U.S. Command Perspectives on Campaigning in Support of Integrated Deterrence

Editors:

Dr. Belinda Bragg (NSI, Inc.),
Dr. Hriar "Doc" Cabayan (Lawrence Livermore National Laboratory)

May 2023

23-S-2060

SMA Perspectives

Emergent Issues for U.S. National Security

SMA Perspectives Series

The Joint Staff and the United States military adhere to the maxim that effective strategy formulation starts with a proper diagnosis of the environment. This is particularly true when the operational environment has high levels of interactive complexity across various domains. In these settings there are no easy choices, but we know from centuries of experience that the best plans are informed by thoughtful, disciplined exploration of ideas and diversity of thought. In pursuit of this axiom, the volumes in the SMA Perspectives Series are a concerted effort to harvest the informed opinions of leading experts but do not represent the policies or positions of the U.S. government. Our hope is that the ideas presented in this series expand the readers' strategic horizons and inform better strategic choices.

Series Editor

Dr. Hriar "Doc" Cabayan (Lawrence Livermore National Laboratory)

Volume Editors

Dr. Belinda Bragg (NSI, Inc.), Dr. Hriar "Doc" Cabayan (Lawrence Livermore National Laboratory)

Copy Editor

Mr. Nathan Heath (NSI, Inc.)

Editorial Board

Mr. Robert Jones (USSOCOM), Dr. Robert Toguchi (USASOC)

Contributing Commands

USAFRICOM; USCYBERCOM; NORAD and USNORTHCOM; USSOCOM; USSTRATCOM.

Accessing SMA Publications

All SMA reports can be browsed and downloaded from https://nsiteam.com/sma-publications/
For any questions, please contact Ms. Mariah Yager, JS J3, SMA (mariah.c.yager.ctr@mail.mil)

Disclaimers

The views expressed in these papers are those of the individual authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government. The purpose of this series is to expose a range of views and stimulate thinking on ways to address challenges that the U.S. faces.

Mention of any commercial product in these papers does not imply Department of Defense (DoD) endorsement or recommendation for or against the use of any such product. No infringement on the rights of the holders of the registered trademarks is intended.

The appearance of external hyperlinks does not constitute endorsement by the United States DoD of the linked websites, or the information, products, or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

Table of Contents

Executive Summary

Dr. Hriar "Doc" Cabayan
Lawrence Livermore National Laboratory (LLNL)
cabayan1@llnl.gov

The 2022 National Defense Strategy (NDS) states:

> The Department will advance our priorities through integrated deterrence, campaigning, and actions that build enduring advantages. Integrated deterrence entails working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and our network of Alliances and partnerships. Tailored to specific circumstances, it applies a coordinated, multifaceted approach to reducing competitors' perceptions of the net benefits of aggression relative to restraint. Integrated deterrence is enabled by combat-credible forces prepared to fight and win, as needed, and backstopped by a safe, secure, and effective nuclear deterrent. (Austin, 2022)

The 2022 NDS explains that while the Joint Force seeks to deter aggression, it is also campaigning to counter adversary moves short of armed conflict and build enduring military advantage such that adversaries calculate war to be too risky.

In the previous SMA Perspectives volume, "Emerging Strategic & Geopolitical Challenges: Operational Implications for US Commands," contributors from ten military commands provided overviews of the challenges they face in their respective AORs and how they plan to ameliorate the risks and maximize the opportunities that these challenges present. In particular, contributors noted the need for greater understanding of adversaries' interests and priorities and better mechanisms for collaboration across the USG and other stakeholders.

This SMA Perspectives volume builds on these observations and focuses more tightly on how some of these Commands are thinking about campaigning in support of integrated deterrence objectives.

Brief Summary of Key Themes Articulated by the Commands

There is consensus amongst all contributing Commands that there is a need to transition Integrated Deterrence from theory to practice and establish a DoD-wide accepted integrated deterrence framework. There is also consensus that the integration should extend across all domains as a global Joint effort. These include the full spectrum of Defense, interagency, allied, and partner organizations. Toward this end, contributors highlight a number of Command capabilities that support integrated deterrence.

Cyberspace is an indispensable component of U.S. and allied military strength, and thus a core element of integrated deterrence.

The triad of Cyber, Space, and SOF capabilities offers new options for deterrence that will be compelling both in competition and conflict and could manifest in ways that were previously unseen.

Continuous, comprehensive, and coordinated campaigning (such as that done by SOF) actively contributes to integrated deterrence, fosters resilience, and lays the foundation for creating a unique warfighting advantage.

Successful models of interagency cooperation (such as USAFRICOM's work with DoS and USAID) exist and have proved successful in applying the basic premise of integrated deterrence.

Bottom line: Purposeful experimentation and thoughtful reflection are key to providing a basis for future exploratory discussion and debate around the campaigning to achieve integrated deterrence for the nation. Additionally, U.S. and allied capabilities and strategies aside, deep understanding of potential adversary decision calculi and behaviors will be central to successful integrated deterrence.

The sections below briefly summarize each of the contributions from the Commands. The summaries are primarily meant to entice the reader to read the full chapters and have intentionally been kept short.

USAFRICOM

In her article, Ms. Michele Wolfe makes the point that military coups across the African continent can derail long-standing U.S. security cooperation activities. She goes on to state that during such periods, aggressive strategic competitors can take advantage of the gaps created by the suspension of U.S. security assistance programming. To uphold strong African partnerships during such tumultuous times (such as coups), USAFRICOM's 3D approach— Department of State (DoS-Diplomacy), USAID (Development), and USAFRICOM (Defense)— embraces integrated deterrence promoting an agile strategy that allows DoS and USAID to lead in areas where they are best suited and able. She reminds readers that U.S. government whole-of-government approaches that rebalance military efforts with other instruments of national power are consistent with the Pentagon's definition of integrated deterrence, as well as a central part of USAFRICOM's mission.

She concludes by stating that with USAID's humanitarian efforts, DoS communication channels, and USAFRICOM's engagement efforts, the United States applies the basic premise of integrated deterrence and encourages goodwill with affected countries while maintaining its tougher economic and security restrictions.

USCYBERCOM

In their opening paragraph, Mr. Michael Clark, Dr. Emily Goldman, and Dr. Michael Warner state:

> *All instruments of national power today rely on access to cyberspace for their optimal functioning. At the same time, cyberspace itself and the technologies, programs, processes, and human interfaces that comprise it have become vectors through which adversaries can affect and weaken key sources of strategic strength. For these reasons, the Joint Force must take advantage of the opportunities and mitigate the challenges posed by cyberspace if it is to compete effectively with potential adversaries, deter conflict, and wage war if necessary. The very nature of the cyber strategic environment encourages this continual exploitation of opportunity and vulnerability.*

Cyberspace is a dynamic, interconnected domain where friends, rivals, allies, and foes are in constant contact—and in which strategic advantage flows from the cumulative impact of seemingly marginal activities, as well as operations executed in continuous campaigns. Maximizing cyberspace leverage, therefore, requires day-to-day activities to:

- preclude and inhibit any strategic gains that may encourage opponents to challenge the status quo;
- set the conditions for deterrence success should an adversary challenge by initiating a crisis;
- ensure victory in armed conflict, should deterrence fail; and
- contest malicious cyber actors' infrastructure, capabilities, activities, and finances.

The authors argue that "[t]here is no competition, crisis, or conflict in the 21st century that will occur without some cyber element." The nature of cyberspace makes it an indispensable component of U.S. and allied military strength, and cyber capabilities are most impactful in competition when used to defend forward and contest adversary attempts at exploitation.

Accordingly, the cyber arm of the Joint Force has a three-fold task: 1) integrate and leverage cyber power to fight and win across the physical domains of land, air, sea, and space; 2) campaign in and through cyberspace to set favorable conditions to deter in crisis and win in conflict; and 3) persistently campaign in competition where adversaries seek strategic decision outside of armed conflict.

NORAD and USNORTHCOM

In his opening paragraph, Mr. James "JJ" Jenista states:

> *NORAD and USNORTHCOM continue to seek to innovate and accelerate strategies and capabilities that support homeland defense through globally integrated*

> *operations . . . which relies on and leverages a synchronized effort across the full spectrum of Defense, interagency, allied, and partner organizations.*

He goes on to discuss in detail several aspects of this approach:

- understanding potential adversary decision calculi and behaviors
- prioritizing integrated deterrence as a global, all-domain, Joint effort
- using all assets, resources, and authorities across the full suite of partners
- integrating all instruments of national power
- creating asymmetric strategic advantages
- collaborating to develop and implement robust integrated deterrence

In summary, he states:

> *NORAD and USNORTHCOM are working with other Combatant Commands, the Services, and the Joint Staff to fully implement integrated deterrence, not only with an array of partners in the USNORTHCOM AOR, but also as advocates for deterrence across the Defense enterprise and its many external partners. From that perspective, then, the greatest need is for the Combatant Commanders, Service Chiefs, and Joint Staff to prioritize the application of resources toward global integration, mindful of the goal for integrated deterrence. Institutionalized campaigning aims to sustain the advancement of these strategic efforts over time, and General VanHerck (Commander, NORAD and USNORTHCOM) has already initiated this approach within the Headquarters.*

USSOCOM

In his opening paragraph, Mr. Bob Jones quotes USSOCOM CDR General Bryan Fenton's observation that United States Special Operations Forces (SOF) campaigning contribution to a comprehensive scheme of integrated deterrence is "in our DNA" (*Hearing to Consider the Nominations of: Lieutenant General Bryan P. Fenton, USA to Be General and Commander, United States Special Operations Command; and Lieutenant General Michael E. Langley, USMC to Be General and Commander, United States Africa Command*, 2022).

Jones goes on to point out that SOF is at a historic inflection point where ". . . must return to and reembrace their respective roots, and then move wisely and collectively as one to a bold new future whose value is intrinsically clear." He explores a handful of thoughts relevant to this transition and offers a strawman vision and intent for how SOF will campaign in support of our national strategies.

