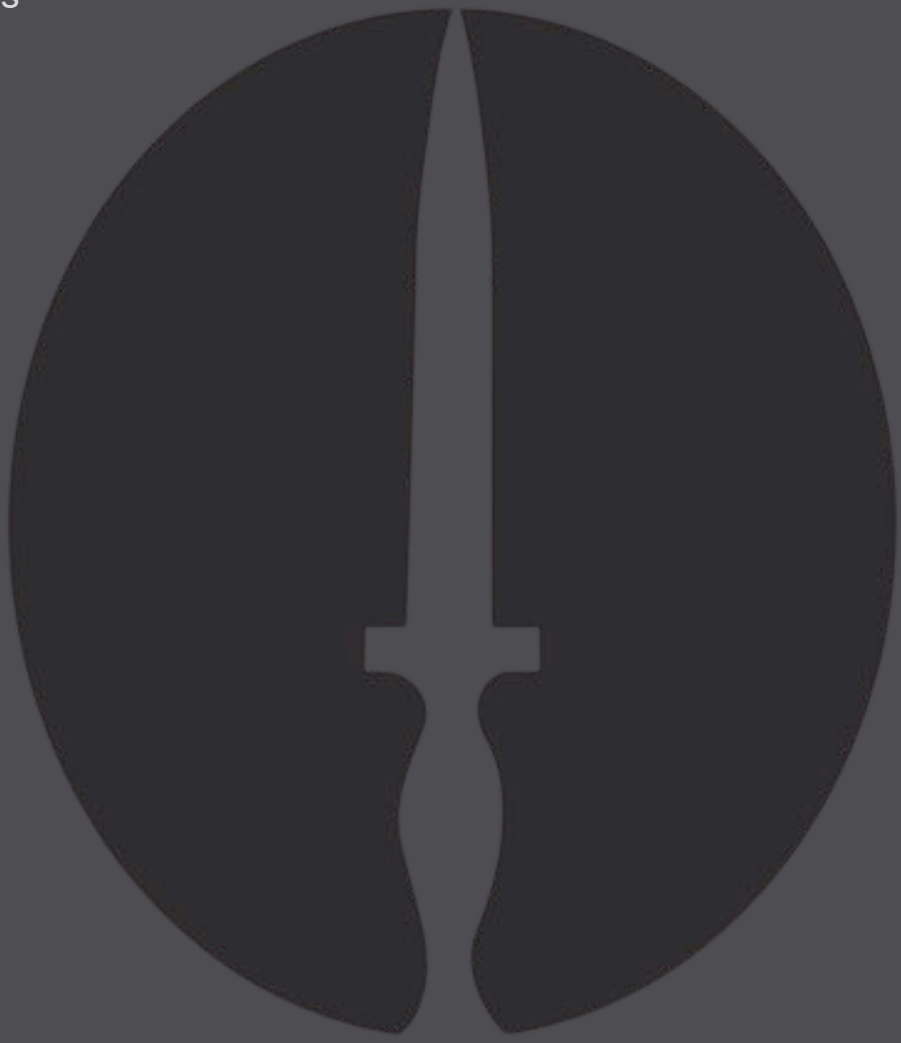
SPECIAL OPERATIONS JOURNAL

Editor: Christopher Marsh
Associate Editor: James Kiras

Included in this print edition:
Volume 7 Issue 1 (2021)



SORA
SPECIAL OPERATIONS RESEARCH ASSOCIATION

Routledge
Taylor & Francis Group

SPECIAL OPERATIONS JOURNAL
2021, VOL. 7, NO. 1, 1–16
https://doi.org/10.1080/23296151.2021.1905224

Routledge
Taylor & Francis Group

Designing at the Cutting Edge of Battle: The 75th Ranger Regiment's Project Galahad

John Stanczak[a], Peyton Talbott[a], and Ben Zweibelson[b]

[a]75th Ranger Regiment, Fort Benning, Georgia, USA; [b]Joint Special Operations University, MacDill AFB, Florida, USA

ABSTRACT

This article addresses the formal introduction of military design into the 75th Ranger Regimental organizational form and function over the last few years by leaders and design facilitators through creative destruction and willingness to experiment in paradoxical and potentially radical ways for emergent Special Operations Forces (SOF) needs. This article presents the core concepts behind Project Galahad, including the need for its formation, the context in which it exercises thought and action, and its structure and form as a disruptive engine of designing for novelty in warfare. This effort demonstrates military design "success" within lofty conceptual goals such as "fostering innovation" or "disrupting legacy systems to provide novel opportunities." Furthermore, this article shows how a broader design movement is simultaneously appearing in various incarnations and similar applications across the United States Special Operations Command (USSOCOM) and international special operations community.

KEYWORDS

Design; ranger regiment; SOF; operational planning

The 75th Ranger Regiment's role in driving change throughout the Army has roots deep within the history of American armed forces.[1] Rangers are known for employing novel, unconventional solutions to complex security challenges, and the recent organizational changes to Regimental staff structure and decision-making processes are no different. In pursuit of maximizing disruptive thinking and organizational transformation, the senior leadership of the 75th Ranger Regiment is forging a new cognitive path better suited for the dynamic, disruptive security demands of tomorrow's war. This article addresses the formal introduction of military design into Regimental organizational form and function over the last few years by leaders and design facilitators, and how each act of creation first required an act of destruction to create cognitive space for experimentation. That act of creative destruction would become known as "Project Galahad."

This article presents the core concepts behind Project Galahad, including the need for its formation, the context in which it exercises thought and action, and its structure and form. It also includes contemporary examples of military design "success" within conceptual goals such as "fostering innovation" or "disrupting legacy systems to provide novel opportunities." Furthermore, this article shows how a broader design movement is simultaneously appearing in various incarnations and similar applications across the United States Special

CONTACT Ben Zweibelson benzweibelson@gmail.com 3818 Cold Creek Drive, Valrico, FL 33596

The authors views are their own and do not represent those of the U.S. government, the Department of Defense, or the U.S. Special Operations Command. This article has been processed through all necessary DoD and SOCOM review policies and is approved for public release in full.

Operations Command (USSOCOM) and international special operations community. To explain the rise of Galahad, we first must revisit the original demand for change under the leadership of the Rangers' Regimental Commander where, despite achieving "success" using the legacy form and function, he would nonetheless take risks to challenge the system within.

In Design, the term "reflective practice" refers to the strong self-appreciation of how and why one thinks and acts in order to generate dynamic alternatives (Beaulieu-Brossard & Dufort, 2017; Gero & Kannengiesser, undated; Schön & Rein, 1994). In late 2017, Colonel Brandon Tegtmeier, 20th Commander of the 75th Ranger Regiment (RCO), set a planning effort into motion as an exercise in *organizational reflective practice*. The RCO recognized the risk posed by a legacy paradigm that applied yesterday's practices to tomorrow's challenges. He decided to take unconventional action toward his own organizational form and took steps to upend the legacy, Prussian-designed Regimental staff system.[2] The RCO was unable to get the necessary levels of focused effort from his staff when problems did not neatly fit into an Army planning model. The Regimental Staff was not postured to provide the Regiment with, to paraphrase design theorist Buchanan, "that which was needed for tomorrow's battle but did not yet exist" (Buchanan, 1992, p. 18).

YESTERDAY'S VICTORIES DO NOT WIN TOMORROW'S BATTLES

Structurally unchanged since its inception, the Regimental Staff (RSTAFF) was based on the standard, industrial-era general staff system that rose to popularity after the Prussian army successes in the Franco-Prussian war of 1871 (Keegan, 1988, p. 40). This staffing model is steeped in a Ranger history as far back as the French & Indian War where Major Robert Rogers led a light infantry company in service of the British Empire by providing reconnaissance and special operations. His "Rogers" Rangers' standing orders helped shape infantry maneuver away from formalized, pitched battles into a far more fluid and adaptive form of ground combat based in the unorthodox security challenges of the New World. Rangers have seen combat in every American war since, though Ranger units were repeatedly disbanded after each conflict ended. As the Vietnam War left the U.S. Army in disarray, Army Chief of Staff General Creighton Abrams established a new peace-time Ranger Battalion with a charter to be a change agent and exemplar of excellence for the rest of the Army. Successive Battalions were born and in 1984 the Regimental Headquarters was established, marking the beginning of the modern Ranger Regiment and an identity of discipline and excellence: *those who do what the rest of the Army does, but further, faster, and harder fought*. Decades later, the Global War on Terror (GWOT) would thrust the Ranger Regiment into an era of what some now define as "post-conventional conflict" that would suggest alternative modes of thought and action in war, even at the strong resistance of established military beliefs representing the modern era of warfare (McFate, 2019; Paparone, 2013).

Since October 2001, the 75th Ranger Regiment has been continuously deployed in support of the GWOT; over half of the modern 75th Ranger Regiment's 34-year existence as of this writing. The resulting evolution of contemporary Ranger identity is inextricable from combat operations in the Middle East and South Asia. The Regiment's GWOT experience both reinforced historic strengths and presented new, emergent challenges within the context of hundreds of rotations to the same operational mission set. This

continuity generates processes and structures that are highly effective at economizing practices and maximizing convergent standardization. The operational demand for continuity leaves little room for those who stray outside time-proven institutional practices. The uncertainty of war makes experimentation, even in conceptual forms, a difficult and controversial undertaking.

Despite this legacy frame, the RCO saw the emerging complex security environment of the 21st century as something that required a new way of operating at the Regimental level, starting with his staff's structure and processes. The rigid, bureaucratic structure of the RSTAFF made it difficult for the unit to address new challenges with old forms; to handle emerging, ambiguous, and complex problems while "keeping the trains running on time." By disrupting it, the RCO would introduce the space necessary to foster novel military thought and action that was otherwise unattainable in the previous structure. In June of 2017, he directed Regimental planning efforts to address this organizational question of both function *and* form. He charged a small team to get to work on alternatives options, providing them ample resources and virtually no conceptual restrictions. The multi-month design inquiry confirmed that the RSTAFF's traditional, Prussian-style structure limited its ability to effectively mass on multiple complex problems requiring expertise from across the RSTAFF. More importantly, however, it was the insular culture arising as an artifact of this structure that drove the human behaviors responsible for these tensions.

Planners proposed two options to transform the Regiment away from the legacy organizational structure. The RCO could re-organize the entire RSTAFF into cross-functional cells aligned to his priorities or establish a standing cross-functional team (CFT) with a sole focus on discrete complex problems determined by the RCO. Whichever choice was made, the Regiment would need to retain the ability to efficiently operate within the larger Army system as well as continue all combat operations ongoing for national security requirements. The re-organize option that flipped the Prussian-style staff structure on its head would be recognized as the superior option, despite the vast undertaking required. However, planners warned that eliminating legacy directorates risked functional chaos in coordinating with adjacent units and did nothing to prevent new silos from taking shape under a different moniker. The CFT, on the other hand, would be independent and unconstrained by existing doctrinal, institutional, or legacy form and function. It would be a dynamic and highly experimental "studio for war" within the Regiment, unlike any other staff function.

