Chilean Army War College. He holds a M.S. in International Relations from the University of Miami and a B.A. in Political Science from the University of Central Florida. His operational assignments include service in Iraq, Djibouti, Chile, and Honduras with multiple deployments in the SOUTHCOM AOR.

SOF Paradigm in Great Power Competition

Editor: Dr. Spencer B. Meredith, III National Defense University[1]

The current National Security, Defense, and Military Strategies identify great power rivalries from Russia and China as two of the main challenges facing the United States for the foreseeable future. The transition from non-state threats to existential ones posted by great powers means more than reallocation of resources, as important as those are for the coming fights. It must also include paradigm shifts in the ways the United States organizes it forces, authorizes their uses, and justifies the application of all elements of national power in the pursuit of national security.

The purpose of this Invited Perspective Paper is to explore the implications of the Special Operations Forces (SOF) Paradigm in the emerging Great Power Competition (GPC) space. It resulted largely from the "SOF Paradigm in Great Power Competition" Speaker Series as part of the Joint Staff Global Competition and Conflict Strategic Multilayer Assessment. Like the Speaker Series, this concept paper evaluates more than existing Special Operations capabilities focused on counter Violent Extremist Organization efforts. More broadly, it considers the ways current approaches can be applied to great power rivalries within the full-spectrum of hybrid warfare. It also expands the potential applications of SOF instruments to historic and emerging areas of the competition space. The project is by no means intended to be exhaustive or the final word on the specific topics, instead presenting promising ideas that represent some of the adaptations currently underway in the Special Operations community.

---

[1] Author <u>contact Information</u>: spencer.b.meredith.civ@msc.ndu.edu

Chapter 1. SOF Paradigm in Great Power Competition

Dr. Spencer B. Meredith, III National Defense University and LTC Mike P. Maloney, USASOC[2]

Viewing VEOs through Great Power Competition

The National Military Strategy makes clear that violent extremist organizations (VEOs) are not going away. It recognizes that while great power competition will define the emerging security environment for the foreseeable future, VEOs will remain a potent threat to the United States. A key challenge as we enter into hybrid warfare with state adversaries is to understand the ways non-state actors evolve as *proxies*, *puppets* and in rare cases, *partners* with great powers. This article addresses several core aspects of VEOs in great power competition, and how the United States can counter the multiplying threats facing the nation.

VEOs are changing their tactics, operational planning, and strategic goals to take advantage of the increasing patronage available by Russia and China. This is being done in part through a growing awareness by VEOs that US attention has shifted away from the Middle East as the central area of operations. That awareness has also identified a wider spectrum of options to threaten US interests in great power competition. The net result has been an increasing intent to include great power goals, methods, and messaging into VEO approaches and activities.

Russia and China actively support converging around common goals to undermine US leadership of the global system. Yet neither patrons nor clients maintain any illusions that either actually believes in the other's self-interests. Instead, these unions serve a few simple purposes. First, VEOs pursue self-interest as vociferously and viciously as Russia and China. At the same time, a key difference is that Russia and China have the ability to play longer games, giving them longer visions of the future. Such perspectives reduce the incentives to maximize efforts through short, sharp bursts of activity, something VEOs must rely on instead. This can be seen through the rapid acquisition of territory, manpower, and materiel during ISIS's initial breakout, the Jalisco cartel's rise to prominence, and Antifa's emergence via increasingly violent street protests. Most of all, *VEOs must strike first, strike hard, and show no mercy to the opposition*. Rigidity of purpose and short timeframes are necessary to ensure they maintain adequate market share in the increasingly crowded field of revisionist ideas and organizations. As a result, *great power patronage gives VEOs much needed attention and operating space to maneuver against an increasingly aware and awakened United States*. <u>The US should expect to see more of this in the future, not less.</u>

Second, great powers can utilize VEOs in myriad ways for the very simple reason that *hybrid warfare incentivizes full spectrum actions at all levels of political, economic, and social settings*. From the obvious violence targeting civilian centers, to the less frequent but still viable regular warfare when VEOs gain the means of state resources—either from their enemies or through illegal arms sales—VEOs have potent weapons that great powers all too readily support. Less obvious avenues also present themselves. Political warfare fought in the world of public opinion does more than seek to frighten

susceptible populations. It also undermines support of otherwise legitimate governments. VEOs can just as easily expose core governance weaknesses that permit VEOs to operate within the state's territory, as demonize the inevitable government "overreaction" to appear strong in the face of VEO challenges. Legal jurisdictions also become the ensuing battleground as VEOs function within the seams of overlapping governmental boundaries. Doing so can effectively throw interagency working relationships into turmoil as all sides devolve into blaming for failures, or clamoring for success at the expense of others. <u>Hybrid warfare therefore offers a gold mine for VEOs in their own right, and infinitely more so when supported by great power states.</u>

The most common method of such support comes as a *proxy*. The Cold War brings to mind the most recent examples of proxy battles, but by no means have they been limited to the last century. Ancient Rome, Cortez in Mesoamerica, Belgian colonial policy, and early 20th century Japanese machinations in Manchuria each exhibit variations of great powers using smaller proxies in their battles with powerful rivals. Equally so, those times also show how non-state actors sold themselves as "Gray Zone" solutions below the threshold of overt, direct hostilities that threaten escalation by powerful states. Critically, the opportunity costs are low for great powers to use proxies, and VEOs can easily manipulate the conditions of great power competition to gain advantage against their own enemies. The net effect is that today's VEOs follow a long line of proxies in great power competition, many of which show clear pathways to "punch above their weight class."

A second variation of VEOs in great power competition minimizes their awareness of great power plans, often with little effort to align goals. These *puppets* are less likely to acknowledge patronage by great powers, if they are even mindful of it. In the case of mass movements in democracies, from the French National Front and Bharatiya Jabata Party in India, to the migrant caravans of central America, the average member likely has no idea of the organization's support by outside actors, let alone their linkages to great power states. Yet the fact of that ignorance does not diminish the benefits such democratic puppets bring to Russia and China. At a minimum, media coverage for these "legitimate" VEOs allows great powers to reap the rewards of undermining the democratic process of rival states. At the maximum, they can swing the tide of elections in favor of pro-Russian/Chinese candidates. Such was the concern in the run up to the 2019 Ukrainian presidential election. Then-candidate Zelensky's apolitical appeal raised the specter of doing more than just upending the established post-Maidan ruling clique. There were worries that he could subvert the very democratic trajectory of Ukraine by submitting to Moscow as Yanukovych had previously done. Such an outcome would certainly not lead to a quiet return into the Kremlin's orbit, but the ensuing chaos would still achieve Russia's chief goal in the region—fundamentally undermining the legitimacy of an independent Ukraine. Whether that possibility remains on the table remains to be seen, but the fact of its potentiality translates further afield for other potential Kremlin enclaves to arise in Europe as in Turkey, Bosnia, and Russian-leaning Bulgaria.

On the other side of the spectrum, the final option for VEO roles in great power completion is also the rarest. *Partners* require far more upkeep and raise strategic operating costs for great powers, not least because the clear connection between VEO activities and great power support threatens great powers' abilities to manage escalation. If such a relationship is to exist then, VEOs must present a clearly unique

---

[2] Author <u>contact Information</u>: <u>spencer.b.meredith.civ@msc.ndu.edu</u>

benefit to the great power. Two common ways include supporting the state's initiatives more broadly as champions of its international reputation in the United Nations, or through directly undermining the partner of a rival great power. Current examples of Hezbollah and the Maduro regime can be seen in this light, even though they also challenge traditional lines of being *either* a state *or* non-state entity.

Hezbollah stands out as a directly funded, openly claimed Iranian partner in the struggle for dominance of both Lebanon and the Levant. It also plays a key role in the regional great power struggle between Shia/Persian Iran and Sunni/Arab Saudi Arabia, to say nothing of galvanizing the counter-Israel movement worldwide. Yet Hezbollah also offers a unique advantage to Iran as a "legitimate" political actor, thereby sanctioning Iran's open relationship with the long-standing VEO. In that sense, Hezbollah crosses boundaries as a state and non-state entity through its official standing in Lebanese politics, and because of that ambiguity, remains a viable and potent tool for great power strategy.

The Maduro regime also crosses those lines, albeit in different ways. Maduro and his narrow clique of kleptocrats currently still have international support from Russia and China as the legitimate government of Venezuela. In large part due to Moscow's "anti-regime change" stance for anti-democratic regimes, and Beijing's resistance to external intervention in even the most heinous human rights conditions, both great powers stand by the standing government against the United States and its Latin American partners. Thus, despite mounting alternative bases of support for opposition governance, the Maduro regime remains the government of Venezuela at the time of writing this paper. However, the extremism of its ideologically driven violence against the Venezuelan people, the vagaries of its legal standing, and the clear necessity of international props to keep it going, all serve as indicators of a VEO partnership operating in great power competition.

Police brutality and torture clearly stand out as main aspects of Maduro's socialist violence. Yet so does fostering the spiraling humanitarian crisis through catastrophic mismanagement of the economic emergency, to say nothing of blocking international aid shipments. Yet Maduro and his supporters do not earn the VEO moniker solely based on violence. Nor does virulent socialist ideology in itself prove sufficient to name a sitting government as a VEO. However, the doubling down on revolutionary ideology in the face of clear evidence that 1) the revolution has failed and 2) the masses of Venezuela have rejected its mass mobilization, indicates that the regime is out of step with the normal practices of governance. Such extremism combines with its pariah status among a growing list of international parties. Under such conditions, Maduro and his supporters have become either an entrenched insurgency or an occupying cadre with contested control over key state resources, all with support from outside actors. Like Hezbollah, the Maduro regime can thus be seen as a VEO partner in great power competition. Doing so reveals the range of options for VEO activity in the emerging security environment, one that far exceeds the preceding post-Cold War era.

Thus, as hybrid warfare between great powers operationalizes everything along expanding lines of contact, VEOs will continue to require direct action by the United States to counter them. *That action must see them as targets in themselves, and see through them to the larger adversaries benefiting from VEOs in great power competition*. It does not take much imagination to identify the scope of possible horrors wrought by a renewed ISIS-type VEO directly funded by Moscow or Beijing. Such a group need not retain ISIS-like caliphate goals, nor would it likely even be Islamist in that regard. The growing counter-US/counter-democratic/counter-capitalist factions within democracies themselves are potent enough movements and fertile grounds to grow renewed socialist VEO uprisings. Putin's reclamation of

past Soviet glories and even more importantly, excusals of past atrocities, further justifies socialism as a narrative of anti-US VEOs. Combined with the "Communist" character of Beijing's statist strategies, one need not gaze far into the future in order for the past to become prologue, and socialism's return to become more than mere coincidence.

To see this way—reconceptualizing the VEO threat as more than Cold War analogs or Global War on Terrorism (GWOT) enemies—and then to act upon that insight, the US must rely on several approaches. First is the need for effective *globally integrated campaigning* as the way to harness full-spectrum elements of national power across the vast competition space. Second, we must develop *intellectual overmatch* to remain agile in identifying 1) strategic vulnerabilities in our adversaries and 2) ways to turn them into opportunities for countering aggressions.

Seeing SOF Anew in Great Power Competition

For nearly two decades, Special Operations Forces (SOF) have been employed worldwide predominantly to counter VEOs. At the forefront of US military efforts to understand and defeat those organizations, SOF operate within the human domain of conflict and specialize in population-centric warfare. The most recent operations have been in the Global War on Terror, but SOF have deeper and wider roots in hybrid warfare that need to be resuscitated for great power competition.

Following the successful unconventional warfare (UW) campaign to overthrow the Taliban regime in Afghanistan, national missions shifted to counter-VEO approaches. At their core, counter-insurgency (COIN), counterterrorism (CT) and Foreign Internal Defense (FID) quickly became the bedrock of the Global War on Terror. Yet COIN and FID have been part of a broader SOF portfolio since before the Taliban arrived on the US radar. However, the post-9/11 fervor focused SOF in narrow ways that allowed many Cold War approaches to atrophy. The resulting "overly-specialized" vision of what SOF can bring to the fight must change as the nation turns its attention to the threats posed by Russia and China.

Functionally, SOF elements are often employed as small, low-footprint teams ranging between two and twelve people. Their tasks generally center on working with partner military, police, humanitarian, and/or governance organizations at the behest of the US Ambassador to that country. That mission set does not preclude countering VEOs though. *SOF elements have been tasked with seeing through training of partner security forces and governance capabilities to the deeper human networks that give rise to and support VEO influence*. This critical skill set makes SOF a vital resource to counter Russia and China in great power competition as well. However, the perception of SOF mastering the "down-and-in" of non-state human networks has limited how decision makers see the scope of their utility. This paper shows that the same human network mastery can and should be applied to "up-and-out" networks in great power competition.

Counter-VEO accomplishments have ingrained this task into SOF identity, with many decision-makers understanding SOF roles as inherently limited to the non-state mission set. Yet viewing the fight to defeat ISIS's physical caliphate only through that lens easily bogs down strategic thinking in the near fight, to the detriment of preparing for the next VEO possible within the Middle East and elsewhere. While the rise of a digital caliphate inspires some interest to look beyond the next ridgeline, the more pressing and dangerous VEO incarnations will be those employed and supported by Russia and China. SOF needs to pivot towards them.