For Jones, SOF's continuous, comprehensive, and coordinated campaigning, "...actively contribute to integrated deterrence, fosters resilience, and lays the foundation for creating a unique warfighting advantage." Based on his own experience, he describes in detail six proposed tenets for effective SOF campaign, underpinned by two foundational elements: 1) a

theory of the problem—the challenge of relevant leadership in an era of shifting power; and 2) a theory of success—Campaigning for Strategic Influence.

He concludes by describing a vision and intent for the SOF forces:

> . . . the essence of how SOF can contribute to integrated deterrence and works to foster the strategic influence necessary to ensure our nation's role well into the future, as leader of a rules-based order designed for an emergent world of shifting power and empowered populations.

USASOC

In his article, Mr. Howard Simkin addresses four key questions:

- How could Irregular Warfare (IW) campaigning support Integrated Deterrence? Simkin lays out several ways, including disrupting the adversary, hardening the environment, resistance, and recovery.

- When should Army SOF take on a leading role in conducting IW campaigning? He addresses this question by stating, "Army SOF should take on a more predominant role in IW campaigning when both support to resistance and unconventional warfare are the main components of the joint force campaign."

- What is different about IW campaigning? Here he states, "IW campaigns depend on Joint, Interagency, Intergovernmental, and Multinational (JIIM) guidance, participation, and integration. DOD normally supports JIIM efforts in IW. Even when they are the lead agency, DOD still depends heavily on its JIIM partners."

- What sort of headquarters should conduct IW campaigns? Here he posits, "For the future joint force, an IW-focused headquarters can be a viable option to conduct IW campaigns."

He goes on to discuss the recent emergence of the converging capabilities and effects of Cyber, Space, and SOF in the competitive security environment, which he considers will offer new options for deterrence, compelling both in competition and conflict. He also notes this convergence could "manifest in ways that were previously unseen and unanticipated by our adversaries" and "help achieve unique trans-regional, multi-domain effects to impose costs on and create dilemmas for our toughest adversaries."

He concludes by stating, "With purposeful experimentation and thoughtful reflection, the answers to questions raised in the article may provide a basis for future exploratory discussion and debate on an issue of vital importance to achieving integrated deterrence for the nation."

USSTRATCOM

In his concluding remarks, Mr. Rich "Lefty" McManus makes the key observation that "it is time to transition the concept of integrated deterrence from theory to practice." He addresses two key issues: 1) how observations led to the revival of "integrated deterrence," and 2) the need for a DoD-wide accepted integrated deterrence framework

By way of background, he makes the case that coordination within the USG and between the U.S. and its allies was key to deterrence success in the Cold War era. In the immediate post-Cold War era, these deterrence integration practices atrophied but are required once again in the current security environment. The emergence of two aggressive nations (Russia and China) capable of contesting military dominance and escalating aggression with any instrument of power or in any domain has driven the revival of integrated deterrence.

Mr. McManus goes on to quote the Undersecretary of Defense for Policy, Dr. Colin Kahl, who highlighted the need to integrate deterrence efforts across 1) the government agencies, 2) allies and partners, 3) geographic areas, 4) all domains, 5) time, and 6) the spectrum of conflict. He highlights the need to relearn integration across the DOD and USG agencies, as well as the challenges ahead. McManus notes that shared deterrence approaches ought to "drive dynamic, and often competing, global and regional priorities". He highlights some key features to developing an integrated deterrence framework:

- orient on decisive influence of decision maker perceptions
- recognize distinct deterrence periods
- combine critical deterrence logics
- allow for the scaling of deterrence to the appropriate level of violence
- drive dynamic, and often competing, global and regional priorities

He concludes by stating, "The revival of integrated deterrence is necessary based on changes in the security environment" and goes on to say that, "the United States and its allies seek to deter armed crisis and armed conflict by convincing potential adversaries they can resolve disputes without force, military aggression will not achieve their desired aims, and the consequences of pursuing military solutions are unacceptably costly."

References

Austin, L. (2022). *2022 National Defense Strategy of the United States of America.* United States Department of Defense. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

Hearing to consider the nominations of: Lieutenant General Bryan P. Fenton, USA to be General and Commander, United States Special Operations Command; and Lieutenant General Michael E. Langley, USMC to be General and Commander, United States Africa Command, 117th Cong. (2022) (testimony of Lieutenant General Bryan P. Fenton). https://www.armed-services.senate.gov/imo/media/doc/22-61_07-21-2022.pdf

United States Africa Command (USAFRICOM)

Ms. Michele Wolfe
Senior Operations Research Analyst, USAFRICOM
michele.k.wolfe.civ@mail.mil

U.S. law, via Section 7008 [1] of the State, Foreign Operations, and Related Program Appropriations Act (SFOAA), restricts various forms of assistance, such as foreign military sales or peacekeeping operations, in the event a military takeover of an elected civilian government occurs. Because there is no waiver for Section 7008, military coups across the African continent can derail long-standing U.S. security cooperation activities. The Department of State (DoS) can restore countries' eligibility for assistance only when they have held elections and a democratically elected government has taken office. While countries work through multi-year processes towards the restoration of democracy, aggressive strategic competitors can take advantage of the gaps created by the suspension of U.S. security assistance programming.

Fortunately, though the law prohibits certain engagements with coup-designated countries, other limited categories of DoS and the U.S. Agency for International Development (USAID) can continue under "Notwithstanding Authorities" for certain programs [2], thereby maintaining relationships and communication avenues with newly established government structures. The Pentagon defines this as "integrated deterrence," where the U.S. government incorporates a whole-of-government approach that rebalances military efforts with other instruments of national power. For the U.S. Africa Command (USAFRICOM), the whole-of-government method is not new. Since its inception more than 10 years ago, this cohesive approach has been a central part of the USAFRICOM mission, which is the defense arm of a "3D" effort to support diplomatic efforts led by the U.S. Department of State and development efforts led by USAID. In the context of integrated deterrence, effective USAFRICOM strategy adjusts according to

---

[1] The latest being the H.R.8282 - Department of State, Foreign Operations, and Related Programs Appropriations Act, 2023, submitted to the 117th Congress (2021-2022), on 1 July 2022.

"Coups D'état. Sec. 7008. None of the funds appropriated or otherwise made available pursuant to titles III through VI of this Act shall be obligated or expended to finance directly any assistance to the government of any country whose duly elected head of government is deposed by military coup d'état or decree or, after the date of enactment of this Act, a coup d'état or decree in which the military plays a decisive role: Provided, That assistance may be resumed to such government if the Secretary of State certifies and reports to the appropriate congressional committees that subsequent to the termination of assistance a democratically elected government has taken office: Provided further, That the provisions of this section shall not apply to assistance to promote democratic elections or public participation in democratic processes: Provided further, That funds made available pursuant to the previous provisos shall be subject to the regular notification procedures of the Committees on Appropriations." See Text - H.R.8282 - 117th Congress (2021-2022), 2022, https://www.congress.gov/bill/117th-congress/house-bill/8282/text

[2] Notwithstanding authorities–activities USAID might use to provide assistance when it would otherwise be prohibited. Examples may be International Disaster Assistance, Health and Disease Prevention, and the Food for Peace Act. https://www.2017-2020.usaid.gov/sites/default/files/documents/200sbs.pdf

the circumstances on the continent, allowing different facets of the U.S. government to take point when necessary so that the United States produces a constant and reliable presence that encourages cooperation.

While the total number of coups that occur in a year has decreased in recent decades, a majority of coups happen on the African continent, West Africa in particular. In Africa, it is often not a question of whether a coup will occur during any given year, but rather where or how many. Since 2021, five successful and three attempted coups have taken place in African nations. Typically, usurpers possess the required strength to seize and hold a government until a stronger force ousts them or until elections replace them from power (Ariel & Ploch Blanchard, 2022). When unable to produce instantaneous change, the usurpers struggle to retain power, as the coup soon devolves into a humanitarian crisis. Unstable countries influence the stability of their neighbors, which consequently incites more coups. External actors, such as Russia's well-known use of private military contractors, add another layer of violence and uncertainty. Therefore, USAFRICOM must plan for the possibility that coups will disrupt military engagements and opportunities across Africa.

Successful coups derail USAFRICOM military activities with the host nation for years to come. In the aftermath of the event, the Secretary of State determines whether Section 7008 applies. If so, it restricts many forms of economic, security, and investment assistance (Harrison, 2022). USAFRICOM works with various African countries on security cooperation activities such as training and exercises. Part of those military-to-military agreements include assessments that the country will use U.S. training and equipment in appropriate ways (e.g., border security, preventing illegal fishing, etc.). If a coup overthrows a country's governmental structure, the military-to-military relationship stops. For example, the recent coup in Burkina Faso halted many of the planned military-to-military engagements for subsequent months[3]. If USAFRICOM did not incorporate a whole-of-government approach, contacts could atrophy or be replaced. Strategic competitors might then use the U.S. absence to their advantage, acknowledging the new regime and gaining agreements such as fishing rights or arms sales. In this author's opinion, when the country returns to a state in which U.S. military-to-military engagements can continue, the relationship reignites one of three states:

- Contacts who have past experience working with U.S. security assistance wish to re-engage;
- New contacts with no memory of previous military-to-military engagements require a restart of the relationship from scratch; or

---

[3] Where authorities permit, the United States remains committed to supporting the Burkinabe people in their struggles for accountable governance, security, and stability. Due to the military coup d'état in January 2022, foreign assistance including security assistance to the Government of Burkina Faso is restricted pursuant to Section 7008 of the annual appropriations act. In recognition of the continued threat posed to Burkina Faso by violent extremist groups, certain security assistance programs, primarily law enforcement, are continuing under available authorities.

- Contacts who turn away from U.S. involvement and turn, or have already turned, to strategic competitors.

Via any of these states, many processes, such as joint exercises or foreign military sales, may face the need to restart entirely. Coups can devastate U.S. military avenues within a country, and the consequences can far outlast the events themselves.