The Regiment's most acceptable option became to add an additional staff entity devoted entirely to the "deeper" issues within the organization. Named PROJECT GALAHAD in a nod to the code name given the Regiment's WWII predecessors, Project Galahad answered directly to the RCO, whose charter to the newly minted team was simple and direct: *Generate quick results through focused effort and be judged by the results produced for the Regiment*.[3] Importantly, the RCO directed the team to develop solutions, not execute them; that was for the staff to do. Galahad acted autonomously and independently of the Regimental staff, in entirely unorthodox forms devoid of traditional staff rules and requirements. There were no limitations and no restrictions on budget, travel, or schedule. There were no requirements to attend daily battle rhythm events or meetings. Galahad took guidance directly from the RCO and coordinated with the Regimental Executive Officer, Regimental staff primaries, and the Battalion Executive Officers. This unique cell was not a "shadow" staff or merely a think tank existing at the "ivory tower" level of an organization

as some Commander Action Groups (CAGs) have been critiqued in being.[4] It was not an industrial "R&D" center either, as Galahad would exist to address the most vexing and convoluted Regimental issues on the RCO's plate. Rather, Galahad was an experimental complex problem-solving cell at the tactical level for an O-6 Commander frustrated with his organization's inability to solve them.

Galahad would need to break out of the institutional norms of the legacy Regimental staff structure to critically self-reflect, experiment with alternative concepts, and introduce radical unconventional options that came with their own risks, opportunities, and consequences. Often, design activities would unfold in unfamiliar ways, yet through experimentation and alternative theories the design action would open new cognitive doors for the command team to explore entirely different opportunities for thought and action. Through three years of experimentation underpinned by complexity theory and reflective practice, Project Galahad undertook a new way of thinking far removed from the traditional processes of doctrine. This shift would be from analytic optimization and reductionism toward that of divergent and experimental thinking: *military design*. The term here is not at all pigeonholed within the narrow confines of U.S. Army Design Methodology or any single service-imposed doctrinal template for designing.[5] Instead, Galahad follows a multidisciplinary design school of thought espoused across SOCOM and beyond by the Joint Special Operations University and other similar multidisciplinary programs.(Beaulieu-Brossard, 2020; Jackson, 2019a; Zweibelson, 2017b; Zweibelson, Whale, & Mitchell, 2019)

Galahad in execution since 2017 has provided a 'Janusian mindset'(Rothenberg, 1971) for the Regiment, presenting paradoxical and alternative concepts while disrupting traditional military modes of logic such as linear-causal thinking, singular end-states, and an overemphasis on engineering and analytic reasoning in war.(Bloomfield, Burrell, & Vurdubakis, 2017, p. 2; Meiser, 2016; Monk, 2017) Galahad enables this partly through its unique posture as a crossover between the varying "silos" of the Regiment and its access to multiple stakeholder perspectives from across the USSOCOM enterprise. It operated within dozens of networks, leading it to synthesize perspectives from across the organization. This included unpopular, ancillary, or even counterintuitive positions on difficult, elusive topics concerning the Regiment. It also served as something of a "blind-spot" catch for many staff efforts, although not limited to addressing the function and maintenance of existing institutionally sanctioned practices, methods, and doctrine such as an Army Red Team. Rather, Galahad *could question the form itself*, and consider radical and highly disruptive concepts that would normally be dismissed or marginalized in conventional discourse. To accomplish this, the Galahad team would adapt irregular and nonlinear battle rhythms and engage across the organization in an emergent fashion. The virtue of being welcomed and present amongst the varied clans substantially enhanced the effectiveness and understanding of a Galahad design activity, compounding the return-on-investment for the organization. This would also soften the institutional resistance to consider highly unorthodox concepts, the critique of deeply cherished organizational processes, as well as amplify minority perspectives.

Designing for security challenges is now taking hold in a powerful way within the 75th Ranger Regiment. Ranger Battalion Command Sergeants Major now send junior Noncommissioned Officers to formalized design courses that expose them to various design schools of practice and competing theoretical bases. Ranger staff officers seek out a variety of design practices and self-development well outside the traditional military planning

methods or PME-centered decision-making program offerings. This transformation took several years of gradual, grassroots efforts centering largely in the Galahad cell while influencing larger and larger effects across the Regiment. This would culminate in an institution-wide design effort that cemented military design ethos across the Regimental leadership.

In March 2020, Colonel Todd Brown, the 21st Regimental Commander hosted a 3-day design conference with over 100 participants from across the entire Regimental command teams and key staff sections. Design facilitators from SOCOM's Joint Special Operations University led a series of design exercises that generated rich, collaborative dialogue, followed by tangible decisions about future task organization, senior enlisted management, and focused equipment modernization efforts.[6] While some initially found the tables full of LEGO, markers, and Post-It notes curiously out-of-place for a leadership off-site event in the Ranger Regiment, by the end of the 3-day design workshop, participants walked away with a newfound appreciation of the benefits of military design practice as applied to complex security challenges for the Regiment. This conference proved the exceptional value of investing in divergent, disruptive, and unorthodox modes of *sensemaking* for complex security challenges outside of doctrinal or institutionally sanctioned forms.

Project Galahad has formalized a culture of flattened, dynamic innovation within the Regimental force structure to provide the Regimental Command Team with radical concepts, alternative perspectives, and critical reflection concerning Regiment's crucial mission set and strategic orientation. This is the birth of a military design team tailored to a Brigade-sized Infantry force with special operations capabilities and national-level mission orientation.

THE MEANING OF DESIGN AND ITS RISE TO MAINSTREAM SECURITY STUDIES

Project Galahad first encountered military design concepts while searching for broadening opportunities at the Joint Special Operations University (JSOU). Galahad members attended JSOU's *SOF Design & Innovation Basic Course*, a week-long immersion into design thinking, systems theory, postmodern warfare, and a wide range of disciplines within a dynamic classroom environment where unorthodoxy became the norm from the first day's "ice-breaker" exercise (The JSOU JAWS Exercise and How SOCOM is Dropping Cognitive Tools with Military Design – YouTube, 2020). Through this and subsequent courses on design, disruptive and critical thinking, Galahad quickly determined that security design would be an important core component of how it would onboard new members and approach complex security challenges for the Regiment. To Project Galahad, design thinking *itself* represented what the RCO had known the organization needed but did not yet possess: a mode for unlocking novelty and shedding irrelevant or outdated practices quickly. It was a different, yet effective way to approach "wicked" problems that did not lend themselves to traditional staff processes and structures (Buchanan, 1992; Conklin, 2008; Nelson & Stolterman, 2014).

The modern concept of designing for societies originated with the Industrial Revolution, primarily in commercial applications where the product design became the central focus. Modern design seeks what is "new" or an improvement for users, goods, and services; more abstractly, for human expression of organizations, decision-making, and understanding complex reality (Buchanan, 1992, p. 18; Krippendorff, 2000, pp. 2–4; Protzen & Harris,

2010). Militaries are exceptionally proficient in convergent thought and action where analytic optimization, uniformity, and repetition permit rapid exploitation of known "best practices" even within the chaotic landscape of human organized conflict. However, militaries are notoriously ill-equipped to pivot to divergent, experimental, and emergent practices in these same contexts. Instead, the institutional straitjacket of ritualization, legacy belief systems, and linear, causal reasoning tend to close military organizations off to real critical reflection upon the "why" of how militaries think and act in war. Thus, designing in security applications requires an ability to realize why one's organization thinks and acts in war the way it does, to critically reflect and challenge processes that require adjustment, disruption, or elimination.

As a verb, to "design" is to create an idea, method, activity, or tangible artifact that did not exist previously, and is needed (but not necessarily wanted yet) by the military organization frustrated by existing constructs proving insufficient or counterproductive to current warfare. There is a decidedly destructive aspect of design, in that before one creates the novel, an existing flawed or outdated construct must be selected for destruction as frequently stated by the father of military design, Israeli Brigadier General (retired) Shimon Naveh.[7] Every historically significant figure from Aristotle to Martin Luther King Jr. first destructively challenged legacy paradigms before giving rise to alternative methods of sensemaking. Conventional military decision-making methodologies essentially lack any mechanism for challenging the status quo or reflection beyond that which is prescribed within doctrine and practiced (Graicer, 2017b; Jackson, 2019a; Naveh, Schneider, & Challans, 2009; Paparone, 2019; Ryan, 2016). Whether at national military training centers, military classrooms or in combat, the military organization is rewarded for following set rules and processes or improving them and discouraged or even punished for attempting activities that disrupt, contradict, or damage the institutional standards and dominant beliefs. Unorthodox or experimental constructs are neither welcomed nor generally authorized unless filtered through a rigid and hierarchical vetting process for inculcation into existing military doctrine and education. This normally suppresses or terminates any real innovation or drives it underground.

Military design has been for decades an underground movement comprised of heretics, outsiders and trouble-makers critical of the dominant military form and function; this makes for designing in warfare to be a career hazard. Nonetheless, designers have demonstrated a deep desire to improve and break with irrelevant military form and function since the beginning. The first example of formal military design methodology placed into operation occurred in the 1990s with the Israeli Defense Forces and represents the first time a design logic attempted not to enhance, *but to entirely replace* a military's sensemaking and decision-making methodology for theory and action in war (Feldman, 2007; Graicer, 2017a; Weizman, 2007, pp. 210–212). Today, there is an ever-growing military community of practice that researches, experiments, and practices with a wide range of international military design methodologies across multiple disciplines and from the tactical and technological to the strategic and multi-national partnership levels in war (Beaulieu-Brossard & Dufort, 2017; Jackson, 2019a; Zweibelson, 2018). Military design in various formats now exist in multiple service doctrines, is provided at many different levels of professional military education (PME). Due to design's emphasis on disruption and drawing from radical fields such as postmodernism and other areas well outside established military topics of research, design is critiqued as being too confusing, difficult to learn, too unorthodox to

become mainstream, and too radical to be integrated into modern military strategy and planning activities. Despite the controversial aspects of design, the topic also continues to be associated with terms such as: innovation, disruption, transformation, and game-changing aspects of security challenges.

A military design team equipped with design education and *given the expectation to think divergently* will assume a deeply disruptive, experimental role that generates new cognitive maneuver space for that unit command team. Many of the institutional "sacred cows" are set for slaughter, and a reflective mind-set attempts to consider the organization systemically (system-wide, interconnected, dynamic, emergent) over the reductionist preference found in analytical rationalization (break things down, categorize, apply rules, reassemble, solve) (Morgan, 2006, pp. 1–36; Naveh et al., 2009; Putnam, 1983). Furthermore, military design teams operate in a continuous cycle of divergent and convergent processes rather than attempt to force a single, convergent pathway to a solution. Military designers reflect on their internal values and belief system and acknowledge their frame for understanding reality and war. They then seek alternative perspectives that unlock entirely dissimilar ways and meaning for the organization to reframe the security context (Zweibelson, 2016, 2017a). The creativity and open-mindedness to consider '*what could be* as opposed to "*what must be"* requires humility and the ability to continuously question one's assumptions and biases. The divergent, iterative, and experimental aspects of this design approach require very different skills, support, and interaction within the military organization (Graicer, 2017a; Jackson, 2019a; Martin, 2011, 2015).