As the United States dusts off the peer competitor playbook and gazes out at the global competition space once again, some have argued instead that SOF should remain primarily, if not exclusively tied to what it "does best" with VEOs only. *This short-sighted view misses both the modularity of SOF and the complexity of hybrid warfare*. While tying SOF to the VEO problem might appear to free up conventional tools for the global competition space, critically, the United States is not re-entering the Cold War battlespace. That environment is gone forever, having morphed with GWOT into the full-spectrum hybrid warfare of the 21st century. The current competition space is more complex, moves faster throughout population-centric networks, and lacks the established Cold War "red phone" dampening mechanisms to control the rate of escalation. Accordingly, a vital tool to understand this new environment and generate options to compete well over time is already in the appropriate places. Deployed SOF teams can and must be a vehicle for seeing through VEOs to great power competitors. Doing so increases the options for SOF to support conventional operations and the other elements of strategic competition.

Viewing the global competition space through the VEO lens coincides with many of the other existing SOF approaches. The United States needs partners that can fight and hold terrain, albeit most effectively when backed by coalition airpower and with coalition provided arms and equipment. The United States needs the support of local governments to motivate their populations to resist VEO narratives and remove resources from VEO movements. Most importantly, the United States needs defined goals and objectives to demonstrate success against these organizations. The defeat of the physical caliphate in Iraq and Syria; the removal of all ISIS forces in Sirte, Libya; or the degradation of the Taliban's ability to influence the government of Afghanistan, have been put forward as ways to defeat VEOs. Instead, by viewing the global competition space through the hybrid warfare lens, VEOs become a piece on the chessboard rather than the main opponent. As a result, SOF elements that were previously limited to certain moves in the VEO game can now employ more effective moves in support of strategic victory against great power opponents.

Chapter 2. Special Operations Command Europe's Resistance Operating Concept (ROC)

Dr. John DeRosa and Dr. Otto Fiala (with support from LTC (R) Jim Worrell)[3], Special Operations Command Europe

Background

1. Historic Backdrop. During the Cold War, both NATO and Warsaw Pact forces, particularly the United States and the Soviet Union, maintained vast numbers of military forces along the Iron Curtain border in Europe. Additionally, several NATO allies also maintained stay-behind networks within their countries to act against Soviet forces in case of invasion, maintain popular morale and send intelligence out of occupied territory to non-occupied NATO allies. Upon the dissolution of the Soviet Union, the stay-behind networks were completely dismantled.

In the 21st century, a resurgent Russia began to re-assert its power and influence in several former Soviet Republics. These actions resulted in its seizure of Crimea and support to separatists in Eastern Ukraine. These actions and the Russian threat to the Baltic nations led to the U.S. European Defense Initiative (EDI) in 2014. Concurrently, recognizing the lack of enough forward deployed conventional forces to provide effective deterrence, SOCEUR began exploring the concept of resistance with our Baltic NATO allies as well as other allies and partners.

2. Project Beginnings. SOCEUR began developing this multinational concept with certain allies and partners in 2014, through the method of seminars. The seminars were rotated among the nations in order to gradually increase participation from other government Ministries. These seminars included writing workshops in later 2015 through 2016 to outline the concept and fill the gap of a lack of specific doctrine. Later versions of the ROC benefitted from additional seminars, workshops and exercises.

3. Resistance Defined. Eventually, the ROC defined resistance as: "A nation's organized, whole-of-society effort, encompassing the full range of activities from nonviolent to violent, led by a legally established government (potentially exiled/displaced or shadow) to reestablish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power."

The ROC

1. Doctrinal Gaps. This document was developed to meet very specific planning requirements and fill existing gaps in the doctrinal literature of the participating nations, including gaps in U.S. Army and Joint doctrine. The primary reason for this was because of the lack of doctrinal guidance for pre-conflict resistance planning with allies and partners. Though much was borrowed from existing U.S. Army, Joint and other U.S. government publications, none of them had the direct treatment of the topic necessary for our purposes or were succinct enough for allies and partners who spoke English as their second language.

---

[3] Author contact Information: john.derosa@socom.mil; otto.fiala.ctr@socom.mil; gordon.worrall.ctr@socom.mil

2. Relevant Joint Doctrine. The ROC's definition of resistance carves out a space within the definition of Unconventional Warfare (JP 3-05). It describes an organization authorized by the legitimate government of an ally or partner, to fight a foreign occupier, which we assist through our application of UW. Specifically, the ROC's definition focuses on restoring the territorial integrity and national sovereignty of an Ally or Partner Nation (A/PN), in accordance with international law, and contains pre-conflict planning implications. Resistance as a concept falls under UW but is refined to describe a form of warfare by an A/PN against an occupying power, and can be supported by the Joint Force. Thus, USSOF engage in UW to support A/PN resistance.

The present joint definition of "resistance movement" (JP 3-05) allows its application against a "legally established government," making "resistance movement" practically synonymous to "insurgency." The current UW definition of "resistance movement," can be interpreted to mean that a resistance movement can be applied against a (legally established) "government." In contrast, the term "resistance" as used in the ROC, describes an organization which only acts against a foreign occupier. Consequently, the ROC's definition of "resistance," which is widely understood and accepted by SOCEUR's Allies, is not currently defined in joint doctrine. Additionally, the term "resistance" has positive historic and present-day resonance.

3. Critical Points for Resistance.

a) Purpose - The purpose of the resistance effort is to; gather and transmit information outside of occupied territory, support the morale of the occupied population, disrupt occupier control, and assist the entry of friendly conventional forces to remove the occupier. Historic analysis reveals that national resistance efforts against foreign occupiers are not alone successful without a powerful outside partner. Efforts without powerful external partners fail against powerful and ruthless occupiers. Additionally, during peacetime phase zero planning, U.S. support to the development of resistance organizations within specific allies and partners is a strategic communication message to a potential adversary by supporting deterrence.

b) National Legal Framework - A primary point within the ROC is consistent emphasis on the development of a national legal framework authorizing the establishment and development of a resistance plan and resistance organization. Many Cold War era European stay-behind groups lacked sufficient legal authorization. Such lack of sufficient authorization for some of their preparatory activities as well as directions given to them by their concerned ministries jeopardized their legitimacy. Aspects of these organizations were made public during the dissolution of the Soviet Union and their questionable legitimacy politically tainted them. The ROC consistently emphasizes a supporting legal framework for their establishment and adherence to the law of war during occupation.

c) International Law - The development of a pre-crisis resistance organization is authorized by the sovereign national government. The ROC emphasizes the need for threatened governments planning resistance to also plan to exile certain leadership to pre-planned and arranged locations in order to continue to retain sovereign representation of occupied territory. Under international law, the displaced or exiled government retains its status as the legitimate representative of the occupied territory and will be recognized as such by the U.S. During an occupation, the sovereign national government, displaced or exiled, authorizes and directs the activities of the resistance

organization against an occupier. These activities must be consistent with the nation's rule of law and international legal norms. Comportment with international law is critical to retaining international support and legitimacy.

4. A Common Planning Guide. The ROC serves as a common planning guide between SOCEUR and allied planners through common terms, definitions and perspectives. For U.S. planners, it also explains relevant U.S. doctrine and distinguishes resistance from insurgency under unconventional warfare. Terms such as "guerrilla," "auxiliary" and "shadow government" were carried over from U.S. doctrine for the sake of ease of reference. Using these terms facilitates the use of common, existing, and historical terms, and preserves their terminological utility while also facilitating further research on the topic.

5. Resilience Defined. In addition to the concept of resistance, national resilience was also discussed throughout the seminars. The ROC devotes a chapter to national resilience. Societal resilience has two primary aspects for our purposes. First, national resilience describes a cohesive and integrated nation, able to withstand foreign efforts to gain leverage within that nation by asymmetric or hybrid methods. Second, strong national resilience will support resistance against a foreign occupier to regain territorial integrity and national sovereignty. The ROC defines resilience as: "The will and ability to withstand external pressure and influences and/or recover from the effects of those pressures or influences."

Principles of Resistance Planning

Resistance is a legitimate form of national warfare against a foreign occupier. Once established and developed, it can be used against a foreign occupier in situations of partial or full occupation, as well as against proxy forces denying national sovereignty and operating on behalf of a foreign power.

1. Organizing Entity. Prior to a crisis, the government establishes an organizing entity to establish, develop, and guide a resistance organization for use against a potential occupier (full, partial or proxy occupation). This entity, ideally within the Ministry of Defense (MoD), is responsible for pre-execution planning and organization of the resistance campaign. The organizing entity should recruit effective leadership for each resistance component (Underground, Auxiliary, Guerrilla Forces, Public Component) to assist in resistance organization and preparation, and who will form the core cadre. The organizing entity develops, rehearses, and tests the resistance plan.

2. Unifying Purpose and Intent. The success of a national resistance is dependent on a population's support, involvement, contributions, and necessary resources to accomplish resistance campaign objectives. A common purpose and government ability to motivate the population to take action is fundamental to a national resistance.

3. Guiding Narrative. Established well before a crisis, a well-crafted resistance narrative will unify government and societal functions to integrate public and private sector efforts with minimal friction. The narrative will provide the basis for communication between the government, its population, and the international community. Additionally, a well-crafted resiliency narrative can also serve as a strategic deterrent to adversaries.

4. Resilience. Preparation for resistance by the above described organizing entity bringing unity and purpose to the effort, and supported by a guiding narrative, contributes to resilience. Enhancing and

institutionalizing collaboration among government ministries, civic organizations, and the larger public is critical to success. This collaboration helps build a more resilient society and strengthens resistance networks established in the event resistance is required. A society's resilience contributes to deterrence and supports national defense planning, to include resistance to regain national sovereignty, as well as the final post-resistance restoration of sovereignty.

5. Maintenance of Rule of Law and Political Legitimacy. Adherence to the rule of law is intrinsic to the concept of legitimacy. The application of the rule of law maintains political legitimacy.

> **a. Rule of Law** – Adherence to the rule of law refers to programs conducted to ensure all individuals and institutions, public and private, and the state itself are held accountable to the law, which is supreme. The rule of law is characterized by just legal frameworks, public order, accountability to the law, access to justice, and a culture of lawfulness. Rule of law requires laws that are publicly promulgated, equally enforced, independently adjudicated, and consistent with international human rights principles. Resistance activities must adhere to the rule of law at all times.

> **b. Political Legitimacy** - Political legitimacy is based on an understanding of the state as a political organization formed through a social contract. In the social contract, legitimate political authority comes from the consent of those being governed. To demonstrate its support for the rule of law and bolster its case for legitimacy, any violent or nonviolent measures the resistance conducts should fall within the framework of applicable national and international law.

6. Control and Oversight of Resistance Activities. Effective planning between government ministries, interagency organizations, military, and other societal elements assists in establishing structure, processes, and expectations that help control and mold resistance behavior. Resistance leadership must maintain command and control of all resistance activities to ensure compliance with legal standards and ethical mores inherent in the resistance narrative. Elements conducting resistance activities outside the command and control of the regional and national resistance leadership risk discrediting claims of adherence to the rule of law.

7. Whole-of-Government and Whole-of-Society Collaboration (Total Defense). Government resistance planning prior to crisis outbreak is central to successfully establishing the components and capabilities for resistance activities. The national government should institutionalize collaboration among and across governmental organizations, civic organizations, and the larger public in order to prepare the society for resistance, which also contributes to building resilience. Detailed integration and collaboration among government organizations is necessary to effectively plan for resistance.

8. Agility and Adaptability. A resistance campaign can be influenced by both supporting actors and adversarial actors. Resistance campaigns must possess the ability to adapt to changes. Supporting actors may adjust the degree, type, or timing of support and the adversary may adjust the methods used to consolidate control over occupied territory and its tactics employed against resistance.

9. Post-Crisis Continuity of Government. Continuity of government plans for a displaced or exiled government must be made and must address certain requirements, in addition to plans for a shadow government in occupied territory.

a. Inter-governmental and International Coordination - This activity helps ensure resistance roles and responsibilities are well understood and increases the credibility and legitimacy of an exiled or displaced government. Inter-governmental planning engages other governments and international planning, including leveraging diaspora, engages other international organizations and entities.

b. Legal and Policy - A legal framework must be established and recognized to enable preparation and execution of resistance plans and activities. The legal and policy frameworks should also enable inter-ministerial and inter-governmental strategic communication and information sharing agreements that respect operational security requirements, support successful resistance operations, and enhance legitimacy. The long-term purpose of these frameworks is to retain legitimacy throughout the period of occupation and return to pre-conflict status.

c. International Agreements - During pre-crisis, formal agreements with allies, partners, and international/multinational organizations (as applicable), in support of a resistance campaign, facilitate legitimacy, increase resiliency, can deter an adversary, and streamline actions necessary during resistance.

d. Pre-planned Resistance Networks - Required resistance networks that should be planned and possibly staffed with core cadre during pre-crisis as part of the resilience effort include, but are not limited to: logistics, medical, information/messaging, finance, education/training, transportation, recruiting, communication, intelligence/counterintelligence, security, and sabotage and subversion.

Way ahead

1. ROC Publication. In 2018, ROC V5 was presented to the Swedish Defense University and the Joint Special Operations University (JSOU) for review for potential publication. After academic review of the ROC, each institution agreed to publish it. Publication by the Swedish Defense University places the ROC into European academic circulation while making it accessible to a broad European based audience. Publication by JSOU places it into U.S. Special Operations Forces circulation while also making it accessible to a broad military audience.

2. Planning, Exercises and Training. SOCEUR continues to support A/PNs in their resistance planning efforts by integrating planning, exercises and training. These activities are accomplished through joint planning and training in those nations, as well as training the concerned SOF of select nations at stateside facilities. Additionally, in coordination with SOCEUR, JSOU offers three courses to U.S. and A/PN personnel on the topics of resistance and unconventional warfare, with each course targeting a different audience and level of understanding. These courses are offered to continue the development and co-education of both U.S. and A/PN concerned personnel.