Coups prohibit most USAFRICOM plans, but DoS and USAID have different restrictions. To excerpt the Congressional Research Service Report on Coup-Related Restrictions:

> *"Section 7008 explicitly exempts aid to promote democracy.*
>
> *The restriction also has generally not applied to*
>
> - *aid fully implemented by nongovernmental organizations rather than the government,*
>
> - *aid authorized or appropriated "notwithstanding" any other provision of law, which in FY2021 includes most humanitarian assistance; funds provided through the Assistance for Europe, Eurasia, and Central Asia (AEECA) account; aid to some specific countries (e.g., Egypt and Pakistan, along with certain aid for Sudan); and aid for some specific purposes (e.g., counter-narcotics, counter-crime, and anti-terrorism), or*
>
> - *aid the President has authority to provide in certain conditions notwithstanding restrictions in law, subject to congressional notification." (Text - H.R.8282 - 117th Congress (2021-2022), 2022)*

Aid is a dire need throughout much of Africa; as such, the U.S. government usually allows health and humanitarian assistance efforts to proceed during a military coup, with appropriate caveats. As the lead for development, USAID's persistent presence helps to lessen the effects from the Section 7008 reduction in military security cooperation. According to ForeignAssistance.gov, in the past year, USAID continued to plan and execute humanitarian programming for the Burkinabe and Malians in addition to longer-term development programs focused on health, education, and food security (U.S. Agency for International Development (USAID) and U.S. Department of State on behalf of United States Government agencies reporting foreign assistance., n.d.). By maintaining USAID's persistent presence, the U.S. reduces the negative connotations from the Section 7008 reduction in military-security cooperation.

As the lead for diplomacy, ambassadors and their teams promote U.S. policy aimed at a peaceful return to a civilian government with free and fair elections as swiftly as possible. Their in-country involvement can catalyze high-level meetings that promote transition and convey the United States' continued interest. The DoS and other interagency members remaining in country reaffirms the U.S. commitment to the partner nation and can help to refute assertions by strategic competitors that the United States has abandoned the country.

In the same vein, USAFRICOM does possess a less restricted avenue to continue USAFRICOM military-to-military relationships. USAFRICOM can apply face-to-face engagements and other non-military avenues to maintain ties. Powerful permitted activities include naval port visits and senior leaders' visits in country for one-on-one meetings with the government's leadership. Senior DoD leaders can reinforce diplomatic messaging on the importance of peaceful elections and convey eagerness to renew military assistance. With USAID's humanitarian efforts, DoS's communication channels, and USAFRICOM's engagement efforts, the United States applies the basic premise of integrated deterrence and encourages good will with the country while maintaining its tougher economic and security restrictions.

It could be argued that these efforts are either not enough or too much during a coup. Some may say that if a country destabilizes, the United States should cut ties completely. Another critique might claim that additional military involvement would assist the country in getting back on its feet more quickly. Either way, it is a knife's edge.

To argue the former: Cutting ties completely implies the United States either never wishes to re-engage with the country or that Washington is content to reinvest incredible time, money, and effort into the country when/if it climbs out of its coup-torn state. This severing opens avenues for strategic competitors such as Russia and China. Terrorists recognize unstable countries as potential safe havens, creating further chaos in an already turbulent place. After these influencers intervene and the country is fortunate enough to restore democracy, then Washington must contend with competing adversarial nations and/or systemic violent extremism.

To argue the latter: If the U.S. exerts military efforts to assist in the country's stabilization, then the United States could become embroiled in an unhealthy political situation. The international community would accuse the U.S. government of developing a puppet state or even attempting a takeover. The history between the Western world and African nations connotes resentment of any foreign power, but especially Western power, which exerts too much influence. The French exit from Mali provides a recent example, but the United States bears its own examples, in which military aid turned into resentment and then into painful extractions. The United States does not do well politically with long, drawn-out conflicts.

When a coup affects a country, U.S. law dictates specific restrictions to operations in that country, but the whole-of-government approach aims to ensure continuity to help USAFRICOM continue to work toward its strategic defense goals. The United States maintains consistency in its reactions to coups—the in-house government understands the why (we do not arm or train coup-led governments) and the how (e.g., returning to free and public elections), which facilitates a return to a more congenial state. In the meantime, non-military oriented and more humanitarian-focused efforts continue so that contacts and good feelings endure. The fluidity between the DoS (Diplomacy), USAID (Development), and USAFRICOM (Defense) allows the United States' strategy to absorb violent distraction, such as coups, and adapt interactions accordingly. Therefore, to uphold strong African partnerships during

tumultuous times, USAFRICOM's 3D approach embraces integrated deterrence, promoting an agile strategy that allows DoS and USAID to lead in areas where they are best suited and able.

References

Arieff, A. and Ploch Blanchard, L. (2022). *"An epidemic of coups" in Africa? Issues for Congress.* Congressional Research Service. https://crsreports.congress.gov

Harrison, S. (2022, February 23). *The complexities of calling a coup a coup*. Lawfare. https://www.lawfareblog.com/complexities-calling-coup-coup

Text - H.R.8282 - 117th Congress (2021-2022): Department of State, Foreign Operations, and Related Programs Appropriations Act, 2023, 8282, United States House of Representatives, 117 (2022). http://www.congress.gov/

U.S. Agency for International Development (USAID) and U.S. Department of State on behalf of United States Government agencies reporting foreign assistance. (n.d.). *ForeignAssistance.gov.* https://foreignassistance.gov/

United States Cyber Command (USCYBERCOM)

Mr. Michael Clark
Director of Cyber Acquisition and Technology, U.S. Cyber Command
michael.a.clark67.civ@mail.mil

Dr. Emily Goldman
Strategist, U.S. Cyber Command
eogoldm@cybercom.mil

Dr. Michael Warner
Command Historian, U.S. Cyber Command
mwarne2@cybercom.mil

All instruments of national power rely on access to cyberspace for their optimal functioning. Digital networks and data enable the political, economic, diplomatic, military, and intelligence exercise of power. At the same time, cyberspace itself and the technologies, programs, processes, and human interfaces that comprise it have become vectors through which adversaries can affect and weaken key sources of strategic strength. For these reasons, the Joint Force must take advantage of the opportunities and mitigate the challenges posed by cyberspace if it is to compete effectively with potential adversaries, deter conflict, and wage war if necessary.

Decades ago, adversaries recognized America's dependence on digital data and networks and started working in and through cyberspace to impact vulnerable sources of national power (both in the United States and other countries). They developed capabilities to exploit American intellectual capital, to compromise the privacy and thus the security of individual Americans, and to impugn the legitimacy of America's institutions (to citizens, allies, and creditors). By doing so, they hoped to erode U.S. economic power, political stability, and military overmatch—and to do so without resorting to armed conflict. The very nature of the cyber strategic environment encourages this continual exploitation of opportunity and vulnerability.

Despite diplomatic, economic, law enforcement, military, and intelligence efforts over the last generation, this erosion has not been deterred and has not stopped. Indeed, the lack of powerful responses by the United States and allied nations seemingly emboldened adversaries in cyberspace. Several Presidents and Congresses have therefore agreed that significantly improved military cyberspace capabilities based in the Department of Defense must be sustained and employed against adversaries to counter their cyber campaigns, to help deter armed conflict, and, should deterrence fail, ensure the Joint Force can fight and win. If the nation is ineffective in cyberspace, it cannot succeed in strategic competition, crisis, or deterrence of armed conflict.

Integrated Deterrence

The 2022 *National Defense Strategy* revolves around the concept of Integrated Deterrence. It calls for seamless operations across domains, theaters, and the spectrum of conflict, leveraging non-military tools, buttressed by partners, and supported by network integration. The *Strategy* explains that while the Joint Force seeks to deter aggression, it is also campaigning to counter adversary moves short of armed conflict and building enduring advantages to sustain the military strength that convinces adversaries war is too risky.

Cyberspace is an indispensable component of U.S. and allied military strength, and thus a core element of integrated deterrence. Cyber capabilities and forces provide mission assurance for Joint Force operations. They are essential to assuring command and control; to defending Department of Defense Information Networks (DODIN) and coalition warfighting networks; and to securing weapons systems, platforms, military-critical infrastructure nodes such as ports, and the defense industrial base (DIB). Working with partners, which is central to integrated deterrence, cannot occur without secure networks for sharing actionable intelligence and conducting combined operations.

Integrated deterrence recognizes that our adversaries have holistic strategies and that the U.S. military requires its own holistic approach to secure American interests and advance national goals. Accordingly, it strives to optimize the use of all instruments of military (and national) power.

Many military capabilities, of course, have utility short of armed conflict and, in conjunction with other instruments of national power, can bolster integrated deterrence, as the *National Defense Strategy* suggests. The United States has long leveraged its nuclear and conventional capabilities to support deterrence by *threatening their use* against aggressors. Rather than being held in reserve as additional threats for reactive strikes if deterrence were to fail, however, cyber capabilities are most impactful when *used* in competition to defend forward and contest adversary attempts at exploitation. Such operations can also have the effect of setting conditions for deterrence, crisis management, and, if necessary, prevailing in conflict. In short, they help build the enduring advantages called for in the *National Defense Strategy*.

To understand this concept, it is essential to plan based on the reality of cyberspace as a dynamic, interconnected domain where friends, rivals, allies, and foes are in constant contact—and in which strategic advantage flows from the cumulative impact of seemingly marginal activities and operations executed in continuous campaigns. This point is crucial. In the other warfighting domains—land, air, sea, and space—contact with adversaries is more or less episodic, and strategic decision virtually always occurs in armed conflict. In cyberspace, strategic decision can occur in competition. Therefore, maximizing cyberspace leverage requires *persistence* in day-to-day activities to preclude and inhibit opponents' strategic gains that may encourage them to challenge the status quo, to set the conditions for deterrence success should an adversary challenge by initiating a crisis, and to ensure victory in armed conflict should deterrence fail.