While the concept of iterative experimentation is critical for success in complex systems, it is dangerous territory for a design team operating in a results-oriented military institution. Where business leaders would applaud even a 25% success rate on projects derived from research & development, military leaders often do not have the time, tolerance, or resources for "failed" experimental approaches to change. Military culture often features a deep institutional fear of the concept of failure and contemporary professional development discussions and ethics reform efforts experience major issues with how and why "failure" is understood. Commanders are naturally reticent to break things that have worked "well-enough," in their organization, and often look for results to beat the tyranny of the command timeline. Field grade leaders with a low career tolerance for modest evaluations are unlikely to assume the risk of coloring outside the lines. These are broad brush strokes, but fair ones in that the military innovators in modern history are often visionary and also frequently punished or ostracized by their peers. They are later revered by subsequent generations that benefited from their willingness to challenge the system at great personal sacrifice. This does not make for attractive career decisions nor inspire creative risk at any level in most military organizations despite the popularized slogans and claptrap by senior leaders for "out of the box thinking" and "learning organization", "innovative forward thinking" and the like.

Militaries appear to readily accept change if it is incremental and additive to existing practices. The military organization frequently brokers in addition while avoiding subtraction (Lauder, 2009; Paparone, 2019; Zweibelson, 2015b). Change that disrupts, destroys, or replaces deeply cherished practices or established beliefs and identity is much less common, and the fear of such radical disruption generates significant opposition and skepticism. Thus, it becomes critical for the organization and for the design team to translate novel concepts into actionable planning criteria that do not risk outright organizational rejection.

The message of the idea itself must be carefully crafted (Naveh, undated document; Tsoukas & Hatch, 2001; White, 1990). To effectively translate design to action, designers must become familiar and comfortable with an organization's resistance to change and contemplate a variety of modes to enact substantial transformation despite these resistances. Often the solution the organization *needs*, as defined by the design team, is radically different than what the organization will *accept*, and frequently the call to drop one's favored conceptual tools to pick up unfamiliar or novel ones becomes a major undertaking for institutional reform (Weick, 1993, 1996).[8]

Learning from several implementation failures early in the program, Project Galahad adopted a conceptual, "some is better than none" approach. The team had to learn that the accepted idea may be only a loose derivative of the "best" approach. In 2017, for example, the "best" option would have been to re-design the entire RSTAFF, yet the corresponding disruption all but ensured the broader institution would reject such radical experimentation and disruption of the established norm. The "acceptable" solution was, therefore, Project Galahad itself. With a deliberate focus on the implicit and explicit needs of key stakeholders and deep reflection, design teams can anticipate this institutional resistance and account for it early. If done persuasively and within a dynamic and imaginative format, teams will be able to offer a range of compelling design opportunities set within a range of possible futures. A rich design narrative frames these opportunities to explain the opportunities, risks, and anticipated consequences of these novel actions.

CONSTRUCTING A GALAHAD WITHIN THE TRADITIONAL INFANTRY ORGANIZATION

The 75th Ranger Regiment is unlike most other Army Infantry Brigades in two important regards. Admittedly, these enabling factors give the organization a distinct edge in creating a team such as Project Galahad. First, the Rangers enjoy the luxury of the first pick of the top-quality professionals desiring service in any capacity in the organization. There is no shortage of high performers waiting in line for their chance to join the organization. Secondly, the Ranger Regiment enjoys a higher level of resources and force flexibility than most BDE-sized organizations. However, the team would come to find that it was not the talent, money, or authorities that truly gave them an edge. Anyone in Galahad would say this was possible in any Army Brigade with appropriate command emphasis and the right mix of people with *the right attitudes*. Ironically, the best security designers are often not also the best planners; expecting a strong military planner to flip from high-convergent reductionist analysis into high-divergent ideation and experimentation is a common failure in military design talent management. Even worse, military organizations that "dual-hat" staff operational planning cells to oscillate from design to planning in compressed timelines will often just get one and never the other.

The Rangers learned from these previous institutional failings, and took additional consideration in how, why and where to implement a dedicated design team for maximum impact. For Galahad to prove most effective to the organization, a culture of psychological safety and humility among its members was paramount. Without it, Galahad would conform to the identity and opinions of its senior officer at the sacrifice of free exchange of thought that could develop more thorough concepts. Galahad had to challenge, disrupt and even confront the RCO with both a design alternative framing of the legacy system (how

things have been) as well as a controversial and experimental range of alternative futures and normative options (what *could be* for Regiment in a wide range of unimagined tomorrows that challenge the traditional expectations). This degree of discourse, controversy, and experimentation requires careful yet bold initiatives and mature personalities.

Leaders manned Galahad primarily based on assessments that candidates had the right personality. The importance of building Project Galahad as a "team" rather than a "section" would enhance cohesion and foster a completely trusting context needed to radically challenge Regimental sacred cows. This team dynamic allowed for a whole greater than the sum of its parts; where accountability, creativity, and the free exchange of ideas and perspectives could emerge in a safe, encouraging context. It was, therefore, necessary to strike a balance of people humble enough to check their ego and recognize how their experiences give them a unique paradigm or "window" through which they see the world. They would also need to be willing to question the status quo and deconstruct assumptions that could evoke vigorous resistance. COL Tegtmeier and later COL Brown would not pile all the Regimental top performers into one special design cell, nor would they invoke staff fratricide by granting exclusive and superior access to this particular team in disruption of existing institutional norms. Rather, the RCOs took a tailored approach by combining the personalities most conducive to supporting the Galahad mission as a new supporting element within the overarching Regimental purpose.

Galahad learned that the ideal number of members was between 5–6 people. Less than five let to groupthink while more than six led to cliquing or potentially fractions within the design team. In the Regiment, the preponderance of these came from Rangers that would otherwise supplement the Regimental operations section (S3 shop). The core of the design cell consisted of a senior MAJ, CPT, MSG, and civilian contractor. Galahad needed a senior field grade with a high level of influence in the organization to coordinate at the requisite levels required, acknowledging the unavoidable power dynamics of military centralized hierarchies. A senior captain would coordinate and direct team efforts and serve as the action officer of the design cell. A Senior Enlisted Advisor (E-7+) with organizational experience and influence provided a senior enlisted perspective, engaged directly with the Regimental Sergeant Major and facilitated access with the enlisted population. The civilian contractor provided continuity and knowledge management as Rangers rotated positions. For the remaining few, it was critical to have members of diverse backgrounds with unique experiences inside and outside of the organization so that Galahad could foster diversity of thought and enable multiple stakeholder perspectives, even internally. Even a team member that had just joined the Regiment provided value with no conditioning to the cultural norms and processes that could inhibit divergent thought.

Galahad, by the very intent of their composition and "anti-staff" configuration that bucked the Regimental standardization and traditional norms, would take particular actions to attempt to mitigate any potential "them versus us" tensions aforementioned as observed in similar Strategic Initiative Groups (SIG), CAGs and military think tanks.[9] Sensitive to how the lack of participation in the daily churn of the staff may be perceived, Galahad placed special emphasis on performing essential "Ranger tasks" at every available opportunity, thus softening the tension of a design cell seemingly able to diverge from otherwise rigid organizational rulesets. They manifested for every airborne operation, participated in "Standards Week" events, and pulled their weight in staff duty shifts.[10] While not required to attend meetings, Galahad's OIC would deliberately attend as often as practical to

maintain touchpoints with the staff and keep a pulse on organizational initiatives. This was in addition to the unorthodox engagements Galahad was doing simultaneously to the directed Regimental meetings and battle rhythm.

To get the most return on investment while prioritizing experimentation and imagination, Galahad established a deliberate onboarding process to prime Rangers to "drop their tools" conceptually and begin to reflectively practice a design outlook that would augment Galahad's almost "pirate organization" existence at the edge of innovation, experimental risk, and real-world consequence for disrupting the organization.[11] The onboarding process included completion of JSOU's premier "Basic Design and Innovation Course" or SOC3440, where students are introduced to many of the design methodologies that frequent the Galahad workspace.[12] The Regiment would later make the JSOU design course mandatory for all Galahad new cell members from 2019 onward, and recommend Regiment-wide attendance when possible to inculcate design thinking across the organization and seed future Galahad recruits.

To maximize the organization's return on its investment in Galahad, Regimental leadership sponsored extensive training and education opportunities for the team. Galahad leaders created a holistic development program focused on leading theories and practices in brain and social sciences and creative problem solving. Galahad discovered and participated in the Brain Performance Institute's "Strategic Memory Advanced Reasoning Training (SMART) Training".[13] This course, developed through research from the UT Dallas' Center for Brain Health, informs participants on daily routines and methods that engage frontal networks and bypass the limbic system to develop deeper level thinking, creativity, and meaningful learning. Galahad would also draw from the multi-disciplinary design education at JSOU and pair that with this psychological-biological approach to creativity from the SMART program. Galahad members took the NEO-PI-3 assessment,[14] with follow up executive coaching from the Regimental psychologist to increase self-awareness and to effectively account for the impact of a new member on the overall network of personalities for the team. To round out this process, a series of readings and podcasts were developed, to include Cal Newport's "Deep Work," which serves as a guide to limiting distractions and focusing on cognitively demanding tasks (Newport, 2016). Galahad's multi-disciplinary education would require time, resources, and the energy of Regimental leadership to build a powerful, tailored design cell capable of executing the demanding requirements as envisioned by COL Tegtmeier and further enhanced by COL Brown.

MILITARY DESIGN IN ACTION: HOW GALAHAD CONTRIBUTED VALUE TO THE REGIMENT

In the fall of 2017, the Ranger Regiment found itself facing the challenges of near-peer warfare when the Comprehensive Nuclear Test Ban Treaty Organization (CTBTO) detected an unusual seismic event in East Asia (2017Sept DPRK: CTBTO Preparatory Commission, n.d.). American policymakers interpreted this event as a show of force and a threat to U.S. National security. The Department of Defense quickly diverted its focus to "Large Scale Conflict", and the Ranger Regiment, still engaged in the counter-terrorism fight, had to be prepared to do the same. Project Galahad's first task materialized here and represented a difficult mission-set for an organization that had been largely engaged in the GWOT for two continuous decades of combat rotations. Galahad initiated movement on the RCO's

broad aspiration: "*prepare the Regiment to pivot toward war on the Korean peninsula.*" Galahad logged extensive international travel to hold planning sessions and discourse with a disparate range of stakeholders and synchronize efforts with key influencers in the SOCOM enterprise. Galahad's design recommendations here would drive the RCO's decision to fundamentally change the training cycle and reallocate resources to initiatives addressing critical shortfalls. With this major shift in how the Regiment planned and prepared for business, Galahad earned immediate credibility as a "heavy-hitting" entity of the Regiment in uncertain times and emergent, unfamiliar challenges.