3. Allied Doctrine. NATO presently does not recognize resistance as a form of warfare, due primarily to the Cold War experiences of certain nations with stay-behind forces that were not properly legitimized by those nations. Thus NATO does not possess applicable resistance doctrine. SOCEUR seeks eventual incorporation of aspects of resistance into NATO doctrine. Though the resistance concept was developed within the European theater of operations, specifically against a Russian threat, it has applicability in other parts of the world, such as the INDOPACOM area.

4. Application outside Europe. Other regions also have a history of resisting occupying powers. Recently, the People's Republic of China has become more assertive and expansive in the INDOPACOM region. It has taken drastic steps against potential internal opposition (i.e Uighurs), become more assertive towards its neighbors, and created artificial islands in the Spratly Islands chain for potential military use. The nations on its periphery, including island nations to its south and east, thus face a situation very similar to some of the nations on the west of Russia's periphery. Thus, increased resiliency among those nations as well as knowledge of resistance preparation as outlined in the ROC would benefit them as well.

Conclusion

Resistance is not a new form of warfare but has been historically used by nations against foreign occupiers. Resistance can be planned during peacetime in a pre-crisis environment to prepare against a specific foreign threat. The successful preparation and conduct of resistance relies on national resilience. A cohesive nation is better able to withstand foreign asymmetric or hybrid methods to gain leverage within that nation in order to weaken its national resolve. Strong national resilience can deter foreign aggression and if deterrence fails, it will support resistance against a foreign occupier to regain territorial integrity and national sovereignty.

Chapter 3. Sabotage, Subversion, and Nonviolent Resistance: A Nuanced Approach to Special Warfare in Great Power Competition

Dr. Jason Spitaletta (Maj, USMCR), The Johns Hopkins University Applied Physics Laboratory[4]

Abstract

As US Special Operations Forces (SOF) conceptualize their role in contemporary great power competition, they must draw upon and apply the lessons learned from decades of research and operations in irregular warfare, including the experiences of the Special Operations Executive (SOE) and Office of Strategic Services (OSS) during World War II, in order to provide unconventional options in support of conventional sociopolitical objectives. These lessons are particularly relevant to the US Army Special Operations Forces (ARSOF) who view resistance as their raison d'etre (Meredith, 2019). The following paper draws from research conducted on the psychological aspects of insurgencies and revolutions published as a chapter entitled "Nonviolent Resistance" in *Human Factors Considerations of Undergrounds in Insurgencies, 2ⁿᵈ Ed* and a chapter entitled "Human Factors Consideration of Underground in Cyber Resistance" in *Resistance and the Cyber Domain,* both components of the US Army Special Operations Command's Assessing Revolutionary and Insurgent Strategies (ARIS) project[5].

Introduction

The purpose of underground[6] psychological warfare is often to cultivate support among the neutral and uncommitted; to raise morale and reinforce existing attitudes and beliefs among the committed; to undermine confidence in the existing government; and to lower the morale of government forces and personnel (Bos et al., 2013). In contemporary great power conflict, underground psychological warfare must nest within the larger national strategy but be sufficiently distinct from those efforts to afford Special Operations Forces (SOF) both the freedom of maneuver and operational security required of activities that entail both overt and covert aspects. This freedom of maneuver is necessary to afford tactical flexibility since, historically, the substantive content of psychological operations is likely to be determined at the highest echelon of the organization. However, the rapidity with which a resistance movement can interact with various target audiences has resulted in a more decentralized approach to influence (Bos et al., 2013). The aforementioned substantive content must be framed as resistance in order to capitalize on the psychological and/or operational expertise of SOF. Underground

---

[4] Author contact Information: Jason.Spitaletta@jhuapl.edu

[5] https://www.soc.mil/ARIS/ARIS.html

[6] The term "underground", outside the study of insurgencies, typically refers to the relatively inaccessible subculture of any particular sector. In a revolutionary or insurgent movement, the underground refers to a clandestine organization established to operate in areas denied to the armed or public components or conduct operations not suitable for the armed or public components. The underground is generally responsible for leadership and organization, recruiting, intelligence, financing, logistics, training, communications, security, subversion & sabotage, and psychological operations (Bos et al., 2013).

psychological warfare is conducted in a variety of forms: mass media and face-to-face persuasion; leaflets and theatrical performances; programs for local civic improvement; and threats, coercion, and terror. Underground psychological warfare conducted by the Special Operations Executive (SOE) and Office of Strategic Services (OSS) during World War II are replete with examples in each of these forms (Foot, 2004, Chalou, 1995) and can be used as an example of SOF integration in great power competition.

The term "human factors" has a rather broad set of interpretation depending on the context in which the phrase is used. The Intelligence Community considers Human Factors Analysis (HFA) the evaluation of psychological attributes (motivation, thinking style, beliefs, and personality), cultural attributes (values, beliefs and norms that influence behavior), behavioral attributes (responses to context or stimuli independent of personality), as well as the neural correlates of those attributes In order to influence decision-making (how individuals and groups select a course of action), information-flow (how individuals and groups acquire information required to make a decision), objective reasoning (how individual and groups process information they receive), neurobiological changes to (or away from) specific states, and ultimately, behavior of individuals and groups in any state or organization (Spitaletta, 2016). SOF should prioritize HFA in its intelligence requirements as a rich contextual understanding of the relevant human factors is a necessity in any form of irregular warfare.

Irregular warfare has evolved considerably since SOE and OSS operated in occupied and/or otherwise denied areas of various WWII theaters; the subsequent eras saw wars of national liberation and the emergence of religious and commercially-based resistance movements (Crossett, 2012). The development of computer-based communication technologies has not changed the nature of irregular warfare, but it has altered the characteristics, such as speed, reach, and effectiveness of the psychological battle to inform and influence various target audiences. As a result, these technologies have become the logical medium for political and psychological warfare (Bos et al., 2013). Irregular conflict is no longer geographically constrained or relegated to the grievances of a local in-group but often waged, violently and nonviolently, globally for a local political objective. From peaceful social mobilization (Barry, 2011) to "internet guerrilla warfare" (Carlin, 2018), cyberspace has become an increasingly contested operational environment. SOF will need to consider the cyber domain in their planning considerations as it, more so than any ungoverned physical territory, has the potential to enable disproportionate effects on small groups and individuals and these asymmetries should be exploited to advance US objectives (USASOC, 2015). Included in those considerations, must be the more nuanced approach to unconventional warfare, whether as a main or a supporting effort, that includes sabotage, subversion, and nonviolent resistance.

Sabotage

Sabotage denotes actions to withhold resources from the government's counterinsurgency effort by acts of destruction. This includes acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources (Bos et al., 2013). These types of operations, referred to as agitation during the Cold War, include tactical observable actions that reinforce strategic psychological warfare operations (Bos et el, 2013).

There are two common forms of this type of action propaganda by insurgent groups: one focuses on specific actions that alleviate suffering among the people and demonstrate the insurgents' ability to accomplish set goals, while the other focuses on military acts, violence, sabotage, and punishment of traitors among the local population. Both show that the insurgents are powerful in spite of being outnumbered. It is a truism of psychological warfare but bears repeating: the combination of words and actions, when applied with planning and consistency, is more powerful than either used in isolation (Bos et al., 2013).

The increasing reliance of critical infrastructure in the developed world (and in many places in the developing world) on the Internet make for innumerable opportunities for sabotage. Highly sophisticated and/or well-protected supervisory control and data acquisition (SCADA) systems require both a high degree of skill and persistence (the combination being rare in many cyber collectives), but make for logical targets of more politically-committed organizations. Attacking SCADA systems also creates a defensive prioritization dilemma for local security (and cyber security) forces. These dilemma actions force the authorities to choose between allowing such activities to continue, and taking the risk that they will build into something significant, or imposing harsh punishment on people who are engaged in a seemingly benign activity (Barry, 2011)

Subversion

Framing a component of a great power competition as resistance, an organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability, is useful when conceptualizing a clandestine role for SOF. Identifying a target of resistance, for example the internal security forces, which bear a major share of the burden of maintaining order, provides a foil for a nascent movement (Bos et al., 2013). The underground's use of subversively manipulated crowds and civil disturbances adds a new dimension to the problem of maintaining internal security. The difference between civil disturbances that are subversively manipulated and those that are not can be expressed in terms of objectives. Strikes, riots, and demonstrations usually have limited goals, such as better working conditions or social changes, whereas subtler efforts like factory production slowdowns attempt to degrade industrial capacity (Bos et al., 2013).

The Internet has dramatically increased the opportunities for both subversion and sabotage, integral aspects of comprehensive underground psychological operations. Subversion refers to actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority (Bos et al, 2013). The manipulation of existing or complete fabrication of social movements (or astroturfing) can have profound economic, political, and psychological effects even at the societal level (Kraemer, Whiteman, & Banerjee, 2013).

Organizations can leverage large-scale subversive capabilities to achieve direct effects or to use as a deception operation to obfuscate their true intent. The intentional spread of disinformation through the use of botnets has become a common tactic by state and non-state actors (Shao et al., 2018), forcing security forces and/or political opponents to respond to false information puts them at an information disadvantage preventing them from anticipating the effect of any story or operation. In some cases, botnets were used to promulgate disinformation about government atrocities by fabricated humanitarian organizations (Reno & Matisek, 2018). A particularly effective approach is deliberately targeting "key influencers", accounts with numerous followers likely to interact with bots,

to forward the information and establishing a false sense of credibility via social proof that contributes to the proliferation of misinformation (Stella, Ferrara, & De Domenico, 2018).

Nonviolent Resistance

Nonviolent resistance has long played role in many underground and revolutionary activities; Gene Sharp identified 198 types of nonviolent action dating back centuries. As the technological means by which social movements are organized have evolved to include modern technology and social media, unique technology-mediated forms of protest have also been developed (Bos et al., 2013). Some social movements rely on nonviolent tactics exclusively; some integrate them with military actions (although this tends to undermine the legitimacy of the nonviolent aspects), and many have developed ways to subversively manipulate nonviolent actions such as street protests to provoke violent confrontations, justify retaliatory attacks, or divert attention from other actions. Nonviolent actions can be classified into three broad categories: attention-getting devices such as street protests and street performance art; noncooperation techniques such as boycotts and work slowdowns; and civil disobedience campaigns such as sit-ins and mass protests (Bos et al., 2013).

Nonviolent resistance continues to play a prominent role in many underground and revolutionary activities, and the 21st century has witnessed a synthesis of the global technological networks that link computers on the Internet and social networks to result in innovative forms of protest (Kleinberg, 2008). The exhaustive set of tactics Sharp identified typically focus on the physical domain, however, there are numerous corollaries to cyberspace and thus nonviolent cyber resistance has manifested in innovative forms of protest have emerged in the post-Cold War era. Although few have managed to mobilize a sufficient number to displace a regime, they have provided a forum for a youthful demographic to engage in creative, often social-media-directed alternatives to the picketing and chants their elders employed (Barry, 2011). Participating in nonviolent cyber resistance can take many forms, from changing one's avatar (Satell, 2015) to espousing a form of resistance clothing (Delistraty, 2018). Successful social movements tend to 1) directly confront and reframe perceptions about a particular sociopolitical issue, 2) exploit existing social networks and simultaneity to achieve the greatest effect, and 3) connect the ideologues to the mainstream population (Satell, 2015).

Both cyber activism and hacktivism have made each of these attributes both more accessible to the average individual and/or accentuate the effect of them. This trend is likely to continue, as the opportunities for the voiceless to find their voice are numerous and growing as is discontent with the political status quo and the concomitant passivity. In order for cyber enabled nonviolent resistance to be an effective instrument of US statecraft, the "disruptive" thinkers within the US must recognize their own in other nations and implement the appropriate tactics to enable them to accomplish their sociotechnical and/or political objectives (Maxwell, 2017).

Summary

Sharp's legacy looms large in contemporary ARSOF doctrine and practice. His key theme is that political power is not derived from the intrinsic qualities of those in positions of authority but from the consent of the governed, and thus the latter possess the moral and political authority to take it back. This theme can, and should, serve as the basis around which a resistance movement can be developed. Sharp assumes the set of universal human rights published in Article 21 of the United Nations' 1948 *Universal Declaration of Human Rights* (UN, 1948) and postulated that nonviolent resistance and its' concomitant

tactics are a tactically effective and means to challenge government authority without sacrificing moral authority. The premise of nonviolent resistance remains that political power is not derived from the intrinsic qualities of those in positions of authority but rather is derived from the consent of the governed.

Unconventional warfare in cyberspace may be the future of Special Warfare (Knapp, 2012; Eidman & Green, 2014) and, if so a better understanding of not only cyberspace but also its unique ecology is required (Maxwell, 2017). An understanding of human factors is arguably more critical in irregular warfare than in conventional warfare; but in great power conflict the lines are further blurred and thus SOF must comprehend and ultimately exploit the common behavioral and social dynamics to their extremes. This comprehension takes on existential significance when they involve a resistance movement weighing trade-offs between reliability and flexibility, a strategic choice whether to embrace violence or nonviolence, or an individual's judgments about whether to trust an ideology, a social contact, or a charismatic leader.

Understanding a population's support or rejection of such movements requires understanding of a broad set of political, economic, and social factors, and often requires an understanding of how individuals respond to oppression, violence, or terrorism (Bos et al., 2013). This nuance at the intersection of intranational and international conflict is where SOF should focus their organization, training, and equipping in order to deliberately develop a capacity (USASOC, 2015) that their forbearers in the SOE and OSS had to develop under fire.