Campaigning

For the past several decades, before the Department of Defense identified China as our pacing threat, U.S. adversaries have run campaigns in cyberspace to influence elections; spread disinformation; circumvent sanctions; disrupt supply chains; and steal intellectual property, military research and development, and personally identifiable information. Our adversaries recognize that cyber capabilities have distinct value when employed in competition against opponents because they can achieve strategic gains without escalating to militarized crisis or armed conflict. Of particular importance for the Joint Force, continuous cyberspace campaigns targeting the U.S. defense industrial base and manipulating the global financial infrastructure for sanctions evasion have eroded U.S. military overmatch, which underpins integrated deterrence. Campaigning to contest malicious actors' infrastructure, capabilities, activities, and finances is key to thwarting the cumulative strategic gains adversaries have been reaping at our expense.

The *National Defense Strategy* calls for campaigning in competition below armed conflict to "improve our position and reinforce deterrence while limiting, frustrating, and disrupting competitor activities that seriously affect U.S interests, especially those carried out in the gray zone" (Austin, 2022). Campaigning aligns well to operating in cyberspace, where change is constant, opportunity is fleeting, superiority is temporary, and advantage favors those with initiative. Lessons learned since 2018, when U.S. Cyber Command gained greater authorities to operate, show that campaigning is the "essential way" to employ cyberspace capabilities and forces for strategic effect across the competition-conflict continuum.

Campaigning is how U.S. Cyber Command operates. In 2018, the Command adopted the operational approach of persistent engagement to give the U.S. the cyber initiative in contests with real and potential adversaries. Persistent engagement means employing a continuous operational tempo that seizes and maintains the initiative to compete and set favorable security conditions in and through cyberspace and the information environment necessary to secure, defend, and advance U.S. strategic goals. Persistent engagement involves enabling and acting in a domain of continuous activity where there is no operational pause. In cyberspace, security rests on our ability to *continuously* anticipate how adversaries will seek to exploit our vulnerabilities and, if necessary, how we can exploit theirs. The insights that result from sustaining such anticipation make the Joint Force more effective and adversaries less capable and confident in cyberspace. Persistence sets conditions in our favor so that we both succeed in deterrence and win in competition.

Campaigning enables U.S. Cyber Command to generate insights, opportunities, and options that constrain adversaries' freedom of maneuver and deny them leverage in crisis and conflict. When cyber forces hunt forward on partner networks, tip industry, publicize malign activity, and expose malware, they preclude options, reduce attack vectors, and deny terrain to malicious actors.

Doing so in competition further supports integrated deterrence by boosting the credibility of the nation's whole-of-government posture to deter and, if necessary, respond. Cyber forces secure and enable Joint Force deterrent and warfighting capabilities. On order, cyber forces support the resilience (redundancy, rapid recovery, and restoration) of other instruments of national power so they can be applied effectively to deter and respond. When U.S. Cyber Command enables partners, it boosts their warfighting credibility as well.

Finally, campaigning sets favorable conditions for the Joint Force in contingency by undermining the adversary's desired crisis and war conditions. Operations that deny initiative, constrain options, reduce capacity, and erode confidence complicate competitors' military preparations and sow doubt in the ability to achieve a military *fait accompli* or prevail in a war of attrition. Continuously generating organizational friction through cyberspace operations diminishes adversaries' trust in their people, capabilities, tactics, and tools. Keeping adversaries off-balance and focused inward diverts time, talent, and treasure from warfighting preparation. Campaigning in and through cyberspace confers other benefits as well. It can degrade competitor warfighting capabilities. It thwarts malicious information campaigns aimed at undermining U.S. political will and eroding alliance cohesion. It can also deny the adversary coercive power in crisis and conflict by helping detect, mitigate, and remove malware from U.S. and partner critical infrastructure.

Cyber capabilities can operate with great speed and agility, but such attributes usually must be developed and deployed over months or even years. As a result, U.S. Cyber Command has learned from recent events that in cyberspace, crisis and contingency operations are "come as you are," with limited ability to provide new options at the speed of operational relevance. Therefore, building enduring advantages and generating cyber response options for crisis management and conflict must begin with campaigning in day-to-day competition. Balancing the resource commitments to continuous campaigning below armed conflict with patient capabilities development for options in support of armed conflict is a key challenge for the Joint Force. There is a symbiosis between them, but understanding and optimizing them remains a work in progress for the Department of Defense.

Progress through learning by doing has also revealed the integrating role U.S. Cyber Command operations can play with governmental, private sector, and international partners. True integrated symbiosis has occurred between the Command and the National Security Agency, advancing the nation's capacity to seize and sustain the initiative in cyberspace. Alignment with critical private sector companies has produced a capacity for anticipatory resilience at home while greater cooperation abroad has created defend and hunt forward operational advantages that seize back initiative and unbalance opponents.

Conclusion

We live in a digital age. There is no competition, crisis, or conflict in the 21st century that will occur without some cyber element. Strategic competitors present an array of challenges to the United States, undermining our nation's strengths by exploiting our cyber vulnerabilities.

They engage in various forms of malign behavior, coercion, and aggression against the United States and its allies (though so far below the threshold of armed conflict). Cyberspace is a major arena in this strategic competition because the terrain features poorly defended resources, and campaigns of theft, disruption, and disinformation have produced strategic gains without the risks that accompany the use of force.

Effective military power today cannot be exercised and employed at scale without cyberspace support. Cyber capabilities, forces, and operations are essential to winning in competition, to achieving integrated deterrence, and to maintaining superiority across all other warfighting domains. Cyberspace and the electromagnetic spectrum will be vigorously contested as adversaries strive to control the information high ground and shape conditions to their advantage in crisis and conflict. The United States cannot afford to cede initiative in cyberspace. Nor can we fall behind adversaries who are less constrained, more risk acceptant, and who have been campaigning to win in competition.

National defense is no longer (if it ever was) simply a matter of deterring or winning in armed conflict. It is also about winning in strategic competition with nuclear-armed and autocratic adversaries when war could be apocalyptic. Accordingly, the cyber arm of the Joint Force has a three-fold task: 1) integrate and leverage cyber power to fight and win across the physical domains of land, air, sea, and space; 2) campaign in and through cyberspace to set favorable conditions to deter in crisis and win in conflict; and 3) persistently campaign in competition where adversaries seek strategic decision outside of armed conflict.

References

Austin, L. (2022). *2022 National Defense Strategy of the United States of America.* United States Department of Defense. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

North American Aerospace Defense Command (NORAD) and United States Northern Command (USNORTHCOM)

Mr. James M. Jenista
Special Advisor to the Director, NORAD & USNORTHCOM J7
james.m.jenista.civ@mail.mil

Introduction

Homeland Defense is the first priority in the National Defense Strategy (NDS). The separate but inseparable North American Aerospace Defense Command's (NORAD) and United States Northern Command's (USNORTHCOM) approach to Homeland Defense is to assert a leadership role to innovate and accelerate strategies and capabilities that enable and enhance globally integrated operations. The Commands leverage "institutional campaigning" to advance and embed the requisite operational mindset into all aspects, actions, activities, and processes necessary to advance NDS objectives. Cooperation and a unity-of-effort-focused approach among allies and partners are key enablers to institutional campaigning. This is accomplished by translating a campaign and its intermediate actions and milestones into the context of a partner's existing procedures, such that collaborative efforts can advance more quickly in a shared framework and lexicon.

NORAD and USNORTHCOM's combined strategy establishes a broad integrated deterrence capability through synchronized efforts across the spectrum of Defense, U.S. government, allied, and partner organizations. NORAD and USNORTHCOM's chapter in the June 2022 SMA Perspectives paper, "Emerging Strategic and Geopolitical Challenges: Operational Implications for US Commands," (United States Joint Staff, Strategic Multilayer Assessment Office, 2022) introduced integrated deterrence. The following key elements warrant additional detail:

- Understanding potential adversary decision calculi and behaviors is essential to understanding how to implement integrated deterrence.
- Integrated deterrence is not constrained by geography; it entails the Joint Force working seamlessly across military domains, theaters, and the spectrum of conflict...
- ...and the USG using all available assets, resources, and authorities across the interagency, allies, partners, NGOs, and private industry.
- Integration of the instruments of national power to include military, economic, informational, and diplomatic;
- Creation of asymmetric strategic advantages for the nation; and
- Collaborative development and implementation of integrated deterrence across the USG and other stakeholders

Understanding the Adversary

In his March 2022 testimony before the Senate Armed Services Committee, General Glen D. VanHerck, Commander NORAD and USNORTHCOM, identified our competitors and potential adversaries:

> *Today, strategic competitors, rogue nations, [and] nonstate actors possess the capability to strike institutions and critical infrastructure in the United States and Canada. Our country is already under attack every day in the information space and the cyber domain. Our competitors, especially Russia and China, are spreading disinformation, actively sowing division and internal discord with the intent to undermine the foundation of our nation, our democracy, and democracies around the world. (VanHerck, 2022)*

We can infer that our competitors are not deterred by our current defense posture, calculating that engaging in activities such as those listed in General VanHerck's statement is worth the risk (and cost) of what they perceive to be our likely response. Thus, to dissuade further malign activities, we can change one or both sides of the equation: innovate our defensive agility to increase the resources a competitor must commit to reach a given objective, or increase the competitor's perception of our expected response to one that exceeds the value of reaching their goal.

The latter option tends toward an escalation of threats and counter-threats, whereas the intent is to deescalate away from crisis or conflict. Accordingly, NORAD and USNORTHCOM are concentrating instead on a Homeland Defense Design focused on advantages gained through integrated deterrence, including gathering, analyzing, and exploiting existing sensor data that can be shared between allies and partners to increase domain awareness and expand the decision space available to senior leaders. Adversaries will find it more difficult to find and exploit vulnerabilities, significantly increasing the investment of resources necessary for success.

Since our competitors' efforts, such as the PRC's Belt and Road Initiative, are global in scope and long-term on the time scale, the Department of Defense must accelerate its own globally integrated approach to resource prioritization and allocation and sustain it in a way that endures across the many shorter planning, budgeting, and execution cycles with which we are familiar. The challenge to stay the course is significant, and indeed our competitors are counting on us to frequently change plans and lose momentum.