Another "early win" for Galahad was its second major design project: redesigning a Campaign Plan (CAMPLAN) for the Regiment. Campaign planning is a classic implementation of the "ends-ways-means" construct at the operational level of war. It consists of the linkage of tactical operations to achieve strategic objectives, centered on the military hierarchical form and function (Meiser, 2016; Monk, 2017; Naveh, 1997, pp. 8–14; Naveh et al., 2009, pp. 36–46; Paparone, 2008, 2013, pp. 90–97; Zweibelson, 2015b). CAMPLANs are often unwieldy and cumbersome, capturing dozens of Lines of Efforts (LOE), sub-LOEs, supporting tasks, and priorities. The RCO realized the bureaucratic creep of the process coupled with the increasingly incompatible, rigid planning format and cautioned that " . . . *this cannot become something that is hundreds of pages long, pontificating without any real use or application to the force.*"[15] As Galahad represented the innovation cell for the Regiment, it needed to appreciate the methodological structural issues with the CAMPLAN form *itself* instead of attempting to generate alternative yet doctrinally adherent variations that would still result in an overly rigid, mechanistic, and legacy oriented product. Galahad would focus on the design tensions existing somewhat abstractly throughout modern military planning methods, and alternative design considerations that could modify or circumvent some of the major concerns for the Regiment.

Galahad drew from design theory as well as the wide commercial application of scenario planning (or strategic foresight) that organizes differently from the reverse-engineered, analytically optimized military "single desired end-state" logic (MacLean, 2008; Sikander, 2016; Wack, 1985; Wilkinson & Kupers, 2013). Instead of generating a CAMPLAN, Galahad developed what it called the "Ranger Strategy Process" that deviated from the traditional single-desired-future state for CAMPLAN structuring. The Ranger Strategy Process included an annual conference bringing together dozens of the Regiment's senior leaders to discuss investments for the future and capitalized on considering multiple alternative futures where the Regiment would not eliminate undesired ones in an analytic, reductionist fashion. Rather, they would explore opportunities, risk, and consequences across multiple diverse and often paradoxical futures. This system helped ensure key decisions were made with not just the current commander in the room, but the next three. A range of possible and emergent futures were considered, particularly some radical ones that were controversial and often unimagined if drawing from previous linear strategic constructs for Regiment associated with established Regimental methods.

In another example of Galahad providing design deliverables for the Regiment, it would focus on Ranger talent management. In July of 2019, COL Brown gave Galahad a project he titled the "War for Talent." His aspiration was for the team was to design a new system that would, "*Recruit, sustain and retain the most talented NCOs in the Army.*" To implement such a program, Galahad first had to appreciate the system and the behaviors that drive Rangers to depart military service, reenlist for more time in the Regiment, or to assess for

other organizations. Members traveled to every Ranger Battalion to hold rank-free interviews in civilian attire with cross-sections of the formation. Galahad surveyed Rangers from Private to Sergeant Major to gain an appreciation of their lives, desires, beliefs, and careers. This was under the human-centered design approach of "stakeholder analysis" or "empathy mapping." Galahad sought to learn both the "what" *and* the "why" behind stakeholder thoughts, feelings, actions, and words. The meaning behind the decisions and the narratives from a wide range of stakeholders outlined core tensions and highlighted ways to disrupt or challenge some institutional barriers for retention and recruitment transformation.

Galahad ultimately proposed a design opportunity to experiment which formed a completely new staff section to meet the education, wellness, and career management needs of Rangers in a different model than previously done. In a symbol relatable to the warrior mind-set of Rangers, they named it the PHALANX program, an ode to the Greek Phalanx, where the effectiveness of the force was dependent on its weakest link. The program consisted of three pillars that formalize career progression, facilitate continued education, and provide resources to enhance human performance – both physically and mentally.[16] This program continues through today with continued development and a fusion of design thinking coupled with immediate military planning and evaluation.

CONCLUSIONS AND ANTI-CONCLUSIONS

To the outside observer, Project Galahad has, quite frankly, met with more failures than successes. Yet those failures were within the iterative design process of experimentation, critical reflection, and reframing to consider new opportunities, risks, and consequences. In some ways, the embrace of iterative, dynamic "experiment-fail-reflect-opportunity" is different, unorthodox, and even disruptive to deeply cherished Ranger values. Yet Galahad has offered the Ranger Regiment something that it has never had before: a dynamic, radical approach to problem framing that exists outside of the "ends, ways, means" and clear "identify the problem, execute a preplanned solution, assess" logic that has been a framework for Ranger Officers and NCOs for years. The failures of Project Galahad represent the holistic process where, over time, major innovations become reachable that otherwise were impossible to see (Stanley & Lehman, 2015). To the untrained eye, these failures will appear as pointless efforts that lack direction or substance; criticism of design typically demands some guarantee of success before the experimentation is even undertaken which reflects complete misunderstanding of design in war. However, as Amazon's Jeff Bezos says, "You have to be willing to be misunderstood if you're going to innovate" (Clifford, 2018). Substantive change is rarely clear until well after the dust settles.

On the other hand, the Regiment's willingness to "fail fast" and to accept an unfinished product led toward much of Galahad's successes as well as a reflective practice of "thinking about one's thinking" for learning through disruption (Beaulieu-Brossard & Dufort, 2016; Paparone, 2019; Schön, 1984). The military's design movement is more than just an excuse to shoot holes in the current processes and methodology; it gives the organization permission to "fail" in a way that transcends a singular focus on the organizational "function" and permits a disruption of previously unchallenged organizational "forms." If one is building sandcastles with only one bucket to use, the entire range of possible designs is limited to what a bucket-shape of sand can do. However, when one can realize the shape of one bucket, and encourage the organization to challenge and replace one favored "bucket shape"

with others that are unfamiliar or unrealized, the new opportunities for vastly different sandcastle designs become possible. In instances of putting men and women into harm's way to achieve the nation's military objectives, the Ranger Regiment permits no room for failure; however, an organization's embrace of this international military design movement (Beaulieu-Brossard, 2020; Beaulieu-Brossard & Dufort, 2017; Jackson, 2020) demonstrates that it is willing to learn and to embrace failure to ultimately maintain its lethality and adaptability in a future that is far from linear or predictable.

Notes

1. The authors wish to thank the following people for their assistance in reviewing, editing, and assisting in the creation of this article: COL Todd Brown, COL Brandon Tegtmeier, LTC Adam Armstrong, LTC Ari Martyn, MAJ Aaron Heaviland, MAJ James Barker, CPT Nicholas Naquin, MSG Raye Perez, Mr. Glenn Legg, and Mr. Joe Hester.
2. The Regimental staff conducted a multi-month design inquiry into this problem, ultimately determining that *"RHQ's structure is arranged in silos, resulting in an inability to effectively process information and mass on multiple complex problems that require expertise from across the staff."* The problems with changing that structure were too numerous to be considered feasible in the short-range span for options.
3. In 1943 over 2,750 "Merrill's Marauders," commanded by BG Frank D. Merrill, marched into Burma on a long-range mission behind Japanese lines with no precedent or blueprint for success. Code named "The Galahad Project," the Marauders marched for 5 months through over 750 miles of jungle terrain, successfully capturing Myitkyina, reopening the Burma Road and enabling land resupply of China. The Marauders were later rebranded the 475th Infantry, the predecessors to the 75th Ranger Regiment.
4. Martin recounts his own troubling experiences while serving in a CAG for NATO Training Mission-Afghanistan and the difficulties of bridging design to the broader staff functions. See: (Martin, 2011).
5. For instance, the U.S. Marine Corps introduced their own interpretation of Army Design Methodology in draft, unofficial doctrine while several failed attempts to force SOCOM into a "SOF Design Way" further illustrate this service-centric trend of seeking a singular and branded methodology exclusively for one service and not others.
6. For examples of JSOU's particular design educational approach, see: (Military Design 101: JSOU Enabling Innovative Thought and Action for USSOCOM – YouTube, 2020, p. 101; The JSOU JAWS Exercise and How SOCOM is Dropping Cognitive Tools with Military Design – YouTube, 2020).
7. (S. Naveh & O. Graicer, personal communication, October 15, 2019, p. 15:43) (Bureau, 2013a).
8. We use the term "solution" here sparingly, as it is frequently misinterpreted in security design. Solutions are temporary and fleeting- in complex emergent security contexts what appears to be a "solution" today can morph quickly into disastrous patterns tomorrow. Instead, referring to the work of Russell Ackoff, security designers consider problem resolutions and dissolutions in particular vice the standard mechanistic "solution inventory-problem identification-application-repetition" cycle.
9. On CAGs and SIGs applying military design, see: (Zweibelson, 2015a).
10. Regimental Standards week is series of physical assessments that Rangers must pass annually to be eligible for continued service in the organization.
11. On the metaphoric device of "pirate organizations" as well as the role of high-risk experimentation through destroying existing institutionalisms in order to create space for creative innovation, see: (Bloomfield et al., 2017; Bureau, 2013a; Durand & Vergne, 2012).
12. For more information on JSOU design courses, see their registrars and course catalog online at: https://www.socom.mil/JSOU/_layouts/15/jsou.public/pages/Courses.aspx.

13. ("High Performance Brain Training," n.d.) BPI frames its brain training programs: *"Based on the brain science of neuroplasticity, we know that our brains are adaptable and trainable, driven by how we engage every day. In the same way that we can improve our bodies through physical fitness, we can increase our focus, creativity and mental efficiency with targeted strategies and healthy brain habits."*
14. The NEO-PI-3 is a standard questionnaire of the five-factor model. In addition to measuring the five major domains of personality, it provides insight into the six facets that define each domain. (Costa & McCrae, n.d.).
15. Authors paraphrasing RCO guidance issued at the time. Both RCOs reviewed this article prior to publication and confirmed the accuracy of all attributed quotes.
16. A full description of this program would exceed the scope of this article. Galahad intends to focus a future military design article on this particular Galahad design deliverable to expand this in detail.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

REFERENCES

2017 Sept DPRK: CTBTO Preparatory Commission. (n.d.). Retrieved from https://www.ctbto.org/the-treaty/developments-after-1996/2017-sept-dprk/

Beaulieu-Brossard, P. (2020). Encountering nomads in Israel defense forces and beyond. In *Concepts at work: On the linguistic infrastructure of world politics,*pp. 1–20. University of Michigan Press.

Beaulieu-Brossard, P., & Dufort, P. (2016, October 16). *Introduction to the conference: The rise of reflective military practitioners*. Hybrid Warfare: New Ontologies and Epistemologies in Armed Forces, Canadian Forces College, Toronto, Canada.