References

Barry, (2011). Sound of Post-Soviet Protest: Claps and Beeps. New York Times Online. Retrieved from
http://www.nytimes.com/2011/07/15/world/europe/15belarus.html?pagewanted=all

Bos, N.D., Spitaletta, J.A., Molnar, A.R., Tinker, J.M., & LeNoir, J.D. (2013). *Human Factors Considerations of Undergrounds in Insurgencies, 2nd Ed*. Alexandria, VA: Alexandria, VA: US Army Publications Directorate.

Carlin, J. P., & Graff, G. M. (2018). *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. Hachette UK.

Chalou, G. C. (Ed.). (1995). *The Secret War: The Office of Strategic Services in World War II*. DIANE Publishing.

Crossett, C. (Ed) (2012). *Casebook on Insurgency and Revolutionary Warfare Volume II: 1962-2009*. Alexandria, VA: US Army Publications Directorate.

Delistraty, C. (2018). When Wearing a Graphic T-Shirt is a Revolutionary Act. Garage. Retrieved from
https://garage.vice.com/en_us/article/zmgmd4/graphic-t-shirt-revolutions.

Eidman, C.R. & Green, G.S. (2014). Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare (Unpublished Master's thesis. Naval Postgraduate School, Monterrey, CA.

Foot, M. R. D. (2004). *SOE in France: An account of the work of the British Special Operations Executive in France 1940-1944*. Routledge.

Kleinberg, J. (2008). The Convergence of Social and Technological Networks. *Communications of the ACM*. 53 (11), 66-72.

Knapp, E.D. (2012). Unconventional Warfare in Cyberspace (Unpublished master's thesis). U.S. Army War College, Carlisle Barracks, PA.

Kraemer, R., Whiteman, G., & Banerjee, B. (2013). Conflict and astroturfing in Niyamgiri: The importance of national advocacy networks in anti-corporate social movements. Organization Studies, 34(5-6), 823-852.

Maxwell, David S. (2017). The Cyber Underground-Resistance to Active Measures and Propaganda: "The Disruptors"-Motto: "Think for Yourself. Small Wars Journal. Retrieved from http://smallwarsjournal.com/jrnl/art/the-cyber-underground-–-resistance-to-active-measures-and-propaganda-"the-disruptors"-mot-0

Reno, W., & Matisek, J. (2018). A New Era of Insurgent Recruitment: Have 'New'Civil Wars changed the Dynamic?. *Civil Wars*, *20*(3), 358-378.

Satell, G. (2015). How social movements change minds. *Harvard Business Review*. Retrieved from https://hbr.org/2015/07/how-social-movements-change-minds

Shao, C., Ciampaglia, G. L., Varol, O., Yang, K. C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature communications*, *9*(1), 4787.

Spitaletta, J.A. (Ed) (2016). *Bio-Psycho-Social Applications to Cognitive Engagement*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

Stella, M., Ferrara, E., & De Domenico, M. (2018). Bots increase exposure to negative and inflammatory content in online social systems. *Proceedings of the National Academy of Sciences*, *115*(49), 12435-12440.

United Nations (1948). *Universal Declaration of Human Rights*. Retrieved from https://www.un.org/en/universal-declaration-human-rights/

United States Army Special Operations Command. (2015). SOF Support to Political Warfare (White Paper 10 March 2015). Retrieved from http://maxoki161.blogspot.com/2015/03/sof-support-to-political-warfare-white.html

Chapter 4. Nonviolent Resistance and Expanding the Unconventional Warfare Toolkit

MAJ Robert McBride and MAJ Thomas Doherty, United States Army Special Operations Command[7]

The Joint Force is challenged to address adversarial actions within the competition space, as doing so may lead to escalation and damage to essential cooperative ties. Army Special Operations Forces (ARSOF) face these same challenges as traditional methods of Unconventional Warfare (UW), in which an insurgency is trained to disrupt, coerce, or overthrow a regime, may be too provocative. Support to a violent insurgency may escalate to greater conflict, result in substantial deaths leading to retribution and destruction of property that complicates reconstruction and stability efforts, or subvert other US diplomatic efforts in a region. ARSOF thus must find ways to achieve the same ends of UW, yet limit escalation to make conducting this mission more palatable if deemed necessary by policymakers. A possible approach that meets this criteria is through the use of strategic nonviolence (SNV).

SNV movements have successful track records of disrupting, coercing, or overthrowing regimes with examples on virtually every continent and amidst a wide variety of cultures. This paper seeks to answer how nonviolent movements work through analysis on the role of power and legitimacy in governance, the dynamics of SNV resistance, and how nonviolent resistance operates in the presence of a radical flank. Historical case studies are examined which demonstrate both the potency of nonviolent resistance, how a movement can be successfully enabled by external actors either covertly or overtly, and how a radical flank could be to the benefit or detriment of a movement.

Many nonviolent resistance movements coexist with violent resistance movements. ARSOF can also enhance the ability of the United States Government (USG) to simultaneously utilize coordinated violent and nonviolent resistance movements in the same theater or country. By doing this, nonviolent resistance could be coupled with violent resistance to form a hybrid warfare campaign. Already proven as a viable strategy, the USG can pair nonviolent resistance movements with violent resistance movements using the violent resistance movement as a positive radical flank to the nonviolent movement.

Because SNV movements can achieve the ends of UW yet remain below the threshold for armed conflict, and because ARSOF capabilities – particularly those within Civil Affairs (CA) and Psychological Operations (PO) – are uniquely suited to support SNV resistance, the authors contends that enabling SNV movements can be a plausible yet nontraditional approach to conducting UW in the competition space.

Theoretical Basis of Strategic Nonviolent Resistance

Prior to reviewing the processes of nonviolent resistance, it is first important to clarify the difference between *principled nonviolence* and *strategic nonviolence*. The difference between these two terms is

---

significant as it helps to quiet any preconceived notions on the effectiveness of nonviolent resistance (particularly in military circles), and highlights that this method has perhaps greater potential in terms of mobilization of a society at large than traditional violent methods. The basic difference between the terms is based on why one would choose to resist nonviolently. Maria Stephan and Erica Chenoweth, two leading researchers on nonviolent action, define SNV as a "civilian-based method used to wage conflict through social, psychological, economic, and political means without the threat or use of violence."[8] Principled nonviolence is tied to an ideological position, usually derived from a religious or ethical basis in which the practitioner could normally be viewed as a pacifist. SNV on the other hand, is tied not to ideology but to pragmatism. Whether deemed by the practitioner to be more realistic due to the resources on hand, or simply the belief that nonviolent methods will be more effective, one does not have to ascribe to religious beliefs to participate in resistance. Thus, the potential for broad-based mobilization for mass resistance from the populace is greater. Gender is not a discriminating factor, nor is age. Female or male, old or young, theist or atheist – none are inherently prohibited from participating. What is "strategic" about nonviolent resistance is that it can be tailored and targeted in specific ways to achieve specific effects within a society, just as a traditional violent insurgency.

The underlying assumption of why SNV works in disrupting, coercing, or overthrowing a regime is fundamentally based on a view of power relations – that a ruler's power, even in authoritarian states, is at least partially dependent upon the consent and cooperation of the ruled. Power cannot be defined solely by *structure* or simply a force that compels someone to do something, but also by *agency* or human valuation and decisions. There is a mix of the two depending upon the context of governance and underlying obedience patterns. A SNV movement seeks to shift the relative power distribution from structure to agency – in some cases "to awaken agency" and shift obedience patterns from the regime to the SNV movement.

Gene Sharp, a preeminent scholar of nonviolence, described two models of power relationships in society – monolithic and pluralistic.[9] The monolithic model describes power as being centered at the top of a large, unchanging power structure, with the people below dependent upon the support and decisions of the ruler. However, a more useful viewpoint on power from the standpoint of one who seeks to enable resistance in a society is the pluralistic model. Under this model, power is not held in a solid manner at the top but in a fragile manner residing amongst the people.[10] Indeed, the people encompass the institutions which perform the mechanisms that enable a society to operate – police, judiciary, military, industry, businesses, schools, religious organizations, media, etc. These institutions are called "pillars of support" and can be both internal and external to the state. The ruler thus only exercises power in a manner in which these pillars provide resources to support the continuation of the regime – ultimately the manner in which the people provide either their tacit or explicit *consent*.

Thus, simply withdrawing obedience from these key institutions disrupts the mechanisms that enable a society to function without the use of violence. Withdrawn obedience affects the effectiveness of

---

[8] Maria J. Stephan and Erica Chenoweth, "Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict," *International Security* 33, no. 1 (Summer, 2008): 7–44.

[9] Robert Helvey, *On Strategic Nonviolent Conflict* (Boston: The Albert Einstein Institution, 2004), 2.

[10] Ibid., 4.

governance, which in turn reduces regime legitimacy (or its right to rule). <u>The key to this logic is that disobedience must be on a large scale in order to have an effect, or at least concentrated in strategic areas in which a regime is highly dependent.</u> Finding these areas is the work of contextual understanding of the *dependence relationships* within a society. Of course, state power is still relevant as some states exercise significant societal control practices or have historically imbedded institutions that affect obedience patterns. Yet, dependency relationships still exist in even the most authoritarian of states which provide resistance opportunities, even if primarily at the local level.

As in other types of warfare, SNV has strategic, operational, and tactical tenets. The overall *strategic* goal of a NV resistance movement is to shift obedience patterns, causing a crisis of legitimacy in governance rooted in decreasing effectiveness, which leads to a self-reinforcing cycle and ideally further mobilization against a regime. The end result of this strategy is to disrupt, coerce, or overthrow the regime. The *operational* objectives are to target the regime's pillars of support while strengthening the movement's pillars. SNV movements exploit cracks within an opponent's pillars that are due to grievances or rivalries, and identify points of least loyalty in an effort to shift obedience patterns.[11] Each party to the conflict – both the nonviolent movement and the regime – has pillars of support at its disposal. Within nonviolent movements, initial pillars of support may be labor unions, academia, professional organizations, certain religious groups, human/women/minority rights organizations, non-governmental organizations (NGOs), etc. External pillars could be friendly governments providing diplomatic support or economic sanctions, international governmental organizations (IGOs), etc.

At the *tactical* level, there are hundreds of different methods in which to employ nonviolent resistance. They can be either acts of <u>omission</u> – refraining from doing what one would typically do – or acts of <u>commission</u> – engaging in acts, both legal and illegal, in which one would not normally partake.[12] Sharp catalogued 198 different methods of nonviolent action and classified them into three categories: nonviolent *protest and persuasion*, *noncooperation*, and *intervention*.[13] These methods are essentially nontraditional forms of *sabotage* and *subversion.*

In employing SNV, considerations must be made to maximize mobilization of the populace, but also sustain the resilience of a movement throughout a campaign. All forms of nonviolent resistance carry some risk of repression or punitive response from the regime. Some nonviolent action could lead to being fired, imprisoned, "disappeared," or even executed. While significant repression can certainly stifle an emerging movement, it can also benefit a movement due to a change in power relationships. Sharp describes this process as political jiu-jitsu (henceforth referred to as *backfire*).

Backfire occurs when negative reactions to the opponent's violent repression against nonviolent resisters are turned to operate politically against the opponents, weakening their power position and strengthening that of the nonviolent resisters. This process only operates *when violent repression is met with continued nonviolent defiance*, as only then is the repression seen in the worst possible light

---

[11] Hardy Merriman, "Theory and Dynamics of Nonviolent Action," in Maria J. Stephan ed. *Civilian Jihad: Nonviolent Struggle, Democratization and Governance in the Middle East* (New York: Palgrave Macmillan, 2009): 21.

[12] Joshua Ammons and Christopher Coyne, "Gene Sharp: The 'Clausewitz of Nonviolent Warfare,'" *The Independent Review* 23, no. 1 (Summer, 2018): 151.

[13] Gene Sharp categorized these methods and provided historical examples in his seminal work, *The Politics of Nonviolent Action* (3 Volumes) Boston: Porter Sargent Publishers, 1973.

by outside parties.[14] Thus, adhering to nonviolent discipline by all resisters is key to success. The effect of backfire may result in further mobilization of the populace, international condemnation of the regime, and even disobedience or defections by members of the regime's security forces.[15] Backfire can be essential to the success of SNV should the opportunity present itself; however it should not be depended upon. A movement should minimize the risk of repression by anticipating regime reactions towards resistance and varying tactical methods between *dispersion* and *concentration* in order to sustain the resilience of the movement. Chenoweth defines the essential tasks of successful SNV movements as: develop an alternate vision of the future with widespread appeal, maximize diverse participation, provoke defections, minimize risk of repression, shift between methods of concentration and methods of dispersion, and anticipate to wage a multi-year campaign.[16] ARSOF is particularly suited to enable these tasks.

External Support to Strategic Nonviolent Movements—"Solidarity" and "Otpor"

The Polish "Solidarity" Movement provides a great example of nonviolent noncooperation methods, how resistance can be mobilized, and the role of external actors in supporting a movement (which could be of particular interest to ARSOF). In August 1980, a nonviolent resistance movement began as a series of strikes in the Lenin shipyards in Gdansk. After a few weeks, the strikes encompassed nearly 750,000 workers across many factories, which proved devastating to the Communist regime that was already struggling economically.[17] Poland was highly industrialized and thus the regime was highly dependent upon the continued obedience from the workers. As this pillar of support shifted, the regime's power was severely lessened. The workers' withdrawn consent created a political opportunity for negotiations with the regime that thus far had never existed. These negotiations resulted in the first independent labor union within a Communist bloc country, later named Solidarity.