All-Domain Approach

Global integration is, of course, about much more than geography, yet the theater and regional approach to defense remains DoD's framework to break the global challenge into manageable chunks, grouped by countries and convenient natural boundaries. But integrated deterrence for the Homeland, to be most effective, implies integrated deterrence beyond the

Homeland, i.e., beyond the USNORTHCOM Area of Responsibility (AOR). Thus, the USNORTHCOM Commander has a vested Homeland Defense mission interest in decisions in forward theaters that include kinetic, non-kinetic, and deterrent options. As General VanHerck remarked in 2022, sensor to shooter, or even just sensor to decision-maker, is too late, as it carries significant risk of devolving to crisis or conflict; what he needs, he explained, is the practical equivalent of "sensor to deterrent options" (*Statement of General Glen D. VanHerck, United States Air Force, Commander, United States Northern Command and North American Aerospace Defense Command,* 2022) to leverage all-domain awareness, information dominance, and decision superiority to deter aggressors and preserve—or return to—competition.

The same principles apply where the physically distinct characteristics of domains (land, air, maritime, space, and cyberspace) and Service control of sensor platforms have led to difficulty sharing data and gaining insights available through true integrated deterrence. As we move forward to implement a Department-wide digital strategy and framework—and the Chief Technology Innovation Officer (CTIO) at NORAD and USNORTHCOM has developed a digital strategy implementation plan in close coordination with the DOD Chief Digital and Artificial Intelligence Officer (CDAO)—we will simultaneously break down both geographic- and domain-specific barriers and unlock an order of magnitude in greater interoperability.

As noted earlier, integrated deterrence at all-domain scope and global scale, oriented toward the cooperation/competition end of the spectrum of engagement and away from the crisis/conflict end, is challenging, as well as counter to the way DOD is organized. It requires leaders of domain-oriented Services, geography-oriented geographic combatant commands, and function-oriented functional combatant commands to bring their capabilities, resources, and decision vectors to bear and align to the maximal deterrent course of action. Headquarters NORAD and USNORTHCOM has hosted a series of recent wargames to demonstrate the effectiveness of this approach to data integration, the Global Information Dominance Experiments or GIDE, which CDAO is now taking forward to encourage data integration and use across not just the Department but the full partnered enterprise for integrated deterrence.

Institutionalized Campaigning

It is one thing to institute global integration in support of integrated deterrence, and quite another to sustain it over time amid changes in leadership, economic conditions, and even climate. To meet the challenge, General VanHerck has turned to the well-developed concept of a campaign and applied it much more broadly than in its traditional operational context. In his March 2023 posture statement, he explains:

> *The feasibility of every other Geographic Combatant Command's plans will require active campaigning in and from North America, and successful defense of the homeland is necessary to deter adversaries and assure allies and partners. Therefore, I have also directed that USNORTHCOM and NORAD prioritize homeland defense campaigning to demonstrate our readiness, capabilities, and resiliency. (Statement of*

General Glen D. VanHerck, United States Air Force, Commander, United States Northern Command and North American Aerospace Defense Command, 2023)

Institutionalized campaigning provides the continuity necessary to maintain strong, reliable relationships with partners, among its other features. For example, partnerships with community emergency responders, NGOs, private sector companies, and Tribal authorities forged during responses to natural disasters are an important component of enduring Domestic Resiliency, which in turn enhances Homeland Defense.

The institutional approach to campaigning begins across the Joint Directorates within Headquarters NORAD and USNORTHCOM, including, for example, how exercises are designed, planned, and executed, where the institutional effort is then extendable upward and outward, enabling large-scale exercises with the full complement of external partners, resulting in an enhanced deterrent effect toward the PRC and Russia.

Integrated National Power

A resilient public and private infrastructure, and the hardy populace that both relies on and operates that infrastructure, ensures a core economic engine that can withstand devastating and extended impacts, such as the COVID-19 pandemic. Resiliency's deterrent effect, reinforced across partnerships aligned shoulder to shoulder both here and abroad, causes a competitor to reassess the full cost of trying to undermine national will, and thus contributes to a successful "deterrence by denial" posture to protect our Homeland and that of each of our allies and partners.

And while national policies, treaties, and other state-level agreements are beyond the direct purview of senior military leaders, Combatant Commanders must still champion for necessary and appropriate support for integrated deterrence at the state level. Over a period of several years, for example, Commander NORAD advocated for updating NORAD defense infrastructure in Canada, and the Minister of National Defence announced in June 2022 that $38.6B will be applied to NORAD modernization projects in Canada over the next 20 years.

Asymmetric Strategic Advantage

In a global competitive environment, in which our potential adversaries do not adhere to the same ethical standards we impose on ourselves, we would consistently lose ground, were it not for our own strategic advantages. Chief among these are our relationships with partners and allies, based on mutual trust and reciprocal security benefits. Still, they are not static but require nurturing; in his 2022 Posture Statement, General VanHerck stated, "[W]e must continue to foster the partnerships and alliances that provide the United States and our international partners with what is perhaps our most distinct asymmetric advantage."

The NORAD Bi-National Agreement with Canada, the Canada-US Combined Defense Plan, and the Canada-US Civil Assistance Plan are representative of one of the closest military partnerships in existence. This does not mean, however, that the U.S. is aligned with Canada

on every issue, such as, for example, on the designation of maritime territorial waters. But the strength of the relationship—and the cornerstone of building coalitions that successfully work together for integrated deterrence—is the emphasis on common ground for common defense, as well as simultaneous acknowledgement of and respect for differences.

A third source of strategic asymmetric advantage, based on a level of individual personal freedom far more expansive than for the populations of our peer competitors, is robust innovation, resourcefulness, and adaptability, whether in the face of adversity or on the doorstep of opportunity. These quintessential American traits, also evident among the citizens in many of our free-society allies and partners, drive much of the technological advancement and economic prosperity that contribute, as noted, to Domestic Resilience and, through its deterrent effect, to Homeland Defense. And, of course, military members exhibit similar characteristics, a tactical and operational advantage that can also support strategic agility and adaptation across the entire Defense enterprise.

Collaborative Development

Finally, a natural extension of individual freedom is the opportunity to collaborate with others to develop initiatives at scale and to accelerate their implementation through unfettered teamwork structures. As integrated deterrence expressly describes a synchronized partnership-based effort, the same teamwork is necessary to anticipate a competitor's new capabilities and adopt innovative solutions ahead of the competitor's deployment timeline. A few examples of this in practice include the spiral development of missile defense systems by the Missile Defense Agency (MDA) even while USNORTHCOM deployed them to the field; the now-standard modularized, verbal, initial approval Request for Assistance (RFA) process for Defense Support of Civil Authorities developed between FEMA and USNORTHCOM; establishment of the Domestic Event Network between FAA and NORAD for rapidly developing air events; and refinement of field support teams between DHHS and USNORTHCOM during COVID-19, adapted to USNORTHCOM support of the Department of State (DOS) for Operation ALLIES WELCOME.

Summary

NORAD and USNORTHCOM are working with the other Combatant Commands, the services, and the Joint Staff to fully implement integrated deterrence, not only with an array of partners in North America, but also as advocates for deterrence across the Defense enterprise and its many external partners. From that perspective, then, the greatest need is for the Combatant Commanders, Service Chiefs, and Joint Staff to prioritize the application of resources toward global integration, mindful of the goal for integrated deterrence. Institutionalized campaigning aims to sustain the advancement of these strategic efforts over time, and General VanHerck has already initiated this approach within the Headquarters.

References

Fact sheet: Funding for continental defence and NORAD modernization. (2022, July 21). Government of Canada. https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/facesheet-funding-norad-modernization.html

Statement of General Glen D. VanHerck, United States Air Force, Commander, United States Northern Command and North American Aerospace Defense Command, 117th Cong. (2022) (testimony of General Glen D. VanHerck). https://www.armed-services.senate.gov/imo/media/doc/USNORTHCOM%20and%20NORAD%202022%20Posture%20Statement%20FINAL%20(SASC).pdf

Statement of General Glen D. VanHerck, United States Air Force, Commander, United States Northern Command and North American Aerospace Defense Command, 118th Cong. (2023) (testimony of General Glen D. VanHerck). https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/03.08.23%20VanHerck%20Statement.pdf

VanHerck, G. D. (2022). *The NorthStar*. NORAD & USNORTHCOM.

United States Special Operations Command (USSOCOM)

Strategic Influence — Campaigning Holistically in Peace, Crisis, and War

Mr. Robert C. Jones
USSOCOM Donovan Integration Group
robert.jones@socom.mil

"Special Operations Forces were born for where we are right now," declared (then) Lieutenant General Bryan Fenton in response to questioning during his Senate confirmation hearing.[1] He went on to explain in concise terms how the type of campaigning required of United States Special Operations Forces (SOF) to "compete and contest" and to balance our counterterrorism (CT) capabilities with our vital contribution to a comprehensive scheme of integrated deterrence was "in our DNA."[2]

The ultimate result of this type of campaigning is to create what is in effect "a ubiquitous SOF presence." In this context, *Presence* is far more than physically being in the places where our interests are challenged most. Perhaps more importantly it means being near the "hearts" of those who would work with us to advance and secure a rules-based order designed to serve the interests of all, as well as inside the "minds" of those seeking to disrupt that system to advance their own self-serving agendas. This is the type of campaigning referred to by Lieutenant Colonel T.E. Lawrence as being ". . . far more intellectual than a bayonet charge" (Lawrence, 1926).