Beaulieu-Brossard, P., & Dufort, P. (2017). *The archipelago of design: Researching reflexive military practices*. The Archipelago of Design: Researching Reflexive Military Practices. www.militaryepistemology.com

Bloomfield, B., Burrell, G., & Vurdubakis, T. (2017). Licence to kill? On the organization of destruction in the 21st century. *Organization*, *24*(4), 441–455. doi:10.1177/1350508417700404

Buchanan, R. (1992). Wicked problems in design thinking. *Design Issues*, *8*(2), 5–21. doi:10.2307/1511637

Bureau, S. (2013). Entrepreneurship as a subversive activity: How can entrepreneurs destroy in the process of creative destruction? *M@n@gement*, *16*(3), 204–237. doi:10.3917/mana.163.0204

Clifford, C. (2018, May 17). *Jeff Bezos: 'If you cannot afford to be misunderstood, don't do anything new or innovative'* [News]. CNBC. Retrieved from https://www.cnbc.com/2018/05/17/jeff-bezos-on-what-it-takes-to-be-innovative.html

Conklin, J. (2008). Wicked Problems and Social Complexity. In *Dialogue mapping: Building shared understanding of wicked problems*. CogNexus Institute. http://www.cognexus.org

Costa, P. T., & McCrae, R. R. (n.d.). *NEO^{TM} Personality Inventory-3* (pp. 2). Sigma Assessment Systems, Inc.

Durand, R., & Vergne, J.-P. (2012). No territory, no profit: The pirate organization and capitalism in the making. *M@n@gement*, *15*(3), 264–272. doi:10.3917/mana.153.0265

Feldman, Y. (2007, October 25). Dr. Naveh, or, how I learned to stop worrying and walk through walls [Online social media and news blog]. *HAARETZ.Com*. https://www.haaretz.com/misc/article-print-page/1.4990742

Gero, J., & Kannengiesser, U. (undated). *An Ontology of Donald Schön's reflection in designing*. Sydney, Australia: Key Centre of Design Computing and Cognition, University of Sydney.

Graicer, O. (2017a). Self disruption: Seizing the High ground of systemic operational design (SOD). *Journal of Military and Strategic Studies*, *17*(4), 21–37.

Graicer, O. (2017b). Beware of the power of the dark side: The inevitable coupling of doctrine and design. In *Experticia Militar* (pp. 30–37). Colombia: Experticia Militar, Revista Profesional del Ejército Nacional de Colombia; Centro de Doctrina del Ejército (CEDOE).
Jackson, A. (2019a). Introduction: What is design thinking and how is it of use to the Australian defence force. *Australian Journal of Defence and Strategic Studies*, *3*, 1–22.
Jackson, A. (2020). *Civilian and military design thinking:A comparative historical and paradigmatic analysis, and its implications for military designers* (pp. 1–31). https://www.airuniversity.af.edu/AUPress/Display/Article/2437970/design-thinking-in-commerce-and-war-contrasting-civilian-and-military-innovatio/
Keegan, J. (1988). *The Mask of Command*. New York: Penguin Books.
Krippendorff, K. (2000). Propositions of human-centeredness; A philosophy for design. In D. Durling & K. Friedman (Eds.), *Doctoral education in design: Foundations for the future: Proceedings of the conference held 8-12* July 2000, La Clusaz, France. Staffordshire University Press.
Lauder, M. (2009). Systemic operational design: Freeing operational planning from the shackles of linearity. *Canadian Military Journal*, *9*(4), 41–49.
MacLean, R. (2008). Environmental leadership: The power of scenario planning in executive communications. *Environmental Quality Management*, *18*(2), 95–100. doi:10.1002/tqem.20210
Martin, G. (2011). A tale of two design efforts [And why they both failed in Afghanistan]. *Small Wars Journal*, 16.
Martin, G. (2015). Deniers of "The Truth": Why an agnostic approach to warfare is key. *Military Review*, *95*(1), 42–51.
McFate, S. (2019). *The new rules of war* (First ed.). New York: William Morrow.
Meiser, J. (2016). Ends + Ways + Means = (Bad) Strategy. *Parameters*, *46*(4), 81–91.
Military Design 101: JSOU Enabling Innovative Thought and Action for USSOCOM - YouTube. (2020, May 4). [Video Mp4]. JSOU campus studio. Retrieved from https://www.youtube.com/watch?v=WjZ-NpjsxUs
Monk, J. (2017). *End state: The fallacy of modern military planning* [Research Report].
Morgan, G. (2006). *Images as organizations (Updated Edition of the International Bestseller)*. London, UK: Sage Publications.
Naveh, S. (1997). *In pursuit of military excellence: The evolution of operational theory*. New York: Frank Cass.
Naveh, S. (undated document). *Northern storm: A narrative of reflective command, systemic learning, and operational design 2002-2005* [PowerPoint Presentation].
Naveh, S., Schneider, J., & Challans, T. (2009). *The structure of operational revolution: A prolegomena*. Fort Leavenworth, Kansas: Booz Allen Hamilton.
Nelson, H., & Stolterman, E. (2014). *The design way (Second)*. Cambridge, Massachusetts: The MIT Press.
Newport, C. (2016). *Deep work: Rules for focused success in a distracted world* (1st ed.). New York: Grand Central Publishing.
Paparone, C. (2008). On metaphors we are led by. *Military Review*, *88*(6), 55–64.
Paparone, C. (2013). *The sociology of military science: Prospects for postinstitutional military design*. New York: Bloomsbury Academic Publishing.
Paparone, C. (2019). Designing meaning in the reflective practice of national security: frame awareness and frame innovation. In A. Jackson & F. Mackrell (Eds.), *Design thinking: Applications for the Australian defence force*, (editor's manuscript pre-publication version, pp. 1–18). Canberra, Australia: Defence Publishing Service.
Protzen, J.-P., & Harris, D. (2010). *The universe of design: Horst Rittel's theories of design and planning*. New York: Routledge.
Putnam, L. (1983). The interpretive perspective: An alternative to functionalism. In L. Putnam & M. Pacanowsky (Eds.), *Communication and organizations: An interpretive approach* (pp. 31–54). Beverly Hills, California: Sage Publications.
Rothenberg, A. (1971). The process of janusian thinking in creativity. *Archives of General Psychiatry*, *24*(3), 195. doi:10.1001/archpsyc.1971.01750090001001

Ryan, A. (2016, November 4). A personal reflection on introducing design to the U.S. Army. *The Medium*. https://medium.com/the-overlap/a-personal-reflection-on-introducing-design-to-the-u-s-army-3f8bd76adcb2

Schön, D. (1984). *The reflective practitioner: How professionals think in action* (1st ed.). New York: Basic Books.

Schön, D., & Rein, M. (1994). *Frame reflection: Towards the resolution of intractable policy controversies*. New York: Basic Books.

Sikander, A. (2016). Scenario-planning as a stand-alone tool for strategic foresight: Limitations and options. *Change Management: An International Journal*, *16*(1), 13–18.

Stanley, K., & Lehman, J. (2015). *Why* greatness cannot be planned*: The Myth of the objective*. Switzerland: Springer International Publishing.

The JSOU JAWS Exercise and How SOCOM is Dropping Cognitive Tools with Military Design—YouTube. (2020, April 10). [Video Mp4]. JSOU campus studio. Retrieved from https://www.youtube.com/watch?v=kf_IQ5uCS8g

Tsoukas, H., & Hatch, M. J. (2001). Complex thinking, complex practice: The case for a narrative approach to organizational complexity. *Human Relations*, *54*(8), 979–1013. doi:10.1177/0018726701548001

Wack, P. (1985). Scenarios: Uncharted waters ahead. *Harvard Business Review*, 73–89.

Weick, K. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, *38*(4), 628–652. doi:10.2307/2393339

Weick, K. (1996). Drop your tools: An allegory for organizational studies. *Administrative Science Quarterly*, *41*(2), 301–313. doi:10.2307/2393722

Weizman, E. (2007). *Hollow Land: Israel's architecture of occupation*. New York: Verso.

White, H. (1990). *The content of the form: Narrative discourse and historical representation* (paperback edition ed.). Baltimore: The John Hopkins University Press.

Wilkinson, A., & Kupers, R. (2013). Living in the futures: How scenario planning changed corporate strategy. *Harvard Business Review*, *91*(4), 119–127.

Zweibelson, B. (2015a). Military 'Deep Dives' and organizational management: The continuing Hazards of Hubris, centralized hierarchies, and insular perspectives | Small Wars Journal. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/military-%E2%80%98deep-dives%E2%80%99-and-organizational-management-the-continuing-hazards-of-hubris-centra

Zweibelson, B. (2015b). One piece at a time: Why linear planning and institutionalisms promote military campaign failures. *Defence Studies Journal*, *15*(4), 360–375. doi:10.1080/14702436.2015.1113667

Zweibelson, B. (2016). Special operations and design thinking: Through the looking glass of organizational knowledge production. *Special Operations Journal*, *2*(1), 22–32. doi:10.1080/23296151.2016.1151753

Zweibelson, B. (2017a). Change agents for the SOF enterprise: Design considerations for SOF leadership confronting complex environments. *Special Operations Journal*, *3*(2), 127–140. doi:10.1080/23296151.2017.1384274

Zweibelson, B. (2017b). An application of theory: Second generation military design on the horizon. *Small Wars Journal*.

Zweibelson, B. (2018, June 20). Designing through complexity and human conflict: Acknowledging the 21st century military design movement. *Design Lecture with Phil Gilbert and Ben Zweibelson on Military Design and IBM Design Movements*. SPADE 2018: Rethinking Defense and Security in the Digital Age, Copenhagen, Denmark.

Zweibelson, B., Whale, K., & Mitchell, P. (2019). Rounding the edges of the maple leaf: Emergent design and systems thinking in the Canadian armed forces. *Canadian Military Journal*, *19*(4), 25–33.

SPECIAL OPERATIONS JOURNAL
2021, VOL. 7, NO. 1, 17–28
https://doi.org/10.1080/23296151.2021.1904570

Routledge
Taylor & Francis Group

Supporting Resistance Movements in Cyberspace

Nicholas A. Bredenkamp[a] and Mark Grzegorzewski[b]

[a]Joint Special Operations University, MacDill AFB, Tampa, Florida, USA; [b]United States Army Special Operations Command

ABSTRACT

One of United States Special Operations Forces' (SOF) core missions is support to unconventional warfare (UW). As SOF continues competing with states below the level of armed conflict, it must adapt to and capitalize on advances in technology to enable support to resistance movements. Other states, namely Russia, have capitalized on digital technologies in their undeclared, hybrid conflicts. The U.S., which will likely find itself on the other side of those conflicts, must rethink and update how it supports resistance movements. We suggest why to make this change now, and in the process offer cyber-based proposals that could be employed in support to resistance

KEYWORDS

Resistance; unconventional warfare; cyberspace

The United States has supported resistance movements challenging entrenched regimes when their objectives aligned with U.S.' interest. Supporting resistance movements has long been part U.S. military strategy. The technique gained considerable recognition in the support provided to national resistance movements against Nazi occupation during World War II. The Office of Strategic Services (OSS) and its famed Jedburgh teams deployed deep into Nazi Europe to link up with French partisans and disrupt German forces in preparation for D-Day (Irwin, 2009). These teams provided weapons, training, and intelligence to the partisans – turning often disorganized pockets of resistance into a strategic asset. Future U.S. support to resistance movements would follow a similar model established by the OSS, a model largely still used today. However, while contemporary models are very similar to traditional models, supporting resistance movements in cyberspace has several advantages over traditional methods.