Solidarity's success in achieving concessions soon spread to intellectuals, professionals, students, farmers, and other groups within Polish society who all called for independent organizations separate from the state. Their calls challenged the very framework of the Polish Communist system. Even though the movement was sidelined temporarily under martial law in 1981, it survived – with significant support from external actors such as the US – and returned in full force in 1988 when additional political opportunities emerged. The Central Intelligence Agency (CIA) under the Reagan administration supported the underground Solidarity movement under National Security Decision Directive 32 for many years in the form of finances, smuggling in printing presses, copiers, fax machines, and other materials for the underground to publicize and continue mobilization around Solidarity's cause.[18]

Mikhail Gorbachev formally instituted the "do it your way" Sinatra Doctrine in 1988, effectively abandoning any violent Soviet repression akin Czechoslovakia in 1968 to crush rising dissent in

---

[14] Helvey, *On Strategic Nonviolent Conflict,* 150.

[15] Stephan and Chenoweth, "Why Civil Resistance Works," 10.

[16] Erica Chenoweth, "The Art and Science of Civil Resistance" *Thammasat Review* 18, no.1 (2015): 1–10.

[17] Maryjane Osa, "Solidarity and Contention: Networks of Polish Opposition," *Social Movements, Protest, and Contention* 18, (2003): 2.

[18] Robert Gates, *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War* (New York: Simon and Schuster, 1996), 450.

Poland.[19] With the abdication of the Soviet Union, the Polish Communist regime had lost its most essential pillar of support for continued existence. Due to Solidarity's enormous support, the government was forced to call for elections – the first official step towards establishing democracy in Poland. Solidarity's candidates swept 99 of 100 freely contested seats in the summer of 1989 and Lech Walesa, the leader of the Solidarity movement, was elected President of Poland in 1990.[20] The use of SNV methods, effective societal mobilization, external support, and political opportunities both created by and granted to the movement cemented Poland's transition from Communism to democracy.

A concrete example of enabling *backfire* on regime actions also occurred in the US's support to Solidarity. In October 1984, Father Jerzy Popieluszko, who was Solidarity's official Chaplain and a highly popular priest, was beaten to death by Polish security services. The CIA subsequently provided Solidarity with 40,000 postcards for distribution that bore the photograph and sermons of the priest. The purpose of the messaging was to enhance Father Popieluszko's status as a martyr, thereby promoting mobilization in support of Solidarity, and prevent the regime from orchestrating a convenient cover up. Public response to this campaign was enormous, with crowds in the hundreds of thousands assembling for services and to protest regime actions. Father Popieluszko's murder and the response from the Polish people was widely seen as a turning point for the movement after the martial law period.[21]

While there was covert support provided to Solidarity under the CIA, there was also overt support. Overt funding support occurred through NGOs such as the National Endowment for Democracy (NED).[22] Less than a decade after Solidarity, support to nonviolent activists emerged again under the Clinton administration. In its continued efforts to curb ethnic cleansing of Muslims by the Slobodan Milosevic regime in the Balkans, a periphery effort to NATO bombings in Bosnia and Kosovo emerged. Clinton used third-party, democracy-promoting NGOs like NED to channel aid to revolutionary causes. Specially appropriated Congressional funds aided grassroots, anti-Milosevic civil-society groups such as the student group "Otpor." Under these special appropriations, the NGOs shifted from traditional roles as election monitors, information clearinghouses, or mobilizers of international support against brutal behaviors of a regime, to financiers and trainers of nonviolent revolutionaries.[23] Another organization of this type, the International Republican Institute, asked Retired Army Colonel Robert Helvey, a student of Gene Sharp who trained Burmese activists in SNV from 1992–1998, to conduct training for the members of Otpor. The training sessions strategized on how to enable mass mobilization from a wide array of Serbian citizens (including defections), how to challenge the regime's "pillars of support,"

---

[19] George C. Herring, *The American Century and Beyond* (Oxford: Oxford University Press, 2008), 600.

[20] James Graham Wilson, *The Triumph of Improvisation* (Ithaca: Cornell University Press: 2014), 148.

[21] Nigel West, *The Third Secret: The CIA, Solidarity, and the KGB's Plot to Kill the Pope* (London: HarperCollinsPublishers, 2001): 205.

[22] David Lowe, "Idea to Reality: NED at 30," National Endowment for Democracy, accessed December 10, 2018. https://www.ned.org/about/history/

[23] Mark R. Beissinger, "Promoting Democracy: Is Exporting Revolution a Constructive Strategy?" *Dissent* 53, no. 1 (Winter, 2006): 19.

and how to avoid repression.[24] Otpor's efforts were ultimately successful in ousting Milosevic from power in 2000 after a contested election in what is now known as the Bulldozer Revolution.

Suitability of ARSOF Support to Strategic Nonviolent Movements

Recognizing their potency, it is important to explore the potential for an external actor to enable nonviolent movements. Through a crosswalk of current ARSOF capabilities coupled with the factors of successful nonviolent movements, we argue that ARSOF, and in particular CA and PO, are suitable actors within DOD to support these movements. Some examples of ARSOF capabilities that would enable the success of SNV movements are as follows: human network analysis to identify key influencers/brokers for mobilization; social network and behavioral trend analysis; media assessments and the identification of key communicators; strategic messaging/framing; target audience analysis and behavioral change methodology, training and resourcing of movements; enabling underground communications; overcoming censorship, etc.

The list of ARSOF contributions to enabling SNV movements is extensive, and it is first essential to understand conditions within a society that provide opportunities to a resistance movement and vulnerabilities to a regime. Examples of these conditions could be factions within a regime, income inequalities, socioethnic divides, etc. Elite divisions in particular are central to provoking defections from security forces for example. Through current human network analysis capabilities, CA can help identify these conditions in a society along with the critical institutions a society needs to function (or its pillars of support). Withdrawn support from these critical areas could amplify a crisis of governmental effectiveness that challenges regime legitimacy. Crises in turn create messaging and targeting opportunities for the movement in which PO can assist. PO can use strategic messaging to build awareness of these conditions to the wider society. They can use *framing methods* in which they identify the source of the problem, tie the problem to a structural issue emanating from the regime (essentially attributing blame) and finally invoke an active sense of agency (or discuss what can be done to change the status quo). Framing is essentially a pre-packaged message that articulates the reality of the audience.[25] For mobilization purposes, these frames should be amplified and extended beyond a local area to the extended population. The Gdansk shipyard in Poland extending their grievances to incorporate other factories during the initial stages of Solidarity is one example. Key brokers such as union leaders, etc that can bring different organizations together under a shared cause would be prime targets as they would enable macromobilization or bloc recruitment that goes beyond mere interpersonal ties.[26] In the course of an ongoing campaign, PO may also need to capitalize on *backfire* messaging in case of violent regime repression on nonviolent resisters.

Resourcing is also essential for success. Movements must get their message out yet avoid censorship or repression by the regime. ARSOF can provide key resources either covertly or overtly to support a movement such as laptops, printing capabilities, illustrators, power generators, fax machines, satellite phones, mobile phones, or campaign paraphernalia. Technical aid such as setting up radio stations and

---

[24] John Bacher, "Robert Helvey's Expert Political Defiance," *Peace Magazine* (April-June, 2003): 10.

[25] Osa, "Solidarity and Contention," 16.

[26] D.W. Lee, "Resistance Dynamics and Social Movement Theory: Conditions, Mechanisms, and Effects," *PRISM Security Studies Journal* 6, no. 3 (2016): 142.

websites could also be provided. If needed, media access can be amplified by increasing capacities of radio stations or other signals, as the Clinton administration did in giving Otpor a live voice in Serbia through the B-92 radio.[27] The goal, however, must be to enable resource generation and eventual self-dependency so the movement does not entirely depend upon external support. Overall, similar to ARSOF assuming the guerilla warfare mission from the OSS after WWII, ARSOF can also be DOD's arm for enabling nonviolent resistance which has traditionally been filled by the CIA or NGOs since the 1980s.

Conclusion: Radical Flank, Hybrid Warfare and Nonviolent Strategies

Like those earlier efforts, any consideration of SNV must include analysis of the *radical flank effect* – the effects a more extreme subgroup has on the acceptability of a generally more moderate group. Increasing attention has been paid to what are known as the positive and negative aspects of a radical flank. Some studies argue the success of some nonviolent movements – such as the Philippines 1986 People Power Revolution (PPR) – was aided by a coexisting violent group. Some scholars have argued that radical flanks allow nonviolent resistance movements to appear more reasonable or the better option. Haines studied the results of the radical flank effect upon the civil rights movement in the US and concluded that a radical flank produced a positive effect for the more moderate groups. [28] However, the benefits of having a radical flank remain contentious. Chenoweth and Kurt Schock have argued that there is no benefit to a coexisting radical flank.[29] Yet, their study also found no direct disadvantage.[30]

The hybrid nature of radical flanks coincides with the current mode of great power competition: a form of warfare consisting of two or more forms that are distinguishable to both the defender and the aggressor while actively engaged in combat, both of which are combined to achieve synergetic effects. A nonviolent resistance movement can be an integral part of hybrid warfare.

The US military has started to expound upon the need to fight in multiple warfighting domains at once. The US military currently refers to this concept as multi-domain operations. Currently, five warfighting domains constitute the multi-domain arena. One of these is the land domain. As discussed earlier, the DoD has focused primarily on how to dominate this warfighting domain by the use of violent force applied upon an enemy, forcing it to obey the will of the friendly combatant commander. Combatant Commanders use what is referred to as non-lethal targeting in a supporting role to violent force. In other words, the strategy is based upon the use of violence as opposed to nonviolence. However, this singular focus has left the use of nonviolent strategies underutilized.

---

[27] Maria J. Stephan, "Checklist for External Assistance to Nonviolent Movements," in *Is Authoritarianism Staging a Comeback?* ed. Mathew Burrows and Maria J. Stephan (Washington D.C.: Atlantic Council, 2015): 211–212.

[28] Courtney Lanston Dillard, "The Rhetorical Dimensions of Radical Flank Effects: Investigations into the Influence of Emerging Radical Voices on the Rhetoric of Long-standing Moderate organizations in Two Social Movements" (PhD diss., University of Texas, 2002), 28.

[29] Kurt Schock, "Radical Flank Effect (USIP/ICNC Webinar)," *International Center on Nonviolent Conflict*, Febuary 6, 2011. https://www.youtube.com/watch?v=O5bcwtijco8&t=328s

[30] Ibid.

Nonviolent resistance provides a methodology that the military can use to operate within a denied enemy territory. It can do this two ways: either by using a surrogate it trained externally from the targeted country or by using the nonviolent resistance movement to make the area into a semi-permissible area. In this way, the movement can again use the existing UW doctrine. Given their nonviolent nature, an advisory may not perceive the same level of threat from the US forces. There will also be less need to move large amounts of weapons which may allow the US to obtain permissions for establishing safe heavens and conducting cross-border operations from neighboring countries.

The process of using a nonviolent strategy can be useful in reducing the need for kinetic operations during post-conflict stabilization phases. Nonviolent strategies are most successful when they unite diverse groups. Additionally, the lack of physical threat posed to regime members by nonviolent methodologies tends to reduce post-conflict revenge killings.[31] The desire to leave democracies governing captured territory has been a constant in United States expeditions abroad. Nonviolent strategies are better at building democracies than violent strategies.[32] In that regard, SNV resistance movements are a feasible, suitable, and acceptable solution for ARSOF to employ in the competition space when traditional UW methods are deemed either too costly or inappropriate. Historical examples demonstrate that employing SNV is a plausible solution and ARSOF has the capabilities of enabling these movements. ARSOF should be able to give policymakers this option for UW if the conditions merit. In addition to a purely nonviolent strategy, the option of ARSOF to coordinate the efforts of a nonviolent resistance movement and a violent resistance movement provides an increased ability of policymakers to create a strategy that fits the local environment to achieve broader strategic goals.

---

[31] Chenoweth and Stephan, "Civil Resistance Works," 13.

[32] Suveyda Karakaya, "Globalization and Contentious Politics: A Comparative Analysis of Nonviolent and Violent Campaigns" *Conflict Management and Peace Science* 35, no. 4 (2018): 315–335. Butcher and Svensson "Manufacturing Dissent," 331. There is other literature available on the theory that NvRMs tend to cultivate democratic structures. For further information see the literature review.

Chapter 5. UW Countergovernance: Political Warfare in Great Power Competition

MAJ Jeffrey Uherka, United States Army Special Operations Command[33]

1st Special Forces Command (1st SFC) realigned in 2014 to integrate civil affairs (CA) and psychological operations (PO) into its command, posturing to create a division of labor of SOF capabilities while maintaining integrated overlap through central oversight. In an environment that employs Army Special Operations Forces (ARSOF), CA may enhance indigenous governance alongside special forces (SF) indigenous security building and PO capacity to influence indigenous behaviors. Thus, 1st SFC's 2014 redesign enables it to simultaneously operate across the political, economic, social, military, and informational environments. 1st SFC's ability to employ simultaneous capabilities across operational variables allows it to attack adversary forces and provide options to replace that adversary force while filling the power vacuum created from its degraded capabilities – the core of *countergovernance*. This article illustrates ways 1st SFC can wield the political and economic operational variables in conjunction with the military, informational, and social, in order to conduct countergovernance. It proceeds by engaging the emerging definitions for governance and countergovernance, and provides a case study of Iranian countergovernance.