It is worth a moment to explore what exactly General Fenton might mean when he speaks of "our DNA."[3] For while U.S. SOF has a collective DNA, it is one made up of a sophisticated blend of unique genetic pools from across the SOF enterprise, our allies, and our partners. Like most commanders of United States Special Operations Command (USSOCOM), General Fenton comes here from the command of Joint Special Operations Command (JSOC). During the height of our post-9/11 response, USSOCOM's commanders tended to come from the SEAL community, where the DNA is rooted in exquisite capabilities in Special Reconnaissance (SR) and Direct Action (DA), and most predominantly from our magnificent Ranger Regiment, where the DNA is that of elite infantry assaults and raids. This was the perfect aspect of SOF DNA for the problem as it was understood at that time, as well as for the solutions SOF was asked to provide. General Fenton, however, is from our Army Special Forces Regiment—a "Green Beret." This DNA is markedly different. Equally important is his rich breadth of senior level experiences over the past several years. It is this unique blend of background and

---

[1] See *Hearing to Consider the Nominations of: Lieutenant General Bryan P. Fenton, USA to Be General and Commander, United States Special Operations Command; and Lieutenant General Michael E. Langley, USMC to Be General and Commander, United States Africa Command,* 2022.

[2] Ibid.

[3] Ibid.

experiences that will frame how he perceives the complex diversity of challenges SOF must evolve to effectively face.

This is primarily the Army SOF DNA that dominated the population-based activities of the Cold War era, from the jungles of Vietnam to the back alleys of Berlin. While few see the current competition as a new Cold War, the emphasis for SOF is very similar. Yes, SOF will campaign holistically for strategic influence and to foster resilience in peace. Yes, SOF will posture for no-fail crisis response. Yes, SOF will work through diverse populations and with a sophisticated network of partners and allies to seek warfighting advantage. Yes, SOF will "balance CT and deterrence."[4] All of this is indeed embedded in our SOF DNA, and the confirmation of a Green Beret with deep experience in Asia and a vision to foster a ubiquitous SOF presence to lead that effort is no accident. As LTG Braga, the Commander of United States Army Special Operations Command (USASOC) points out, "we cannot overestimate the value of generational relationships in providing asymmetric advantages, or for their contributions to an over-arching scheme of integrated deterrence and the defense of the homeland." Now is the time to refresh, refocus, and expand these relationships for modern purpose.

Summary

Like much of the Joint Force, SOF is at a historic inflection point. Some organizations have proven particularly adept at optimizing these points in time. At Apple, there existed a corporate philosophy that helped them to stay on the leading edge of an incredibly competitive technology field—"to abandon successful products, and flee into the future" (Apple representative at SOCOM Sovereign Challenge event, personal communication, circa 2011/2012). Apple used the iPod to iterate small advances in technology each year, both to increase sales and to prepare the marketplace for the remarkably innovative iPhone. Once they felt the marketplace was ready, Apple destroyed the lucrative iPod market and fled to the iPhone. Over the past 14 years we have seen a similar iterative process with the iPhone. Is Apple preparing to once again "flee into the future"? Or have they become wed to a successful product that brought them to where they are today? Today, SOF finds itself in a similar situation.

Has JSOC, and our CT capabilities in general, become our "iPhone"? Have we become overly wed to a tremendous capability that is the result of 20 years of incremental advances and has become a primary focus of much of the force? Will we continue to iterate to improve what brought us to where we are? Or will we realize we've focused too fully on one aspect of our mission at the expense of others? Now is the time for SOF to build upon what we have learned and make a bold shift toward what the challenges of the future demand. Though even bold change must be moderated. A renowned industrial designer, Raymond Loewy, advocated that change must be clearly tied to what people know and expect. The best designs are "most

---

[4] Ibid.

advanced, yet acceptable" (Dam, 2021)—pushing the boundaries of change, but not so far that others cannot still see what they comfortably expect. Apple is a master of MAYA. So, putting a slight twist on Apple's axiom, the various SOF tribes must *return to and reembrace their respective roots, and then move wisely and collectively as one to a bold new future whose value is intrinsically clear.*

This paper explores a collection of thoughts relevant to this transition. First are a family of proposed tenets for SOF campaigning. SOF has long framed itself around well-established "truths" and "Core Activities" (SOF Truths, n.d.; SOF Core Activities, n.d.). The truths are virtually carved in stone, and the latter are a matter of Federal Law. What SOF does not have is a family of tenets to guide how and why we campaign. Offered next is a theory, or perhaps more accurately, a hypothesis. The primary difference between a plan and a strategy is that a strategy is rooted in theory. While higher guidance provides an overarching framework, here we apply a SOF-unique lens to propose a theory of the problem and theory of success refined for the aspects of challenges best suited to special operations campaigning. Lastly is an attempt to pull it all together and offer a strawman vision and intent for how SOF will campaign in support of our national strategies.

Tenets of SOF Campaigning

One can turn to doctrine to learn how SOF operates. Joint Publication 3-05, "Special Operations," (SO) effectively describes how SOF operates across the spectrum of conflict *in "...support of specific theater or national objectives, the majority of SO are designed and conducted to enhance the likelihood of success of the overall theater campaign. SO must complement—not compete with nor be a substitute for—conventional operations"* (United States Joint Staff, 2003, p. I-1). But what are the special operations relevant to modern challenges? It has become increasingly important to consider in greater detail, not just how SOF "operates," but how SOF *campaigns*—holistically and globally, day in and day out—in support of national objectives.

In some ways, "campaigning" is a bit of a misnomer. While I believe SOF should campaign *for* strategic influence, there are many things against which this type of SOF campaigning should carefully guard. For example, it is hard to imagine a role for large, deployed SOF headquarters or named operations replete with broad authorities and permissions. While these mechanisms absolutely served to facilitate tactical action, such power and freedom came too often at the cost of achieving durable and desired strategic results. No, these campaigns must be clearly nested within and supportive of larger schemes of host nation sovereignty, civil actions, and foreign policy agendas—even if (or particularly when) these larger constructs are poorly formed or ill-defined. It is this very ambiguity of structure that lends itself to coordinated schemes of supportive special operations. What SOF uniquely brings are activities that are less provocative and more strategically effective than the large Irregular Warfare campaigns of the past generation—campaigns that invariably morphed to become far too U.S.-centric and dominated by military culture and actions in their execution.

One idea that is gaining traction within the policy community is that of *competitive statecraft*. Perhaps statecraft is always competitive, but the character and intensity of that competition is heating up. The military comes to this contest with the fairly clumsy concept of *irregular warfare*. Why we insist on "irregular warfare" to characterize efforts to thwart challenges that are more illicit than irregular, and conducted largely in peace, is difficult to grasp. Doubly so when the military is seeking to find supporting roles in civilian-led campaigns. Perhaps *military support to competitive statecraft* frames a more productive approach? Words matter, but ultimately it is the character and purpose of our actions that matter most. How should SOF campaign in support of competitive statecraft?

SOF campaigning must be "special," and as such is invariably a supporting effort. These campaigns must advance national interests, support theater campaign objectives in general, and set conditions for the optimal application of Special Operations wherever, and whenever, conflict might emerge. It is through this type of continuous, comprehensive, and coordinated campaigning that SOF actively contributes to integrated deterrence, fosters resilience, and lays the foundation for creating a unique warfighting advantage.

Over the years U.S. SOF have adopted a couple of short lists of tenets to guide our employment. Most famous of these are the "SOF truths" (SOF Truths, n.d.). There is also a pretty good list of five "mission criteria" in JP 3-05, but we have yet to formalize a set of tenets to guide thinking on how SOF campaigns (United States Joint Staff, 2003, p. I-9). So, while this is in no way a comprehensive or official list, the following are some proposed tenets I have come to believe as vital to an effective SOF campaign:

1. *"By-With-Through" is not a single word.* We all need to slow down and fully appreciate each vital nuance of this phrase. While there are several interpretations, here is what it means to me:

   - *"By"*- These are those rare but vital unilateral operations we conduct *by* ourselves or have conducted for us by some surrogate actor.
   - *"With"* — This is a great strength of U.S. SOF—our tremendous network of valuable partners and allies. Whenever possible, U.S. SOF will work *with* our partners and allies as equals in the pursuit of shared interests and solutions. This includes building teams to optimize unique capabilities.
   - *"Through"* — SOF will work *through* relevant populations as our primary medium for action. Understanding who the populations relevant to our interests are and appreciating how they feel about the various sources of governance affecting their lives provides the foundation for much of what we do. *Populations are the modern opportunity space!*

While the past 20 years have been dominated by "By and With," the future competition will likely be weighted more to "With and Through."

2. *SOF conducts the Special Operations subset of Irregular Warfare.* Irregular warfare shares many of the Core Activities assigned to USSOCOM, and the entire Joint Force participates in irregular warfare. Yet it remains essential for SOF to remain focused on those situations that are both necessary to our interests, and yet due to some blend of factors, beyond the abilities of the conventional force. There is no fixed line in this division of effort, and it is incumbent on SOF to continuously seek where we need to be, what we need to do, and to foster unique capabilities for success. This is SOF's quest: to identify, prepare for, and engage upon those operations relevant to current challenges and demanding some unique blend of situational criteria necessary to elevate an operation to one that is "special" (United States Joint Staff, 2003). Going forward, SOF must refine and focus upon the special operations relevant to today's challenges.

3. *Tactical actions for strategic effects.* While all strategies are pursued through the coordinated application of tactics, SOF is a uniquely strategic asset. Whenever possible, SOF should be employed for strategic effect. In traditional campaigning the sum of tactics may well add up to a desired strategic outcome at some point, but in the type of sophisticated campaigning envisioned here, desired strategic outcomes should guide every action.