As these groups start to leverage cyberspace and cyber tools in their struggle, SOF – and specifically U.S. Special Forces as the proponent for supporting resistance movements – have missed opportunities to adapt to this new domain. As technology becomes cheaper and more widely available, increasingly more human activities, including resistance movements, will take place online. As such, U.S. SOF and the resistance elements they support can benefit from adapting cyber-based practices.

The call for cyber-enabled unconventional warfare is not new. COL(R) Pat Duggan has developed this concept for years. Duggan's proposals are not unidimensional and range from cyberspace influence operations to operational preparation of the battlefield to employing cyberspace applications. To Duggan, SOF has a role to play in cyberspace and should be using the tools at its disposal to influence social media networks via UW-pilot

CONTACT Mark Grzegorzewski Mark.Grzegorzewski.ctr@socom.mil Joint Special Operations University, MacDill AFB, 7708 Tampa Point Blvd, Tampa, FL 33621

teams (Duggan, 2014a). These teams, most likely Special Forces due to their cross-cultural competence, would be forward in the sense they would in another's social media networks. Once in these networks, they could both sense the environment and work to influence the environment before and during hostilities. Duggan builds upon the almost limitless possibilities of SOF in cyberspace by noting they could also use cyberspace tools to identify, assess, and evaluate resistance leaders and capabilities (Duggan, 2014b). Thus, rather than having SOF forward and putting service members at risk, reaching out to resistance leaders via cyberspace is a lower risk way in which to build relationships before deploying to the physical environment. Duggan builds upon the possibilities of SOF in cyberspace next by focusing on the applications that can be leveraged via the domain (Duggan, 2016). Here, SOF could leverage tools to have real world effects (e.g. 3-D printing) to financial warfare (via hacking financial systems) to compromising data in enemy networks. Finally, Duggan sees the cyberspace medium as a way to sense adversarial environments and understand what drives an enemy's actions (Duggan, 2016). Once the environment is understood, SOF can then leverage divides within the enemy and exploit situations to SOF's advantage.

In this article, we take up Duggan's call and propose that SOF should increasingly embrace supporting resistance movements in cyberspace. In our estimation, the main barrier in supporting resistance movements via cyberspace is a lack of awareness on what is permitted and what can be achieved. We aim to fill this gap, plus demonstrate the resource savings by digitally supporting a resistance movement. Since cyber-enabled resistance movements are hypothetically less resource intensive, in the form of physical space needed to organize and the time needed to get to those locations safely, they have a lower barrier to entry for participation. Accordingly, cyber-enabled resistance should in fact consume less resources while at the same time providing exponentially more support to resistance movements.

To further examine opportunities for SOF to support resistance movements in cyberspace this paper proceeds as follows. First, we discuss the advantages of supporting a resistance movement via cyberspace. Next, we examine a textbook example of working by, with, and through cyberspace in conflict. While we do not have specific examples of how Russia enabled tactical-level resistance forces by, with, and through cyberspace, we postulate ways in which this support could have been easily provided. In doing so, we demonstrate how investment in cyber-enabled resistance saves costs in material, labor, and time, and consequently achieves a greater impact when compared to not utilizing cyber applications and methods. We conclude with remaining challenges to incorporating cyber applications to resistance support.

WHY CYBER-ENABLED RESISTANCE MOVEMENT?

There is little doubt the internet has drastically increased the effectiveness of our daily lives. It has made the transition of information incredible easy, computation has been streamlined, and automation has cut production time significantly. These benefits extend to unconventional warfare as well, offering several advantages over previous models. Compared to traditional unconventional warfare, cyber-enabled support to resistance movements do not require forces to deploy into harm's way. Rather, SOF can utilize cyberspace to remotely support resistance members from anywhere in the world. As will be discussed, this has benefits both to safety and resources. While it is becoming

increasingly more difficult to remain anonymous online, the anonymity created by cyberspace aids in protecting the identity of both U.S. SOF advisors and their partner forces, making it easier to conceal U.S. support and allowing for new members to join the resistance. Cyber enabled resistance movements typically have a lower barrier to entry then traditional models – receiving support from external state actors or non-state actors requires nothing more than an internet connection, a device such as a computer, tablet, or phone, and a fraction of the member's effort compared to traditional movements (USASOC, 2019). Finally, the ability to support a resistance at scale and to shape the narrative from a distance are attributes that can be found in traditional support to resistance. These factors allow for greater participation from otherwise unwilling resistance members because the interaction takes place in the relative safety of cyberspace, members might be more willing to participate in a low-risk cyber enabled resistance movement then a comparatively high-risk traditional movement.

Traditional unconventional warfare campaigns are extremely dangerous, both politically and in term of the loss of human life (Army Techniques Publication 3-05.1, 2013). For example, resistance members and SOF must evade enemy forces, access to medical care is often unreliable, and techniques to infiltrate the battlespace are often complex and risky (McRaven, 1996).

These missions have a very narrow window of success, but an extremely high pay off. Retired Admiral William H. McRaven described the complexity and risk of such operations in his work *Spec Ops: Case Studies in Special Operations* (1996) by examining what he calls the "relative superiority line," or a threshold when elements of the mission are in balance to give the SOF unit a higher probability of success. Certain benefits of cyberspace can help to tip the scales in favor of a successful outcome.

For example, when SOF deploy forward, they rely on surrogate forces to provide security, ensure their safety, and transport them throughout the battlespace. This is incredibly risky and resource intensive, and both the resistance members and SOF must devote a considerable amount of time on security practices. In comparison, cyber-enabled resistance movements do not require forces to deploy into harm's way, and cyberspace allows the U.S. to remotely support resistance members from anywhere in the world. Resistance members also benefit from the safety provided by cyberspace, and although techniques exist to determine the physical location of a computer's user, virtual private networks and other security measures can protect resistance members by masking their location. While all forms of warfare experience some form of risk, cyberspace support to resistance movements from U.S. soil reduces the physical risk to U.S. forces, as well as reducing the cost to provide support.

Traditional resistance movements can require large amounts of time and resources to be successful. In comparison, cyber-enabled resistance movements require less of a time commitment and resources from both its members and U.S. support. While in historic cases, U.S. support has offset much of the material cost of maintaining the resistance movement, supporting traditional resistance movements remains a time and resource intensive endeavor. In traditional movements, resistance members must accept a high-cost, both in time and effort, to take part in the movement. Participating in the resistance puts their lives at risk and often takes them away from their families and their source of income.

This lower commitment barrier of entry allows members to participate anywhere in the world, maintain their jobs, and continuing with their families–an aspect examined by Chenoweth, Stephan, and Stephan's (2011) assessment of successful nonviolent resistance movements. The researchers claim one factor for the success of any resistance movement is the percentage of the population that can be motivated to join in collective action. In turn, movement's in which "members can more easily retain autonomy, which means that they can often commit acts of resistance without making major life commitment" have a much higher probability of gaining participation (Chenoweth et al., 2011). This phenomena was further examined by Robinson in his analysis of HAMAS members in their resistance to Israeli occupation – although the main cadre was comprised of "true believers" a vast majority of the organization was members who could participate as part of the normal pattern of life (Robinson, 2004).

While these members are unable to participate in fighting in the physical dimension because of proximity, they can be active members of the movement from a distance. This technique allows the resistance movement to essentially "crowd source" worldwide support for their cause, creating a support base far greater than what is possible in traditional movements, establishing what futurist John Robb describes as an "open-source insurgency" (Scott, 2018). Crowdsourcing uses a massive number of people online to achieve a certain task, for example, translating a document or finding a solution to a difficult math problem. The advantage of crowdsourcing is even if thousands of people give minimal support, their combined efforts are still greater than the complete efforts of a small group. Crowdsourced members of cyber-enabled movements can take part at their leisure, being highly active one day and less active the next. The low-level of commitment to cyber-enabled movements – in resources, time, and effort – might lure individuals who would be less likely to commit to a traditional resistance movement.

In his work *LikeWar*, author P.W. Singer examines the notion of a worldwide support base in his study of Bellingcat's counter-Ukraine separatist efforts. Singer and Brooking describe how the safety of the internet allowed average citizens to participate in dismantling an information operation campaign to cover up the 2014 downing of the Malaysian Airlines Flight 17 from the comfort of their homes (Singer & Brooking, 2018). By tapping into the power of crowd sourced support, Bellingcat used self-proclaimed "citizen investigative journalists" to tie Russian-backed separatist to the attack, eventually aiding in an international court case against the separatist. From afar, Bellingcat conducted an in-depth intelligence operation against the separatist and provided names, photos, and contact information of the soldiers responsible for the attack to the international court prosecutors (Singer & Brooking, 2018). Without the protection provided by the anonymity of the internet, these individuals might not have felt safe enough to participate in the operation.

U.S. forces supporting cyber-enabled resistance movements from U.S. soil offer a low-cost option to achieve results comparable to traditional methods. Deploying forces abroad is incredibly expensive, requiring extensive logistical support networks that are often work-force-intensive and costly to maintain. For example, in 2014 the Center for Strategic and Budgetary Assessments determined that when accounting for transportation, housing, food and pay, the cost to deploy each soldier to Afghanistan is approximately 2.1 USD million per service member (Harrison, 2014). In comparison, U.S. based SOF personnel can support cyber-enabled resistance movements without deploying anywhere and little more than a robust internet connection.

The anonymity of the internet plays a crucial role for cyber-enabled resistance movements – it protects both the resistance members and their U.S. advisors. As with the Bellingcat example, the safety provided by the anonymity allowed average citizens to overcome the fear of challenging state-backed insurgents in faraway lands. The lack of face-to-face interaction allows people to overcome the barrier of fear preventing many from joining the movement.

In 2009, Jeffrey Hancock described how online anonymity allows people to overcome their fears as the motivation enhancement effect. The lack of face-to-face interaction online incentivizes individuals to display personality traits they often repress, for example internet trolling, fabricating social media posts, and complete false personas. In many cases, the characteristics an individual displays in-person might be completely different from their online persona and they are often more nefarious (Hancock, 2007). Considering this account, cyber-enabled resistance movements can gain the support of followers who might not have joined a traditional resistance movement because of fear or other psychological barriers. The anonymity of the internet does not just benefit the resistance members; it also benefits their U.S. SOF advisors.