Governance and Countergovernance

From 2009–2018 the Department of Defense (DOD) defined governance as a *state's* ability to formulate rules and processes to articulate interests, manage resources, and exercise power.[34] During this time, the DOD also defined ungoverned areas as locations where sub-state actors do not effectively govern.[35] These definitions of governance and ungoverned areas suggest that governance cannot effectively occur at the sub-state or non-state level and that organizations such as the Liberation Tigers of Tamil Eelam (LTTE) in Northern Sri Lanka in the 1990s or Hezbollah in Lebanon in the 1980s did not perform governance or performed governance ineffectively. These definitions of governance mislead military leaders to underestimate sub-state and non-state actors' ability to wield greater influence and authority than the state. Though the LTTE were barbarous in their tactics against the Sinhalese state, they were able to effectively govern the Tamil populations under their control – arguably better than the Sinhalese state.[36] Furthermore, since its inception in the early 1980s, Hezbollah has provided better governance to Shia enclaves than the state of Lebanon.[37] Acknowledging governance at the sub-state and non-state level is essential because if we fail to effectively analyze the relationship between our adversaries and those populations our adversaries influence, then we will likely fail in our strategy to employ political and economic factors against our adversaries.

---

[33] Author contact Information: jeffrey.uherka@socom.mil

[34] Joint Chiefs of Staff, *Counterinsurgency Operations,* JP 3-24, Washington, DC: Joint Chiefs of Staff, 2009, I–4.

[35] Ibid.

[36] Zachariah Cherian Mampilly**,** *Rebel Rulers: Insurgent Governance and Civilian Life During War***,** (London: Cornell University Press, 2011), 116–123.

[37] James B. Love, *Hezbollah: Social Services as a Source of Power* (Hurlburt Field: JSOU Press, 2010), 21–26.

Thus, in 2017 the 95th Civil Affairs Brigade (CA BDE) collaborated with Johns Hopkins University (JHU) to produce a definition of governance defined as "population control practices employed by power holders to gain and maintain authority and/or influence over a target populace and its resources within the human environment."[38] This definition of governance is more applicable to ARSOF because of its versatility at the tactical, operational, and strategic levels of war. Additionally, though the DOD's 2018 definition of governance has dropped the word "state," the DOD definition still combines "governance" with "government."[39] On the contrary, the 95th CA BDE and JHU definition acknowledges the separation of governance from government. In other words, government is the formal institutions which formulate and enforce the rules while governance is the informal, yet dynamic relationships between those who govern and the governed that may or may not embrace government institutions and responsibilities.[40] Thus, governance is universal and occurs where ever a group of humans gather whether that be the family, the tribe, the clan, the village, or the state.[41] In short, the JHU and 95th CA BDE definition recognizes that both sub-state and non-state actors (or anyone who wields political power) can perform governance.

In unconventional warfare (UW) or irregular warfare (IW), great power competitors wield the economic and political (governance) variables by, with, thru both sub-state and non-state actors. During the Cold War, Iran countered Lebanese governance immediately following the 1979 Iranian Revolution via its proxy Hezbollah. Since then, Russia countered Ukrainian governance in both Crimea and the Donbas in 2014 as a part of its hybrid warfare strategy. While those malign actors sought to undermine democratic governance, 1st SFC is also postured to wield the necessary countergovernance factors at the tactical and operational levels.

DOD directives and doctrine define the range of possible actions. For instance, DOD Directive 5100.01 directs the Army to establish a military government when occupying enemy territory.[42] In addition, DOD Directive 2000.13 identifies military government as a directed requirement for Civil Affairs Operations. [43] Yet CA forces who fall under Special Operations Command (SOCOM) like the 95th CA BDE also abide by an additional SOCOM Civil Military Engagement Directive that directs them to simultaneously partner with friendly networks, engage neutral networks, and counter threat networks."[44] Furthermore, DOD UW doctrine depicts CA's dual role to support instability (or to degrade

---

[38] S.D. Agan-Newton, C.S. Houfek, C.S, *Governance: Defining Governance for the Modern Conflict Environment*. Baltimore: Johns Hopkins University, 2017, 2.

[39] Joint Chiefs of Staff, *Counterinsurgency Operations,* JP 3-24, Washington, DC: Joint Chiefs of Staff, 2018, I-6.

[40] James N. Rosenau, "Governance, order, and change in world politics," in *Governance Without Government: Order and Change in World Politics,* ed. James N. Rosenau and Ernst-Otto Czempiel (Cambridge: Cambridge University Press, 1992), 4.

[41] Stefano, Ruzza, Anja Jakobi, and Charles Geisler, *Non-State Challenges in a Re-Ordered World: The Jackals of Westphalia* (New York: Routledge, 2016), 177-180.

[42] Department of the Army, *Civil Affairs Operations,* Field Manual 3-57, Washington, DC: Department of the Army, 2019, 1-2.

[43] Department of Defense, *Civil Affairs,* Directive 2000.13 (Washington, DC: Department of Defense, 2017) 1, 8, 10.

[44] Special Operations Command, *Civil Military Engagement Directive 525-38*, (MacDill Air Force Base, FL: US Special Operations Command, 2018), 3, 6.

and attack adversary regimes) while near simultaneously to stabilize (or to bolster, support, legitimize) friendly resistance forces.[45]

As a result, just as the 95th CA BDE and JHU revamped the definition of governance, they also concluded the need to summarize DOD guidance into a simple concept. Thus, countergovernance was defined as "activities in the human environment that intentionally undermine or compete with power holders' governance practices and their associated authority and influence."[46] In particular, countergovernance encompasses two categories, *negative governance* and *competing governance*. Negative governance focuses on degrading an adversary's governance activities, capabilities, and legitimacy. Furthermore, competing governance involves "two or more actors maintaining parallel governance structures, vying for recognition and legitimacy via governance activities."[47] The two concepts become complementary when an actor's negative governance allows friendly forces to gain time and space by putting the adversary on the defense. Competing governance then fills the political and economic power vacuums resulting from successful negative governance.

As a result, governance is a subordinate operation within stability – operational environments when an adversary is politically subdued. At the same time, countergovernance is a subordinate mission in operational environments where an adversarial governance structure wields influence and/or authority such as in counterinsurgency (COIN), counterterrorism (CT), irregular warfare (IW), and unconventional warfare (UW) environments.

US near-peer adversaries and great power competitors conduct countergovernance. For example, Russia conducted countergovernance in 2014 against Ukraine within the Donbas and Crimea as a subordinate operation to their hybrid warfare strategy. Russia's countergovernance employed Russian sponsored NGOs, Russian media, and Russian political proxies to perform both competing and negative governance against the Ukrainian government at the tactical and operational levels of wear. While that example has received significant analysis lately, Iran's conduct of countergovernance against Lebanon through Hezbollah warrants a revisit given its long-standing success.

Iranian Countergovernance

The Lebanese Civil War (1975–1990) amidst perpetual Muslim-Arab resistance against the creation of Israel in 1948 were factors which facilitated the creation of Hezbollah following the 1979 Iranian Revolution.[48] First, Lebanon's 1975–1990 civil war between the Christian-dominated government and the Palestinian Liberation Organization weakened the country politically and economically.[49] During this period, Lebanon's central government could not maintain the rule of law and implement policy

---

[45] Joint Chiefs of Staff, *Special Operations,* JP 3-05.01, Washington, DC: Joint Chiefs of Staff, 2015, III-21.

[46] S.D. Agan-Newton, C.S. Houfek, and J.R. Macris, *Countergovernance* (Baltimore: John Hopkins University, 2018), 1.

[47] Ibid, 3.

[48] James B. Love, *Hezbollah: Social Services as a Source of Power* (Hurlburt Field: JSOU Press, 2010), 11–14.

[49] Krista E. Wiegand**,** *Bombs and Ballots: Governance by Islamist Terrorist and Guerrilla Groups* (Burlington: Ashgate Publishing Company, 2010), 92; James B. Love, *Hezbollah: Social Services as a Source of Power* (Hurlburt Field: JSOU Press, 2010), 11.

across its entire territory creating gaps in governance.[50] These gaps signified Lebanon's inability to maintain a monopoly on the use of legitimate coercive force across the country.[51]

The permissive factors facilitating Hezbollah's influence and authority are especially evident within the three Shi'a enclaves: (1) Lebanon's northeastern Baalbek-Hermel governorate, (2) the southern Lebanese border region with Israeli, and (3) the southern suburbs of Beirut.[52] Muslims represented the majority of the Lebanese population after the arrival of the massive numbers of Sunni Palestinians following the PLO's ouster from Jordan after the failed Black September coup attempt. Shiites ranged between 29–40% but with a significant disparity in both health and utility services between Shi'a populations and other populations within Lebanon.[53] Shia representation in the Lebanese central government stemmed from a 1943 unwritten agreement (known as the National Pact) based on demographics at the time. The Pact allocated the Presidency to a Christian, the Prime Minister to a Sunni, and the Speaker of the Parliament to a Shia given each population's numbers at the time.[54] Furthermore, Article Twenty-Four of the Lebanese constitution distributed parliamentary seats equally between Christians and Muslims regardless of population estimates that from 1985 to the present day depict a Muslim majority.[55] Thus, both the Lebanese Constitution and the 1943 National Pact eventually under-represented Muslims in the central government due to immigration and the growing Shia populations. The weak Lebanese government combined with under-represented Shi'a populations to help establish the conditions for Hezbollah to fill the political, economic, and security power vacuums with the clear and consistent support of Iran. Over time, Hezbollah's effective implementation of countergovernance combined with its ability to evolve its strategy resulted in Hezbollah outperforming the Lebanese government.

With Iranian subsidies and direct military support, Hezbollah solved the weak security and the high unemployment rates within Shi'a enclaves by enlisting Shi'a males into Hezbollah's security branch. As the government collapsed in the civil war, Hezbollah's security apparatus quickly exceeded its weakened security capability, resulting in the Lebanese government conceding the legitimate use of force within Shi'a enclaves. This persisted during and after the civil war. In addition, Hezbollah's security forces gained national legitimacy through waging irregular warfare against the Israeli Army within the South Lebanese Shi'a enclave in 2006.[56] In essence, Hezbollah created a competing law enforcement capability across the three Shi'a enclaves and gained greater relative legitimacy than the Lebanese

---

[50] Ibid., 87–88.

[51] Max Weber, *Weber's Rationalism and Modern Society: New Translations on Politics, Bureaucracy, and Social Stratification*, trans. and ed. Tony Waters and Dagmar Waters (New York: Palgrave Books, 2015), 13.

[52] Krista E. Wiegand, *Bombs and Ballots: Governance by Islamist Terrorist and Guerrilla Groups*, (Burlington: Ashgate Publishing Company, 2010), 120.

[53] Judith Palmer Harik, *Hezbollah: The Changing Face of Terrorism* (London: I.B. Tauris & Co Ltd, 2004), 86–87; Krista E. Wiegand, *Bombs and Ballots: Governance by Islamist Terrorist and Guerrilla Groups* (Burlington: Ashgate Publishing Company, 2010), 119–120.

[54] United States Institute of Peace, "Lebanon's Confessionalism: Problems and Prospects," March 2008. https://web.archive.org/web/20090322103601/http://www.usip.org/pubs/usipeace_briefings/2006/0330_lebanon_confessionalism.html

[55] "The Lebanese Constitution," World Intellectual Property Organization, 1995, https://www.wipo.int/edocs/lexdocs/laws/en/lb/lb018en.pdf

[56] James B. Love, *Hezbollah: Social Services as a Source of Power* (Hurlburt Field: JSOU Press, 2010), 1, 15.

government by creating the perception that Hezbollah, not the Lebanese military, protected the populace in general.

Hezbollah's social branch consisting of "social work, education, and healthcare" also competes with the Lebanese government's social services.[57] For example, the education branch provides primary and secondary education within the Shi'a enclaves that has outperformed the Lebanese Department of Education's school system.[58] Lastly, Hezbollah manages contemporary hospitals that far exceed the capacity of Lebanese medical facilities within the Shi'a communities.[59] Thus, Hezbollah has established competing social services, and this establishment itself undermines the Lebanese government's legitimacy.

The organization has thus evolved its political countergovernance against the Lebanese government from negative governance to competing governance. For instance, Hezbollah conducted terrorist attacks that degraded the legitimacy of the Lebanese government throughout the 1980s. These attacks included the April 1983 car bomb at the American Embassy in Beirut, the October 1983 truck bombs that destroyed the US and French barracks, the November 1983 car bomb that destroyed the Israeli military headquarters in Tyre (Lebanon), as well as multiple kidnappings and murders of Lebanese and Western citizens in Lebanon.[60] Yet, at the end of the Lebanese Civil War, upon gaining substantial political and military power, Hezbollah made the pragmatic decision to transition from negative political governance to primarily competing political governance.[61] As an illustration, Hezbollah has participated in every parliamentary election since 1992, slowly gaining political momentum. For instance, in the alliance of March 8, 2009, the Hezbollah bloc won fifty-seven parliamentary seats (forty-five percent of the total seats in parliament). In short, Hezbollah transitioned from conducting both negative governance and competing governance in the 1980s to primarily competing governance strategy in the 1990s, allowing it to gain influence and authority at the expense of the central government. Hezbollah illustrates an example of how a non-state actor on behalf of a near-peer rival (Iran) can achieve influence and authority through a combined countergovernance and governance strategy.