4. *Seek Indirect Approaches and psychological effects.* There is always a time and place for first order logic and physical effects. But as SOF campaigns for strategic influence in peace, the greatest value comes through leveraging the inherent mystique of the force and the application of higher order logic. In this way SOF can shape and execute approaches that are indirect in time and space to the strategic effects one seeks to achieve, while creating multiple, complex dilemmas within the minds of our adversaries. This is particularly essential to a globally distributed SOF Strategic Influence campaign designed to contribute to a larger scheme of integrated deterrence, disrupt and outcompete Violent Extremists, foster positive influence, facilitate resilience, and ultimately create the effect of a *ubiquitous SOF presence in the minds of those who challenge a rules-based order.*

5. *Seek opportunities as well as threats. As* adversaries conduct problematic acts of competition, there will be both winners and losers among the populations and governments they affect. In grievance there is opportunity. It is in SOF's DNA to understand, relieve, or leverage grievances as necessary to advance our interests. Support to Resilience, Support to Resistance, and Irregular Deterrence (particularly Unconventional Deterrence) all spring from populations believing themselves trapped in conditions of legally irreconcilable political grievance. *This is the strategic opportunity space for SOF.*

6. *Design and execute every operation to reinforce desired strategic narratives through its execution.* Our efforts will either foster or burn influence through their execution. Prioritizing the influence we can foster, over the control we can exert, demands every operation be designed and executed in a manner consistent with our professed values as a nation, as well as what we profess we are doing. Maintaining leadership of the

rules-based order is a competition for influence, and it is the great power who fosters influence best who will prevail.

To simply add a written narrative to a tactical action is inadequate. The story various audiences perceive the action to convey will rob credibility from any narrative that is too late, never heard, or incongruent with those immediate perceptions. Therefore, SOF is most likely to contribute to desired strategic effects when every operation is designed first and foremost for the narratives it will convey through execution. This must be a commander-led process and only displaced as the most critical planning criteria by rare exception. Otherwise, tactical criteria will soon dominate course of action selections, and unintended narratives will become dominant, despite our words.

7. *Petit's Paradoxes.* In addition to these proposed tenets, I find tremendous value in this short list of special operations "paradoxes" offered by Colonel (Ret) Brian S. Petit in his prescient 2013 book, *Going Big by Getting Small* (Petit, 2013). Each of the above listed tenets is enhanced through the application of these paradoxes.

When desired, durable, strategic results prove elusive (but we are certain we have the problem right and are executing the book solution correctly), the inclination is to go increasingly larger, harder, more unilaterally, more violently and more provocatively in the pursuit of success. Instead, we are better served to ask the questions, "Do we have the problem right, or are we fixating on some problematic symptom instead?" and "Is the book solution still valid, or has the rapidly changing strategic environment rendered critical aspects of it obsolete or exposed parts as never being correct to begin with?" Regardless, the application of Brian's paradoxical advice in the conduct of SOF campaigning is always wise:

- Less is better than more.
- Steady and slow is (often) preferred over intrusive and fast.
- A supporting role is better than a lead role.
- The wrong man can do more harm than the right man can do good.
- Conceding military control and precision can create better long-term outcomes.

Effective Strategy Demands a Relevant Theory/Hypothesis.

Absent a sound theory of the problem one seeks to address, and of the solution one hopes to apply in the context of that understanding, one is most likely just attacking problematic symptoms with some preferred solution. Symptomatic approaches may generate temporary windows of apparent success, but invariably serve to make deeper problems worse for the effort. In the current strategic environment, problematic symptoms abound. Bin Laden and his al Qaeda organization were problematic symptoms. As were the Taliban. As is ISIS. As are China and Russia. To be certain, one must deal with problematic symptoms, but one must deal with them in the context of the problems of which they are symptomatic. But if these very serious challenges are "merely" problematic symptoms, *then what is the problem?*

1. A theory of the problem — The challenge of relevant leadership in an era of shifting power

   - *Competition is natural.* In this rapidly changing and competitive environment, governments everywhere struggle to stay in step with the empowered, connected, evolving populations they affect. This is true both at home and abroad. This creates gaps in governance. There is an inherent friction caused by these governance gaps that rob a society of its resilience. This in turn manifests into instability, insurgency, and this new dynamic of stateless unconventional warfare we bundle simplistically as "Violent Extremist Organizations." As political grievance grows within a demographic there is both opportunity and vulnerability. Fortunately, it is within our SOF DNA to be the master of both, relieving, or leveraging such grievance as directed for strategic effect.

   - *Gray zones and elevated thresholds of deterrence are natural.* In simplest terms, "gray zones" are the delta between what legitimate authorities say their rules are, and what one's competitors believe these authorities are willing or able to enforce. These are illicit challenges to authority. In eras of rapidly shifting power, it is natural for rising states seek to expand their positions on the world stage, even as declining powers to seek to cling to theirs. These shifting fortunes fuel a full range of competition that runs from legal, where possible, to illegal, when necessary (gray zone), and with war as a last, but increasingly possible resort.

   - *Policy and Governance are equally causation and cure.* Essentially, the empowering effects of modern information technology have served to render critical aspects of "the old playbook" for being a great power obsolete. Seeking excessive control provokes and exacerbates these dynamics and is increasingly unnecessary to the interests we seek to advance and secure. Just as Great Britain evolved from control-based Colonies to an influence-based Commonwealth to find a new stability, so too must the U.S. frame a more tolerant, influence-based approach.

   - Our problem analysis has under-emphasized the governance aspect of causation and the importance of populations, and it has over-emphasized the role of rogue leaders and the ideology employed to enflame and leverage grievance for purpose. To get to better, more durable strategic effects, we must reframe our understanding of these conditions and those who exploit them, and craft a new playbook better suited for an emergent, information-empowered world.

   - The ambitions of rising states and the VEO exploitation of aggrieved populations cannot be deterred, but we can shape HOW they pursue these changes. This reduces the risk of terrorism or the likelihood of major state conflict as we create time and space for civil authorities to evolve to new policies, better tuned for these changed conditions.

2. A theory of success — Campaigning for Strategic Influence[5]

- SOF will employ an orchestrated blend of our core activities through a global campaign of indirect and direct approaches, "competing around the edges" to facilitate our nation's pursuit of our most vital interests (Atwell & Gage, 2021). This frames a proactive campaign across the competition environment. Within this context, SOF will discreetly work to identify and address both challenges and opportunities in holistic approaches designed to mitigate provocation, disrupt and outcompete threats, and contribute to a comprehensive scheme of integrated deterrence. We see populations as the opportunity space in this competition environment, and one SOF is uniquely suited to operate by, with, and through.

- Einstein observed, *"we cannot solve our problems with the same thinking we used when we created them."* While this seems obvious, taking responsibility for the unintended effects of our actions and changing how we think are both incredibly hard. Doubly so when most challenges are inherently illegal under the laws of the system being challenged and we are typically the legal actor. Yet we must do both to prevail. Stasis of thought and action are not an option.

- Success demands understanding problems more accurately, and then framing challenges in ways facilitating positive, proactive, holistic campaigning. To this end we must reframe the VEO problem, disrupt their UW campaigns, and outcompete VEOs for influence with the aggrieved populations upon which they are wholly reliant. In similar ways we will seek points of leverage on state threats to contribute to the integrated deterrence of the challenges they present. In all things we will recognize and optimize the narratives we tell through our actions. In this way SOF will create a ubiquitous presence in the minds of our adversaries, even as we help set the theater, ensuring we are postured to implement a global scheme of indirect and irregular deterrent options. All while prepared to execute no-fail crisis response or to support the Joint Force in major conflict.

In Conclusion, a Vision and Intent.

Vision: Working globally by, with, and through a resilient network of respected Allies, Partners, and Populations, U.S. SOF will execute a holistic scheme of interest-focused activities designed to achieve a ubiquitous presence. We realize our role is small in size and nearly always in subtle support of much larger efforts; yet is also a role that is exquisitely what others cannot do, and with the potential for uniquely vital strategic effects. These special operations campaigns will focus on problematic acts of competition. We will seek opportunities created by our adversaries, to outcompete and disrupt VEOs, posture for no-fail crisis response, prepare for conflict, and implement a family of special operations designed to advance U.S. influence abroad. Through these actions, SOF will help shrink the gray zone and thereby lower

---

[5] See Jones (2021).

the threshold of deterrence as our principal contribution to a comprehensive scheme of integrated deterrence.

Intent: Our intent is to rebalance, reset, and refocus SOF for the missions before us. This demands each component recenter itself in its core equities and then flee rapidly into the future. This will demand hard decisions to dismantle or downsize existing exquisite capabilities on one hand, even as we develop and field new ones on the other.

For the headquarters, our mantra is "Understanding–Influence–Relationships." It is not enough to know our profession. In this critical decade of change, it is absolutely essential for us to question doctrine, definitions, and labels; to understand and address the challenges before us for what they are; and not draw false comfort from our expertise in engaging them as they were believed to be. SOF does nothing alone and is nearly always in support of strategic goals and other organizations. Our success demands influence—not the influence to get others to do what we think best, but rather the influence to garner the trust that we will support and facilitate their larger success. Lastly, we will continue to nurture and evolve historic relationships as the unassailable foundation to the new relationships we will foster going forward.

We were indeed born for this. Old titles, such as "Global Scouts," "State Department Troops," or "Quiet Professionals" will all take on new relevance; and through our campaigns we will indeed soon come to weigh heavily on the minds of those who would work against us, while growing closer to the hearts of those who choose to work with us. This is the essence of how SOF contributes to integrated deterrence and works to foster the strategic influence necessary to ensure our nation's role well into the future, as leader of a rules-based order designed for an emergent world of shifting power and empowered populations.

References

Atwell, K., & Gage, A. (n.d.). *Back to the Future: Resetting Special Operations Forces for Great Power Competition—Modern War Institute*. Retrieved March 31, 2023, from https://mwi.usma.edu/back-to-the-future-resetting-special-operations-forces-for-great-power-competition/

Dam, R. F. (2021, January 2). The MAYA principle: Design for the future, but balance it with your users' present. The Interaction Design Foundation. https://www.interaction-design.org/literature/article/design-for-the-future-but-balance-it-with-your-users-present

Hearing to consider the nominations of: Lieutenant General Bryan P. Fenton, USA to be General and Commander, United States Special Operations Command; and Lieutenant General Michael E. Langley, USMC to be General and Commander, United States Africa Command, 117th Cong. (2022) (testimony of Lieutenant General Bryan P. Fenton). https://www.armed-services.senate.gov/imo/media/doc/22-61_07-21-2022.pdf

Jones, R. (2021). *Strategic influence: Applying the principles of unconventional warfare in peace.* Strategic Multilayer Assessment, United States Joint Staff, J3. https://nsiteam.com/social/wp-content/uploads/2021/07/SMA-Invited-Perspective_Strategic-Influence_Jones_FINAL.pdf#:~:text=Robert%20Jones%20is%20a%20retired%20Army%20Special%20Forces,from%20Zamboanga%20to%20Kandahar%20and%20places%20in%20between.