The anonymity of the internet allows SOF to mask their identity and assume a persona of a resistance member. As Chenowith and Stephen have noted, overt state support to resistance movements can often create a free-rider problem in which local members reduce participation because of foreign support. Additionally, state sponsored support to resistance movements can lead to issues of delegitimization and hinder recruiting efforts with demographics who are hesitant to be viewed as puppets for external actors or associated with the policies of those actors. By assuming an identity of a non-U.S. citizen or fellow resistance member, SOF's support can achieve a more grassroots appeal, and may aid in swaying potential resistance members who may be against receiving direct support from the U.S. By assuming a more palpable persona for reluctant resistance members, SOF can provide support using several methods.

The SOF enterprise most certainly incurs an opportunity cost of committing cyber resources against a problem set that could be diverted somewhere else, but the U.S. taxpayer has already incurred the labor cost of maintaining a workforce capable of providing advice to resistance movements. However, U.S taxpayers avoid the cost needed to transport that workforce to its customer (i.e. the resistance) because the service is provided remotely. As a result, the labor theory of value of cyber-enabled resistance movements is lower than that of a traditional movement.[1] This reduces the cost of cyber-enabled resistance movements and frees critical support networks for other operations. When compared to traditional strategies, cyber-enabled resistance movements have an extraordinarily low-fixed cost to participate, a concept often referred to as a barrier to entry.

Where in typical resistance movements mass mobilization must be harnessed from a common motivating factor, in cyber enabled resistance movements vastly different demographics can be uniquely motivated by their own factors. Utilizing rapid A/B testing, cyber enabled resistance movement can recruit and mobilize each user based off his or her user preferences. The same technology social media and search engines use to know what to market, can be used to motivate individuals based of their own beliefs and preferences. The sheer amount of data, testing protocol, and computation makes this method extremely difficult for traditional resistance movements.

Resistance movements require a certain level of physical ability. That is to say, you must be able to carry a firearm, etc. In comparison, cyber-enabled resistance movements can leverage portions of the population who may be willing to support but physically unable to participate in combat. Moreover, in situations where cultural practices prevent female participation, cyber-enabled resistance allows for that portion of society to be active members of the resistance but not engaging in direct combat.

While enabling resistance movements in cyberspace does not make traditional techniques obsolete, it does offer a new medium and mode for supporting resistance movements with many advantages over traditional methods. Cyber-enabled resistance movements offer a viable option when traditional methods are impractical or difficult, such as regime control over a population or a lack of political appetite for committing ground forces. Supporting resistance movements in cyberspace provides Commanders with options to impose costs on an opponent at scale and distance while preserving resources for other operations. This method is a low-cost, low-risk option for secretively supporting resistance movements in states with high levels of security that make traditional methods impractical. The relative safety provided by the internet aids resistance members in forming a cohesive group without massing them for possible apprehension by regime forces. Further, the obfuscation of the internet allows the resistance movement to develop without exposing itself due to travel or proximity, and masks the resistance member's actions under a cloak of an internet persona.

When combined with robust digital information operations, resistance movements enabled in cyberspace can shape the narrative in their favor. As an example, a resistance movement could amplify the justness of their cause and potentially gain international support for their movement against a repressive regime. Through digital information operations and SOF advisement, resistance movements employing cyber-enabled information operations could mobilize a population and turn a digital cause into real world change.

LESSONS LEARNED: UKRAINE

Researchers' primary focus of Russia's cyberspace efforts in Ukraine have focused at the operational-strategic level (US Army Special Operations Command, 2019). This focus is not unwarranted. Russia achieved objectives through cyberspace that researchers had not yet seen implemented. The levers to achieve these objectives included shutting down power in Ukraine, twice, and melding information operations with kinetic effects to effectively achieve objectives with minimal bloodshed. Quickly achieving objectives and minimizing bloodshed, in a virtually contactless war is how Russia prefers to fight (USASOC, 2017).

The synergies of cyberspace, information, and real-world effects were successful at the operational-strategic levels for Russia. Just the same, Russia could have combined cyberspace, information, and real-world effects to empower the tactical-level resistance movements in the east of Ukraine and in the Crimean Peninsula. From an understanding of the what was possible in Ukraine, SOF can shape its own efforts when supporting resistance movements. Granted, the demographics in Ukraine and history of Russian involvement in that theater certainly played into their ability to target and influence the population. Yet, we contend SOF still can conceptually borrow from Russia's operations and empower resistance forces with the same cyberspace training and tools, albeit with slight tweaks depending on the actors involved and objectives sought.

Control over information in Ukraine made the difference (Galeotti, 2015). Russia learned the lesson of information dominance several times prior to Ukraine, first in Lithuania (1991) and then in Chechnya (and Dagestan) (1994–1996 (and 1999–2009)). In each of these instances, Russia found that when an invading force does not control the narrative, it invites unwanted scrutiny (USASOC, 2017). In response, today Russia scales down their military operations, in effect fighting unconventional warfare, in states within their sphere of influence.[2] Since these states have a past association with Russia, it also means they likely have large Russian-speaking populations residing within them and Russian culture is familiar within these countries. These two attributes definitely play into Russia's success in supporting cyber-enabled resistance operations within their sphere of influence.

Russia first implemented this strategy in Estonia (2007) and later Georgia (2008). As has been recounted elsewhere (Lange-Lonatamishvili, 2014; Ottis, 2008), the dispute in Estonia started over the relocation of a Soviet-era bronze statue and resulted in massive distributed denial of service (DDOS) attacks. Russia claimed it was simply "patriotic hackers" involved in this cyberattack but later analysis showed that the cybercriminal "Russian Business Network" and ethnic Russians helped execute these attacks. The lesson for Russia in Estonia was that cyberspace can be used for strategic messaging and provide plausible deniability for the attacker. In Georgia, Russia used hackers, both native and foreign, to attack Georgian networks to slow down their response to Russia's conventional invasion and to deliver propaganda to both Georgia and the rest of the world. The lesson from Georgia was that Russia could use virtual applications and proxy forces to have real world effects.

Russia achieved blindingly quick success because the Ukrainians (and the West) never anticipated Russia had so well seeded the information environment. Ukraine, which was formally part of the Soviet Union and has a large Russian-speaking population, was certainly an easy target to influence. However, there was never a guarantee of success. To be successful, it required years of preparation of the battlefield. Without preparing the cognitive battlespace, Russia would not have been able to quickly activate opposition groups within Ukraine to achieve strategic objectives before anyone could respond. This meant Russia had to cultivate relationships in Ukraine long before any actual conflict. As part of this cultivation, Russia likely provided clandestine training on how to use cyberspace tools to affect the information environment.

Resources

In terms of cost of the operation, Russia's support to their resistance movement in Ukraine is unknown. According to the U.S. Senate Select Committee on Intelligence report on "Russian Active Measure's Campaigns and Interference in the 2016 U.S. Election," Russia spent 100,000 USD over two years for advertisements which bought 3,400 Facebook and Instagram advertisements. Compared against the 1.25 USD million dollars a month to run the Internet Research Agency, 200,000 USD over two years (US Senate Report, 2020) is a miniscule amount to impact the information environment. This change in the information environment, which was shaped by Russia, created the impression amongst some ethnic Russians that Ukraine did not have a representative government and thus they should resist. For those already willing to resist the Ukrainian government, this message provided confirmation that the government was illegitimate. Thus, we agree with the conclusion of Jolanta Darczewska from the Warsaw Center of Eastern Studies regarding information warfare when she states "It is cheap, it is a universal

weapon, it has unlimited range, it is easily accessible and permeates all state borders without restrictions" (Darczewska et al. 2014, 13).

Other relatively cheap capabilities that Russia employed in Ukraine included the use of botnets to disrupt, deny, and disable Ukrainian communications infrastructure. Botnets as a service (aaS) costs on the darknet anywhere from 200-700 USD for a few hundred bots (or about ($0.50/bot) (Namestnikov, 2009). Among the actions that a botnet could take, and that Russia implemented in Ukraine, include DDoS attacks, theft of data, spamming computers, and accessing compromised devices and their connections. This attack on the communications infrastructure slowed and confused any Ukrainian response to the rising resistance movement in the country. All of these cyberspace actions in Ukraine were most likely facilitated by Russia's national level cyberspace agencies but easily could have been taught to or facilitated by resistance members at a local level. As stressed earlier, all one needs to engage in cyberspace operations is an internet connection, a device, and access to information and tools.

Other actions taken in the Ukraine included uploading pornographic images to Ukrainian protestor's social media accounts, hacking e-mail and social media, and accessing financial accounts (CCDOE, 2015). Again, these cyberspace activities most likely were executed at the national command level. Yet, these activities could easily be conducted by resistance forces when given the proper training and tools. In fact, local resistance forces would be able to micro target local officials even more effectively than a foreign sponsor since they are more familiar with local politics, thereby delegitimizing that official in the eyes of the public.

Anonymity

Russia deployed several cyberspace applications at a distance. These applications could easily have been employed by Russia-backed resistance fighters in Ukraine. One of these applications was a program that was installed on the Ukrainian military's Android devices and allowed them to track artillery fire coming in from the Russians. Unbeknownst to the Ukrainians, Russia had hacked this application, and once the Ukrainians logged into the application to record the incoming fire, it allowed the Russians to geolocate them and more accurately target the Ukrainians (Volz, 2016). Assuming no hackers in the Ukrainian resistance movement, which itself strain credulity, Russia could have easily trained members of the resistance to insert malware[3] into an application. In fact, one can find online tutorials on how to insert malware with prices starting as low as 45 USD (Swinhoe, 2020). If Russia wanted to train resistance members to employ ransomware aaS, that would costs around 85,000 USD (Insights, 2020). Even if those capabilities were deemed inappropriate for resistance forces, they could still be trained on how to access other types of more limited malware on the dark web. By point of comparison, arming a resistance member with an AK-47 costs anywhere from 2,800 USD to 3,600 USD (Forbes, 2017).

Ability and Scale

Due to Ukraine still being dependent on Russian technology before the conflict, Russia had access to social media applications in Ukraine and was able to leverage these mediums to build the narrative that the regime in Kiev was "fascist" and threatening the rights of Russians living in Ukraine. Moreover, when the "little green men" appeared in theater and starting protesting

against the Ukrainian government, it almost certainly encouraged others to rise up and resist the government. Of course, once a proper demonstration was started by these Russian Spetsnaz forces, they would disappear into the crowd and allow the newly emboldened resistance to take over the protest. This same technique could have applications in cyberspace. Russian forces could herd[4] resistance members on social media, amplify grievances, back away from the conversation, and either allow real world conflict to erupt or simply poison the local discourse. Herding would in turn cause the state to expend resources in correcting the narrative, responding to real world violence, and even repairing cyber vandalism (e.g. website defacement).