Conclusion

In conclusion, US near peer rivals have weaponized the political and economic variables through countergovernance to achieve their objectives. 1st SFC's 2014 realignment offers the US military the capability to conduct countergovernance in a UW/IW environment through concurrent SOF effects across the operational variables. ARSOF countergovernance involves conducting negative governance mostly through the political, economic, and informational variables to degrade an adversary power

---

[57] Krista E. Wiegand, *Bombs and Ballots: Governance by Islamist Terrorist and Guerrilla Groups* (Burlington: Ashgate Publishing Company, 2010), 120.

[58] James B. Love, *Hezbollah: Social Services as a Source of Power* (Hurlburt Field: JSOU Press, 2010), 25; Krista E. Wiegand, *Bombs and Ballots: Governance by Islamist Terrorist and Guerrilla Groups* (Burlington: Ashgate Publishing Company, 2010), 120.

[59] Ibid.

[60] Judith Palmer Harik, *Hezbollah: The Changing Face of Terrorism,* (London: I.B. Tauris & Co Ltd, 2004), 36–37.

[61] Krista E. Wiegand, *Bombs and Ballots: Governance by Islamist Terrorist and Guerrilla Groups* (Burlington: Ashgate Publishing Company, 2010), 98.

holder's authority over a population. Competing governance follows negative governance by introducing an indigenous competing governance structure to fill the power vacuum and replace the adversary's influence over the population. Finally, according to Carl von Clausewitz, "War is a continuation of political intercourse . . . war does not change policy into something entirely different . . . The main lines along which military events progress, and to which they are restricted, are political lines that continue throughout the war into the subsequent peace."[62] Hence, countergovernance is a means to weaponize the political and economic operational variables – short of war.

---

[62] Carl von Clausewitz, *On War*, Edited and translated by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 605.

Chapter 6. Countering Electronic Warfare Undermatch in the European Area of Responsibility

CW4 Jeffrey Elwell, Special Forces, United States Army Special Operations Command[63]

Introduction

The purpose of this paper is to identify gaps in current US communications technologies with regards to Russian electronic warfare (EW) capabilities. Doing this will help to answer the following research question: In what ways must US Army Special Operations Forces (ARSOF) adapt to guarantee communications surety in competition with Russia? Advances in Russia's EW capabilities since 2004 have given it a technological advantage over the West, which has been focused mainly on counterterrorism and non-state actors since the end of the Cold War. Current US systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) are vulnerable to Russian EW and anti-satellite capabilities. With the return of great power competition, the potential for conflict between Russia and the West has increased across a wide spectrum of activities and locations. EW is an integral part of hybrid warfare that Russia wages in an aggressive campaign against its neighbors like Ukraine, Georgia, and the Baltic countries of Estonia, Lithuania, and Latvia. The long-term goals continue to be the reestablishment of Russian regional dominance and its role on the international stage. Russia has employed EW in the conflicts in Ukraine and Syria, as well as in Europe to destabilize NATO to that endstate. Also, Russia sells its advanced EW and A2AD technology to numerous other countries, thereby propagating this capability to other potential flashpoints as well.

ARSOF is a critical element of the US strategy to counter Russian aggression and must be able to operate within the contested communications space that any conflict with Russia will entail, be it irregular or conventional. Countering Russian overmatch requires ARSOF to incorporate emerging communications technology, to employ protective measures and tactics that combat and offset current Russian advantages, and to reassess how ARSOF conducts the warfighting function of mission command. Through adaptation in these necessary areas ARSOF can better guarantee communications surety in any future conflict with Russia.

Problem Background

From the end of the Cold War up until Russia's involvement in the Syrian Civil War in 2015, the United States enjoyed airspace dominance and a mostly uncontested electronic warfare environment as it engaged in conflict with non-state actors and less-developed adversaries such as Serbia in the 1990s and Iraq and Afghanistan in the early twenty-first century. During that time, US C4ISR systems became largely satellite-based due to a lack of threats in the electronic environment. These systems are now

---

dependent on satellite communications (SATCOM) or fiber-optic networks to enable information sharing and are a critical component of the Army's mission command system.

Mission command involves the exercise of authority and direction by a military commander to enable disciplined initiative and synchronize operations. As a warfighting function, mission command is a series of "related tasks and systems that develop and integrate those activities enabling a commander to balance the art of command and the science of control to integrate the other warfighting functions" such as movement and maneuver, fires, sustainment, intelligence, and protection.[64] Effectively controlling forces on a rapidly changing battlefield requires the collection and processing of large amounts of information, which is managed through the Army's mission command systems. These systems support a Commander's decision making and are used to conduct detailed planning, enhance communications, and improve situational awareness. C4ISR is the backbone on which the mission command systems ride; however, the inherent dependence on satellite communications has created a strategic vulnerability. US forces, and in particular ARSOF, have become accustomed to having connectivity in even the most austere environments, and commanders expect to receive considerable amounts of information from units in the field to enable timely and informed decisions. If SATCOM were denied, C4ISR systems would be significantly affected.

C4ISR is vulnerable to electronic warfare (EW), which is "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[65] EW is further broken down into the categories of electronic attack, electronic protection, and electronic warfare support. When employed offensively, as in electronic attack, EW can be used to deny adversaries the ability to communicate through radio, to detect incoming threats, or to protect their systems and networks; it involves all spectrums of the electronic environment utilized for C4ISR systems. The disruption of those systems with either the loss of SATCOM or through jamming would have a direct impact on the ability of US forces to execute mission command.

Russian Electronic Warfare

EW has long been a cornerstone of Russian military doctrine. Since 9/11, Russia has examined how the US waged the Global War on Terror and identified an overreliance on satellites for everything from communications to navigation to guiding precision munitions. Russia has endeavored to exploit US vulnerabilities in C4ISR through the development of advanced EW technologies along with a capability to shoot down or destroy US satellites and to jam SATCOM satellites. With their new EW capability, Russian forces can jam US radios and drones, pinpoint the locations of radio transmitters, and spoof the global positioning system (GPS). Russia currently enjoys an advantage because of its ability to place the current US tactical and theater communications architecture at risk.

---

[64] Headquarters, Department of the Army, ADRP 6-0 Mission Command (Washington DC: Government Printing Office, May 2012), 3-1.

[65] US Department of Defense, *DOD Dictionary of Military and Associated Terms* (Washington DC: Government Printing Office, 2018), 78.

Russian Aggression

In the second decade of the twenty-first century, Russia has emerged as a revisionist power bent on changing the US-led world order following the end of the Cold War. Russia attempts to upset that balance of power by bringing Russia and other countries such as China, India, and Brazil to great-power status to challenge US hegemony.[66] Putin claims that NATO's expansion into Eastern Europe is aggressive and a direct threat to Russian national security. In reality, Russia is an aggressive imperial state that seeks to retain the ability to dominate former Soviet republics like the Republic of Georgia and Ukraine to maintain a strategic position against NATO and the West.

To counter NATO expansion into countries such as Ukraine and Georgia, Russia employs a combination of efforts including both armed conflict, and those short of armed conflict to confuse observers and make a coordinated response by the international community difficult. Russia used this strategy, sometimes referred to as "hybrid warfare," during the annexation of Crimea and in support of pro-Russian separatists fighting in Eastern Ukraine. According to Nolan Peterson, "Russia's modern hybrid warfare doctrine combines the use of conventional military force with other non-kinetic means such as cyber-attacks and propaganda to sow chaos and confusion among the enemy—both on the battlefield and deep behind the front lines."[67] EW is an integral part of hybrid warfare, and Russia employs it in eastern Ukraine to support pro-Russian separatists and in Syria, where Russian forces have supported Bashar al-Assad's regime in the Syrian Civil War since 2015. Nor is Russia's use of EW exclusive to conflict areas. During NATO Exercise Trident Juncture in Norway in November 2018, Russia jammed GPS signals, affecting the navigation of exercise participants and civilians alike.[68]

The US strategy to counter Russian aggression involves a combination of deterrence and active measures to demonstrate to Russia that the US will not tolerate imperialist aggression. Proactive steps to demonstrate US resolve include military engagement and security cooperation to ensure that US allies and partnered nations are resilient and can counter Russian aggression. Known as irregular warfare (IW), this military activity differs from a traditional state-on-state conflict involving massed armies and instead encompasses counterinsurgency, unconventional warfare, foreign internal defense, counterterrorism, and stability operations.[69] IW may be conducted unilaterally by US forces, but more likely it is a multilateral effort and may involve surrogates or proxies as was seen in the Cold War. IW is a means for the US to compete with other nuclear-equipped great powers such as Russia and China in a way that is less likely to escalate into a global war.

---

[66] The Kremlin, *Russian National Security Strategy* (Moscow: Ministry of Foreign Affairs of the Russian Federation, Dec 2015), accessed January 6, 2019, http://www.mid.ru/en/search?p_p_id=3&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_3_struts_action=%2Fsearch%2Fsearch#, 4-25.

[67] Nolan Peterson, "A Lesson for NATO from Ukraine," *The Daily Signal* (April 06, 2018), accessed September 15, 2018, https://www.dailysignal.com/2018/04/06/lesson-nato-ukraine-war-russia-smartphones-might-safest-way-communicate/.

[68] Emily Birnbaum, "NATO: Russia jammed GPS signals during exercise with US troops," The Hill (November 14, 2018), accessed January 25, 2019, https://thehill.com/policy/defense/416625-nato-russia-jammed-gps-signals-during-exercise-with-us-troops.

[69] US Department of Defense, *DoD Directive 3000.07: Irregular Warfare* (Washington DC: Government Printing Office, May 2017).

Unlike US conventional forces, ARSOF is specially trained to conduct IW as a vital component in the strategy to counter Russian aggression. ARSOF supports IW through the conduct of special warfare, which is "an umbrella term that represents special operations forces conducting combinations of unconventional warfare, foreign internal defense, and/or counterinsurgency through and with indigenous forces or personnel in politically sensitive and/or hostile environments."[70] ARSOF are already deployed to Syria, Ukraine, and Eastern European countries conducting special warfare to counter Russian hybrid warfare and help to create a deterrence to Russian aggression.

Many academics believe that a war between the U.S./NATO and Russia is highly unlikely because the stakes for Vladimir Putin are too high from a domestic standpoint, and because of the potential for escalation to a nuclear exchange. As a result, the conflict between Russia and the West will likely be through IW. In this environment, the threat of Russian EW is still significant as ARSOF may come into contact with Russian-backed proxies or surrogate forces.

Despite the unlikelihood of a conventional war between Russia and the West, Russia's continuing aggression against its neighbors and NATO means that war is still a genuine possibility as a miscalculation on the part of Russia or NATO could cause an isolated incident to spiral out of control. Any conventional fight between the US and Russia would be a worst-case scenario. The role of ARSOF in this type of conflict would be in support of the greater conventional fight, providing support to resistance and enabling joint fires to degrade Russian A2AD. To perform those missions, ARSOF must operate in denied areas for extended periods in the highly-contested EW environment where Russian security forces will have the ability to jam communications or geo-locate ARSOF teams. To survive, ARSOF require communications systems that have a low probability of intercept and detection by current and future Russian EW capabilities.

Closing the Gaps

The evolving threat posed by Russia's EW capability requires ARSOF to continually adapt to provide SOF effects in the event of a conflict. To do this ARSOF must modernize its current communications system, which has become static and inflexible. In addition to technological solutions, ARSOF must make electronic protection a priority in the concept of how they execute mission command against a near-peer threat.

Current technology offers a solution to enable ARSOF to at least partially overcome the Russian EW threat. ARSOF radio systems are hardware-based, purpose-built and optimized for size, performance, weight, and power; however, they are expensive and time-consuming to design and produce, and cannot be easily modified. Software-defined radios, on the other hand, can receive upgrades by changing the software load, enabling the receiver to run multiple waveforms or accept new ones. This feature would enable ARSOF to acquire new radio technology as it emerges without having to buy additional equipment. In addition to software-defined radios, two-channel radios allow one receiver to transmit and receive voice communications and data simultaneously, allowing users to carry one radio rather than two. Combining *two-channel radios with software-defined radio technology* provides a

---

[70] Headquarters, Department of the Army, *ADP 3-05: Special Operations* (Washington DC: Government Printing Office, January 2018), 7.

programmable, easily upgradeable system that allows operators to monitor voice, text, and video simultaneously while having the ability to adapt to the evolving EW threat.

Mesh networks offer a broader systemic solution to ARSOF that was previously provided by SATCOM-based systems like the FBCB2. Unlike conventional Wi-Fi that has a wired connection between access points and switches or a wired LAN, a wireless mesh network provides communication between network nodes, and between nodes and clients all over radio instead of cable. Because information passes point-to-point, the radio can be configured to use the optimal waveform for the environment, reducing power output because the receiver only needs to transmit enough power to communicate with another network node. By reducing power output, the individual node is less susceptible to being located by the enemy via direction finding. The networks are also adaptable in the event one node goes down, reworking itself to compensate via new nodes. When used in conjunction with software-defined two-channel radios, mesh networks provide considerable flexibility to ARSOF teams and make them less vulnerable to Russian EW.

The loss of SATCOM, as well as if Russia cuts the undersea cables connecting North America with Europe, would cause a considerable issue for long-haul data transfer via network communication with stateside-based servers. Existing technology such as microwave, is an option making up about 35% of terrestrial communications due to its considerable bandwidth. However, it requires a series of relays to transmit over long distances. To transmit over the horizon, a technique known as troposcatter can be employed to bounce the signal off of the atmosphere—similar to HF, which is picked up by a receiver at the other end. However, when using troposcatter, there is the potential for the loss of some signal. Another option for data transfer is light fidelity (or Li-Fi) technology that uses visible light to transfer data. Like microwave, Li-Fi is capable of transporting large amounts of data. One drawback is its reliance on line-of-sight requiring relays to continue the signal over the horizon. Another limitation to Li-Fi technology is that it can be disrupted by smoke or particulates in the air, both of which occur during combat operations. Neither of the proffered alternatives provide the same performance or reliability of SATCOM; however, they can provide work-around alternatives for long-haul data transfer in the event SATCOM or the undersea cable network is denied.