Narrative

With control over the narrative within the theater, Russia was able to not only reify the belief amongst some Ukrainian-Russians that they were under attack by an illegitimate government but also to shape the narrative internationally. Through the use of numerous groups with Russian nationalist agendas in Ukraine, to include Cossacks paramilitaries and the Night Wolves motorcycle club, Russia was able to achieve plausible deniability. Make no mistake about it, these groups were funded and trained by Russia (Meadows, 2014). Accordingly, Russia made use of these forces to shape the narrative of threatened Russians resisting the Ukrainian government, and being supported by volunteers from Russia who were there to defend democracy and human rights (USASOC, 2017). This messaging was reinforced by the amplifying and reinforcing impacts of Russia Today's (RT) YouTube channel and Russian social media (VKontakte or "VK") which reported on each other's stories and made the resistance appear more impactful.

Another way in which Russia employed cyberspace effects in Ukraine was through the use of jamming equipment which can block transmission of data (Kofman, Migacheva, Nichiporuk, Radin, and Oberholtzer, 2017). In this case, this jamming equipment was transported by Russian ships but easily could have been handed off to resistance members to block data transmission by the Ukrainian government. By reducing the ability of Ukraine to communicate, it stifled their efforts to reincorporate parts of the breakaway territories. Used by a resistance force, this jamming equipment could stifle local authorities and slow the state's ability to respond to sabotage carried out by the resistance.

CONTINUING CHALLENGES TO INCORPORATING "CYBER"

As laid out above, incorporating more cyber-enabled resistance operations lowers resource costs, increases anonymity, increases ability and scale, and allows a first mover advantage to shape the narrative. Each of these contribute to an overall positive net assessment, however we would be remiss if we did not point out challenges in cyber-enabled resistance campaigns. First, in the case we examined, each of the aspects of cyber-enabled resistance perfectly aligned. This will not be the case with most resistance campaigns. In crafting this nearly ideal cyber-enabled resistance campaign, Russia was able to test out capabilities in other regional conflicts (e.g. Estonia and Georgia) before determining under what conditions they could achieve an optimal cyber-enabled resistance campaign. Moreover, Russia had deep cultural and historical knowledge of each of these states, Ukraine, Estonia, and Georgia, which saved time when planning these campaigns. Not every state, and particularly the United States, will have these conditions preset before a campaign starts. Therefore, a planner should not anticipate that all cyber-enabled resistance campaigns will be plug-and-play.

Second, we should not assume that when inserting cyberspace into resistance operations that the enemy will not respond. In resistance, it is a constant tug of war between offensive actions and defensive responses. As such, if SOF attempts to enable resistance forces with cyberspace capabilities, a regime may respond with disabling tactics, such as shutting down the internet within the country. Short of shutting down the internet, resistance members and SOF must always protect themselves with digital tools like the Onion Router (TOR) or using virtual private networks (VPNs). These capabilities mask communications and keep resistance members and SOF one step ahead of the opposition. If the internet is shut down by a country, the resistance must consider setting up proxy domain name servers[5] (DNS). This DNS proxy will not work as quickly as a regular DNS server under normal conditions (e.g. internet at full capacity) but it will find and transfer information with some degradation. Among the problems a proxy server will face, the IP addresses may not transfer all information and messages may not arrive in order. Nevertheless, a DNS proxy server is one way to get around a complete government internet shutdown and is a capability that resistance forces must set up.

Third, while we advocate that internet-enabled resistance forces[6] (Pascoli & Grzegorzewski, 2021) should be involved in a cyber-enabled resistance campaign, there is no guarantee that these forces will adhere to what the client state wants. In the case of Russia, the state had long-lasting, deep ties to their proxy and resistance forces as a result of historical and cultural ties. As such, there is no guarantee to U.S. planners that cyber-enabled proxy forces may not act contrarily to U.S. objectives. Yet, this is no different than the ongoing relationships and concerns that the U.S. has with other resistance forces. Non-cyber resistance forces are readily given lethal weaponry by the U.S. As such, the U.S. military must overcome the mental block that providing cyber support to resistance forces is any different than providing other types of lethal aid. However, the U.S will likely need to deeply vet candidates for cyber-enabled support to resistance since the it will likely not have the same cultural and historical ties that Russia enjoyed.

Fourth, when providing cyber-enabled support to resistance, the U.S. must make sure to provide capabilities and training that cannot be used against the U.S. or its allies. In the case of Russia, they were able to provide specific capabilities that they knew would not come back to harm their own security. The U.S. could find itself in a similar situation in which it enables a resistance force to attack American made technology. In such a case, the resistance force should not be given cyber capabilities or training that would harm the U.S. (unless perhaps the application is first quietly patched in the United States). Instead, the U.S. could still provide remote advise and assist through cyberspace capabilities but not provide cyberspace capabilities that could harm the U.S.

Finally, one of the greatest challenges that constantly plague resistance movements is penetration or infiltration by government entities. A cyber-enabled approach to supporting resistance brings its own vulnerabilities in this respect. Resistance members will not always know whether the person on the other end of the cyber-enabled communications is a SOF member or if they have been infiltrated. Likewise, resistance members will not know whether the cyberspace enabled equipment is riddled with malware, thereby giving away their location. Therefore, both resistance members and SOF must adopt a zero trust model[7] where no one is always trusted and no one is given default accesses. Under the zero trust model, the resistance and SOF should assume that they have been infiltrated and always be on the lookout for vulnerabilities. Once those vulnerabilities are found, they must be corrected and/or patched, while never becoming complacent that vulnerabilities have been completely fixed.

CONCLUSION

Despite years of advocacy, there is still reluctance to enable resistance forces by, with, and through cyberspace. This may be due to a lack of awareness of authorities by senior leaders and fear of a cyber applications causing unintended consequences. As leaders become increasingly aware of what they can do with cyberspace authorities and come to understand cyberspace applications as just another weapon, the U.S. can be on the forefront of action in cyber-enabling resistance campaigns. U.S. competitors, like Russia, are already working within this space and perfecting the execution of multidomain operations, to include cyber-enabling operations. Other competitors, such as China, Iran, and North Korea understand that they cannot conventionally compete with the U.S and that the way to challenge the U.S. is through asymmetric capabilities. SOF, which itself is an asymmetric capability, needs to embrace its role in support to resistance and imbue that support with cyber applications. We have laid out why this shift would benefit support to resistance, and even improve SOF's UW mission. This fight will not go away. SOF must technologically adapt in support to resistance, or it will find itself woefully unprepared for its fights of the future.

Notes

1. The Oxford Dictionary of Economics defines labor theory of value as "value of goods and services determined by the amount of directed and indirect labor inputs need to produce or provide them."
2. States within the Russian sphere of influence are typically associated with those states that made up parts of the former-Soviet Union.
3. Short for malicious software, is a blanket term for software used to wreak destruction and gain access to sensitive information.
4. Herding is the phenomenon of individuals deciding to follow others and imitating group behaviors rather than deciding independently on the basis of their own, private information.
5. A DNS is like a phonebook in that it returns the physical location of website addresses. Once the website is located by the DNS, the internet protocol address of the server is returned with the sought after information.
6. Section 1202 of the Fiscal Year 2018 National Defense Authorization Act provides support to foreign forces, irregular forces, groups, or individuals engaged in supporting or facilitating ongoing or future authorized irregular warfare operations by SOF.
7. A security model based on the principle of maintaining strict access controls and not trusting anyone by default.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

DISCLAIMER

In accordance with 5 CFR 2635.807, the disclaimer certifies the views presented are those of the author and do not necessarily represent the views of DoD, USSOCOM, or its components.

REFERENCES

Army Techniques Publication 3-05.1. (2013). *Unconventional warfare*. Washington, DC: U.S. Department of Defense.

Chenoweth, E., Stephan, M., & Stephan, M. (2011). *Why civil resistance works: The strategic logic of nonviolent conflict*. New York: Columbia University Press.
Darczewska, Jolanta. (2014). The anatomy of Russian information warfare. *The Crimean operation,a case study*. Ośrodek Studiów Wschodnich im. Marka Karpia.
Duggan, P. (2014a, March). UW in cyberspace. *Special Warfare*, *27*(1), 68–70.
Duggan, P. (2014b, January). Man, computer, and special warfare. Retrieved from https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare
Duggan, P. (2016, January). Why special operations forces in US cyber-warfare? *Cyber Defense Review*, *1*(2), 3–79.
Galeotti, M. (2015). "Hybrid war" and "little green men": How it works, and how it doesn't. In *Ukraine and Russia: People, politics, propaganda and perspectives*. Bristol, U.K.: E-International Relations Publishing. https://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/
Hancock, J. T. (2007). Digital deception: why, when, and how people lie online. In Adam N. Joinson, Katelyn Y. A. McKenna, Tom Postmes, and Ulf-Dietrich Reips. (Ed.), *The oxford handbook of internet psychology, pp. 287-301*. Oxford: Oxford University Press.
Harrison, T. (2014). *Chaos and uncertainty: The FY2014 defense budget and beyond*. Washington, DC: U.S. Center for Strategic and Budgetary Assessment.
Irwin, W. (2009). *The Jedburghs: The secret history of the allied special forces, France 1944*. New York, NY: PublicAffairs.
Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., & Oberholtzer, J. (2017). *Lessons from Russia's operations in crimea and Eastern Ukraine*. Santa Monica, CA: Rand Corporation.
Lange-Lonatamishvili, E. (2014). *New face of war: Lessons for Georgia*. Riga, Latvia: NATO StratCom Center of Excellence.
McRaven, W. H. (1996). *Spec ops: Case studies in special operations warfare theory and practice*. New York, NY: Presidio Press.
Meadows, D. (2014, September). Understanding Russia's proxy war in Eastern Ukraine Retrieved from http://euromaidanpress.com/2014/09/14/understanding-russias-proxy-war-in-eastern-ukraine/
Namestnikov, Y. (2009). The economics of botnets. *Analysis on Viruslist. Com*, Kapersky Lab
Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Plymouth, United Kingdom.
Pascoli, S., & Grzegorzewski, M. (2021). Technology adoption in unconventional warfare. *Cyber Defense Review*. forthcoming.
Robinson, G. (2004). *Islamic activism: A social movement theory approach*. Monterrey, CA: Naval Post Graduate School.
Rõigas, H., & Geers, K. (2015). The Ukraine crisis as a test for proposed cyber norms. In T. K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine, pp. 135-144.* : NATO CCD COE Publications.
Scott, J. (2018). *Information warfare: The meme is the embryo of the narrative illusion*. Washington, DC: Institute for Critical Infrastructure Technology Press.
Singer, P. W., & Brooking, E. T. (2018). *LikeWar*. New York, NY: Houghton Mifflin Harcourt.
Swinhoe, D. (2020). How much does it cost to launch a cyberattack? Retrieved from https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html
U.S. Senate, 116th Congress. (2020). *Russian active measure's campaigns and interference in the 2016 U.S. Election*. Washington, DC: Library of Congress.
US Army Special Operations Command. (2019). A Resistance Manual. Fort Bragg, NC: The United States Army Special Operations Command Press.
Volz, D. (2016, February 25). US government concludes cyber attack caused Ukraine power outage. Reuters.