Technical solutions offer some counters to the threat posed by Russian EW. Yet, the application of safe communications practices is also critical. To be able to operate in a communications-degraded environment requires ARSOF elements and leaders to understand the threat and train for it. With a loss of SATCOM, ARSOF would be reliant on high-frequency (HF) radios for over-the-horizon communications, which are vulnerable to both Russian direction-finding and jamming. Reducing their electronic signature requires ARSOF teams to be proactive in protecting the security of their communications, including everything from varying communications transmission times, to using terrain masking, to transmitting a safe distance from their operational locations. Emphasis on EW protection must be incorporated into initial acquisition training of ARSOF communicators during their training pipelines, as well as during collective training and exercises at the unit level.

Lastly, ARSOF must also overcome an institutional culture that has developed fighting counterinsurgencies in which commanders have grown too reliant on constant communication with subordinate elements. A communications-degraded environment will force elements to communicate less to improve survivability even as Russian EW may disrupt components of C4ISR. Video teleconference and portal access would become the exception, not the norm. Adapting to this

environment requires that ARSOF relook the concept of mission command, including methods of control used during the Cold War such as detailed pre-mission planning that is compartmented, the use of communications windows and fixed formats with limited characters for reporting, and pushing intelligence updates and taskings down to tactical elements once daily. Commanders will need to once again become comfortable trusting their subordinate leaders to operate within the scope of their intent and mission orders, and not hearing from a subordinate element for days or weeks in some cases. Returning to ARSOF roots in special warfare will help bring about institutional change in mission command that incorporates the threat of EW into training events and exercises, as well as operational planning and execution.

Conclusion

The threat posed by Russian EW and anti-satellite capabilities to US and NATO communications represents a strategic vulnerability—namely, overreliance on SATCOM as the backbone for communications and mission command systems. With the ever-increasing tension due to aggressive rhetoric from Moscow, the likelihood that the US and Russia will become engaged in conflict grows daily. A conventional war between the two nuclear powers is unlikely, so it is more likely that conflict will be in the form of irregular warfare in regions where there is instability and where one or both countries have a strategic interest.

ARSOF must be prepared to conduct the full spectrum of special operations in such highly-contested communications environments. To overcome Russia's current advantage in EW, ARSOF must adapt to guarantee communications surety requiring a combination of modernizing its current capabilities, employing right tactics, and changing the paradigm of mission command to contend with the threat faced in conflict with a near-peer adversary.

Chapter 7. Becoming Peerless in a Peer-to-Peer Competition

Dr. David C. Walton, National Defense University[71]

As National Security professionals we rely on some foundational guidance to direct our efforts. These last 18-24 months have seen some movement in this regards. There seems to be no shortage of criticism of the process of establishing strategic guidance but at least we have the luxury of a system. In 2018 we published the National Defense Strategy. It's a fairly tight 11-pages or so of the now former Secretary's thoughts about what he thinks is important for the enterprise to focus on. It talks of expanding the competitive space with three main lines of effort – Lethality and Readiness – Allies and Partners – and Departmental Reform. All of this with the underlying mantra of never sequester. It provides 11 National Defense objectives in priority order. It gives us license to be creative in our approaches, to make sustained investments, and be disciplined in our execution. But what it doesn't do is actually give us a strategy. I agree with my colleague Dr. Greg Foster, who in his excellent Defense One article, argues what this National Defense Strategy did was give us an <u>ideology</u> rather than a <u>strategy</u>. At its core, what the NDS did was to officially announce that we, the US Government, now recognize that we must return to a cold war methodology for our continued security. What it did was allow us to admit that our once vanquished peers have returned, some new peers are emerging, and almost none of the old problems…the problems that have been consuming us for the last nearly 20 years have been solved. That's a pretty tough realization. The good news is that we've been here before.

In 2001 Linton Wells penned a memo as part of the Pentagon's prep for the QDR. We should consider what was happening in 2001. We had already "won" the First Cold War, we had showed the prowess of American military might with a smashing victory in Desert Storm, and we were riding American economic dominance across the globe. In short, we had the world by the short hairs with no real competitors except ourselves. An enviable strategic position no doubt. Wells wrote his memo in April 2001. Just 5 months later his analysis on the, and I quote "unpredictable nature of great power relations" proved to be especially applicable. So maybe in this light the fact that our masters have given us in the 2018 NDS an ideology rather than a strategy is better. It is inherently more flexible. It allows us as practitioners some freedom of maneuver. It gives our adversaries…our peers…more to consider.

We, as a strategic enterprise, are busy. Everything is a priority so nothing is prioritized. Nobody has enough time, enough money, or enough people and there seems no let-up in sight. Despite this condition nobody seems to want to say no. Nobody wants to specialize. Because if you specialize then you by default admit that you can't or won't do something and if you do THAT…well then you start to show institutional weakness. If that other entity says they can do it and your entity says that it wants to focus on their core mission…well now that other entity just might get your money or your authorities

---

We need to learn to say no, but not for the sake of not doing whatever is asked of us, rather for the sake of doing what we are supposed to be doing.

Simply put, we took our eye off of the biggest threats in favor of the closest threats. It's not really a matter of blame, and this certainly isn't a DoD-exclusive issue, but this is something that needs to be acknowledged and managed. China's Belt and Road Initiative is proving to be the Trojan horse of injecting suffocating control and exploitation under the guise of development and cooperation. And Russia, who many dismissed as drunken oligarchs and failed authoritarians, has been building a resume of Irregular Warfare victories that shows that while we declared victory at the end of the 4th Quarter of the Cold War, they simply went on playing the game while we were in the locker rooms of the Global War on Terror. While not technically peers, Iran uses it terror proxies to inflict the death of a thousand cuts and North Korea is as unstable and dangerous as ever. Nobody is going to wait for us the catch our breath.

As Linton Wells so poignantly demonstrated, we would be foolish to assume that we know how this will all play out. We would be wise to continue to prepare for the worst…for devastating warfare and demoralizing strife. But we should also think about how to manage catastrophic success. What can and should we do if we get our way? What systems and processes can we build now so that we can maximize the gains that we do make? This acknowledgement that we don't know what is next is a prime argument for the value of education. We train for the known and we educate for the unknown. If there was ever a time to embrace the unknown it is now and educating ourselves, that is the acquisition of knowledge for future application, the enlightenment of oneself, well…I can think of no better time.

So, Great Power Competition is back. But the weird threats still persist. And the unknowns remain unknown. Exactly how are we supposed to develop a unifying strategy to deal with everything…capital E everything? Again, everything is a priority so nothing is a priority. Well, we are professionals so let's dig into our professional toolkit. Let's go back to our National Defense *Ideology*. Does this document give us actionable and practical guidance on how we can become peerless? I guess that all depends on where in the spectrum of 'doing stuff' you reside within the enterprise. But what the return to great power competition and the recognition that we now have peers that need to be managed does do is at the very least gives us a real thing to defeat or at least focus on. In much the same way that we struggle to defeat terrorism, or insurgency, or bring security to under-governed regions with civil unrest for the simple reason they often exist more in ideology than in presence, a peer is much easier to quantify. This is definitely tongue-in-cheek, but in the immortal words of Arnold Schwarzenegger, if we can make it bleed we can kill it. The NDS ideology gives us license to do so.

So how do we actually compete? How do we regain the advantage? Or least how do we at least stop being disadvantaged? In this regard the NDS gives us specific guidance. We become strategically predictable and operationally unpredictable. This is actually really good for us, the executioners of the NDS. As noted by a Soviet author of Cold War vintage: "A serious problem in planning against American doctrine is that the Americans do not read their manuals, nor do they feel any obligation to follow their doctrine." So, our NDS ideology of lethality and readiness, partners and allies, and departmental reform is actually pretty liberating. Lots of room in there for chaos. I would encourage you to read Taleb's *Anti-Fragile: Things That Gain From Disorder*. I think you'll be surprised to learn just how well suited the American fighting force is for a chaotic fight…or as the NDS puts it…operational unpredictability.

One of the concepts that the DoD Education enterprise has been wrestling with is "intellectual overmatch". We have a growing obsession with rebuilding the "stagnated PME system" and regaining the cerebral initiative. In my little corner of the world we approached this problem set first with an inventory. If I'm supposed to have more than you then I better find out what you have. So we are studying what our peers and adversaries teach. Academics are vain by nature and love to publish all of their good ideas, in many cases we are required to do so. It is surprisingly easy to find out what everybody teaches and we have built a fairly comprehensive understanding of what we are dealing with. I'm confident that what we teach and how we teach it is better than our peers, but the synthesis and evaluation continues. As a strategic enterprise we need to all be conducting this inventory. Your peer-adversaries likely won't publish as prolifically as mine, but the information is out there. Establish your analytical frameworks, set your terms and definitions, review all of the threat data, and listen to the analysts. Figure out what it is that your specific function needs to match. In many cases we haven't looked at these things very deeply as they simply weren't the 25 meter targets. Now they are. Once you start to build this understanding you can start to build options to counter the threats, and even better you can build options to provide threats that require countering. In essence, we need to get very smart very fast. We need to know exactly what we are facing. If we want to overmatch, we need to know what we are matching.

We have to learn the intrinsic value of what we each do. What is our unique selling point? What is it that we were chartered to do? We have to ask ourselves what are the knowledge, skills, and attributes that my organization…and <u>only</u> my organization…can accomplish. This may sound counter to our previous discussion about anti-fragility, and mastery of chaos, and operational unpredictability…but they are absolutely linked. In order to break the rules you have to master the rules first. When you start to operate in the operational hinterland of unknown and unknowable variations you will absolutely rely on the good order and discipline of your core competencies. Mastery of core competencies enable execution of your core capabilities. Yes, we can take Tank Companies and dismount them for door to door fighting, but we shouldn't even entertain casual discussion about those tasks until that Tank Company has absolutely mastered Gunnery, and maintenance, and mounted armored maneuver.

In order to enable this mastery we need to learn to say no….and we need to accept no as an answer. This is nearly impossible for most of us. We have built our personal and institutional identities on getting stuff done. 'Whatever it takes' and 'next man up' and 'failure is not an option' are cute little slogans for selling Gatorade and cleats, but this isn't the sort of mentality that builds lasting and effective defense institutions. But we also must recognize that we can't just say no without regard to who should be saying yes. We don't have the luxury of letting any tasks go undone. So we must coordinate and plan and synchronize at a feverish pace and a level of detail befitting that of professionals. At the operational level we can say no, but at the strategic level we need to ensure that somebody somewhere can say yes. An excellent framework to follow that can ensure this coverage is the idea of thinking about your role as a solutions provider rather than a forces provider. When we get taskings we always start with the troop-to task analysis. X problem requires Y amount of forces. Instead, it might befit us to look deeper into what effects we want accomplished rather than what we have to deploy. In this regards we can shift out of the "there is a nail and I have a hammer" mindset towards a "there is a project and we have a toolbox" mindset.

Finally we arrive we the ironclad, lead pipe, guaranteed, rock solid pick of the week good idea to win the next Cold War. We make them spend more than us. History tells us that one of the things that toppled the Soviet Union was their inability to match our industrial output. We outspent them and forced them to keep pace. But I'm not certain that we can do that again and I'm nearly certain that we don't want to. However, we can increase expenditure outside the normal financial sense. We can make them spend time, effort, political capital, and sometimes yes even money for everything they want to accomplish. Let's looks at the the Belt and Road Initiative creatively. What if we were able to create dissent at half of every major Chinese mining operation? A couple of bucket loaders with bad driving habits perhaps that caused minor disruptions. What about if we slowed work at every Chinese port by 1%. A few well-placed Harbor Masters slow to respond to requests. With a few carefully orchestrated and well-planned operations, synchronized across a wide range of targets, and you would start to see some real effects. Sand in the gears so to speak. Sounds like an un-gentlemanly way to go about fighting...a counter to regular warfare…might sound like Irregular Warfare. Almost as un-gentlemanly as widespread and state sanctioned intellectual property rights and patent violations. Or Social Media manipulation that seeks to influence election outcomes. We should make them spend more than us every chance we get.

Which brings us to our final task which is understanding risk. We're not talking about risk to force and risk to mission. What we are really talking about is the risk of inaction over the risk of action. As we've already discussed we've been inactive in the competitive space for decades and in that void our adversaries have evolved and filled the emptiness. Now we find ourselves reacting. There is growing understanding of risk in academia. Now we actually now have the first ever Professor of the Public Understanding of Risk in the Statistical Laboratory at the University of Cambridge. Sir David Speigelhalter is a statistician that now fills this role and his appointment represents an understanding that risk is an absolute factor in building public policy consensus. It certainly is logical to conclude that in the strategy business there might be some cross-over and there is much we can learn about what risk is, how we can define and describe it, and how we mitigate and even take advantage of it.

So our leaders have built for us a foundation. The NDS may not be an actual construction blueprint for us to build our security super-fortress, but at least they have given us an artist's rendition in this security ideology. They have given us license to innovate and freedom of intellectual maneuver. Our peer competitors have been busy in our strategic absence. It's time we got back into the fight.