Lawrence, T.E. (1926). *Seven pillars of wisdom.* London, UK: General Press.

Petit, B. S. (2013). *Going big by getting small.* Parker, CO: Outskirts Press.

United States Joint Staff. (2003). *Joint Publication 3-05: Doctrine for Joint Special Operations*. United States Department of Defense. https://irp.fas.org/doddir/dod/jp3-05-2003.pdf

United States Special Operations Command. (n.d.-a). *Core Activities*. https://www.socom.mil/socpac/Pages/Core-Activities-.aspx

United States Special Operations Command. (n.d.-b). *SOF Truths*. https://www.socom.mil/about/sof-truths

Army Special Operations Forces' Expanding Role in Deterrence

Mr. Howard M. Simkin
USASOC
howard.simkin@socom.mil

In times of drastic change, it is the learners who inherit the future while the learned usually find themselves beautifully equipped to live in a world that no longer exists.

—Eric Hoffer, Reflections on the Human Condition

Purpose

This article will briefly explore the concept of how future Irregular Warfare (IW) campaigning with Army Special Operations Forces (SOF) at the core of a future joint force could be an approach that supports the 2022 National Defense Strategy (NDS) concept of Integrated Deterrence. The article is framed by a set of responses to four foundational questions: 1) How could IW campaigning support Integrated Deterrence? 2) When should Army SOF take on a leading role in conducting IW campaigning? 3) What is different about IW campaigning? and 4) What sort of headquarters should conduct IW campaigns? At the end, this article will provide brief recommendations on a potential way ahead.

Background

Joint Publication 1: Doctrine for the Armed Forces of the United States (JP 1) states that "Irregular Warfare (IW) is characterized as a violent struggle *among* state and non-state actors for legitimacy and influence over the relevant population(s) (emphasis added)" (United States Joint Staff, 2017). It further states that, "In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation's established government. The less powerful adversaries, who can be state or non-state actors, often favor indirect and asymmetric approaches, though they may employ the full range of military and other capabilities in order to erode their opponent's power, influence, and will" (United States Joint Staff, 2017).

No single joint publication governs the major types of IW operations and activities, which include Unconventional Warfare (UW), Foreign Internal Defense (FID), Counter Insurgency (COIN), Counter Terrorism (CT), Foreign Humanitarian Assistance (FHA), and Security Force Assistance (SFA). All activities except UW have their own joint publication. *Joint Publication 3-05: Joint Doctrine for Special Operations* (JP 3-05) covers UW as one of the special operations

core activities.[1] When addressing the subject of IW, JP 3-05 also notes that while conventional forces (CF) conduct some of these activities, "SOF conducts all of them using specialized tactics, techniques, and procedures, and in unique conditions and to different standards, but in a manner that complements conventional force capabilities" (United States Joint Staff, 2020a, pp. II-3).

Joint Publication 5-0: Joint Planning (JP 5-0) defines a campaign as, "A series of related operations aimed at achieving strategic and operational objectives within a given time and space" (United States Joint Staff, 2020b). It also recognizes that the nature of campaigns are changing from a regional focus to one which addresses "transregional (across multiple areas of responsibility [AORs]), all-domain (land, air, maritime, space, and cyberspace), and multifunctional (integration of the seven joint functions)" (United States Joint Staff, 2020b, pp. II-1). This is a significant shift from previous versions of JP 5-0.

The *National Defense Strategy 2022* (NDS) places an increased emphasis on campaigning as one of the three primary ways of achieving our national goals. The other two are integrated deterrence and building enduring advantages. These three ways of achieving our goals are interdependent. As noted in a fact sheet released to the public by the Department of Defense (DoD), "The United States will operate forces, synchronize broader Department efforts, and align Department activities with other instruments of national power, to undermine acute forms of competitor coercion, complicate competitors' military preparations, and develop our own warfighting capabilities together with allies and partners" (Office of the Secretary of Defense, 2022, p. 2). To support this guidance, the joint force must conduct transregional, all-domain, and multifunctional IW campaigns that support Integrated Deterrence as well as building enduring advantages.

How Could IW Campaigning Support Integrated Deterrence?

"Integrated deterrence entails developing and combining our strengths to maximum effect, by working seamlessly across warfighting domains, theaters, the spectrum of conflict, other instruments of U.S. national power, and our unmatched network of Alliances and partnerships" (United States Joint Staff, 2020b, pp. II-2). The use of IW campaigns could serve to strengthen our partners and allies through operations and activities conducted below the level of large-scale combat operations (LSCO). A pertinent and near-term example involves the ongoing conflict in Ukraine, where NATO forces provided the essential training that complicated Russia's military preparations and developed Ukrainian warfighting capabilities. A useful way to envision future IW campaigning may include the following four interdependent concepts: *disrupting the adversary, hardening the environment, resistance, and recovery.*

---

[1] The most recent edition of JP 3-05 superseded *Joint Publication 3-05.1, Unconventional Warfare*, published in 2015.

Disrupting the adversary can serve to protect the homeland and to gain a position of advantage for the United States, allies, and partners. Approaches to disrupting the adversary include actions taken to affect communications, cyber connectivity, space capabilities, energy and logistic supply chains, coercive actions, threat finances, proliferation of weapons of mass destruction, and malign influence. Disrupting the adversary can intentionally impose sufficient cost, doubt, and unbelief in the minds of the enemy decisionmakers so that they are not able to accomplish their campaign objectives. Disrupting an adversary in the future will require investing in new technologies to gain a position of advantage over our adversaries as well as to train and equip Army Forces to conduct disruptive operations.

Hardening the environment can serve to build resilient indigenous capability, capacity to resist strategic adversaries, and the ability to recover from aggression. It can serve to lower adversary confidence levels in their ability to succeed, thereby deterring aggression. Importantly, it also includes measures to aid in recovery, one of the historic shortcomings of resistance movements.

Resistance actively and passively opposes an adversary in the physical, virtual, and cognitive dimensions, with the ultimate objective being recovery. Resistance will enable the joint force to see, sense, stimulate, and strike across the operational continuum. To execute resistance in the future, there must be investments in Remote Train, Advise, and Assist activities requiring U.S. forces to employ advanced technologies such as synthetic training environment, enhanced reality (XR), mesh networked micro satellites, and terahertz communications to train, advise, and assist allies, partners, and resistance movements without U.S. forces being physically present.

Recovery can begin before resistance is over, particularly in liberated areas. Once resistance has decreased, the process of rebuilding a civil society and a government appropriate for the region should move forward.

When Should Army SOF Take on a Leading Role in Conducting IW Campaigning?

Army SOF should take on a more predominant role in IW campaigning when both support to resistance[2] and unconventional warfare[3] are the main components of the Joint Force

---

[2] Support to resistance describes the USG's integrated activities that support a nation or populace to oppose social, economic, political, and military subversion and aggression from external threats or occupiers, or from the repression and tyranny of established governments. Support to resistance provides an overarching framework for the USG to support resistance partners that have operational or strategic goals that align with US national security objectives. The USG can sponsor resistance partners' activities that occur throughout the competition continuum, encompassing cooperation, competition below armed conflict, and conflict or war. Support to resistance includes evolving multiple strategic and operational objectives changing over time and context, including building partner resilience, competing against adversaries, and UW. See United States Joint Staff, (2020a), p. B-1.

[3] Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. See United States Joint Staff (2020a), p. GL-10.

campaign. Since unconventional warfare entails specialized equipment, unique selection of participants, and extensive preparation and training, other elements of the Joint Force, to a large degree, may lack the essential capabilities to perform these unique and complex tasks. Army SOF should also take on a leading role in IW campaigning when the campaign requires integration of portions from USSOCOM global campaign plans and theater-level combatant campaign plans (United States Joint Staff, 2020a, pp. III-4–III-15). Although the Chairman, Joint Chiefs of Staff (CJCS) is responsible for transregional, all-domain, and multi-functional threats, the Joint Force could potentially designate SOF as the lead for addressing specific transregional threats (United States Joint Staff, 2020b, pp. II-2). This approach would make sense when addressing an emerging threat that requires the involvement of credible U.S. forward access and presence.

What is Different About IW Campaigning?

IW campaigns are people centric. They seek to gain legitimacy and influence over relevant populations to attain the campaign's goals. This stands in contrast to traditional warfare campaigns that focus on enemy forces and terrain. IW campaigns are of long duration, potentially extending over a period of decades. Legitimacy and influence are normally built over time, as they have their foundation in trust. Of note, actions or inaction on our part can demolish a foundation of trust in a much shorter time than it took to build. IW campaign planners must always keep this in mind.

IW campaigns can be transregional, particularly against a peer adversary. Our strategic competitors, to a significant degree, are not limited to the confines of geographic, regional boundaries. Strategic competitors, in general, also seek to achieve their goals below the level of armed conflict. To counter their transregional activities most effectively requires a transregional approach. Asymmetric approaches lie at the heart of successful campaigns.

It is important to maintain focus on relevant populations. Establishing cognitive objectives are of primary importance in IW campaigning. Without them, our approach will default to one centered on enemy forces and terrain. While the defeat of enemy forces and possession of terrain are important, their importance to an IW campaign lies in their effect on relevant populations. The key to maintaining that focus is developing measures of effectiveness (MOE) for both legitimacy and influence. Social media scraping, as well as more traditional observations of behavior, could provide empirical data to gauge relative progress made toward improving MOEs.

IW campaigns leverage Army SOF persistent forward credible access and presence. The foundation of trust is built on relationships. Face-to-face interaction is still the best way to build trust. Anywhere that Army SOF has maintained credible access and presence, the opportunities for a successful IW campaign are greatly increased. Finally, IW campaigns depend on Joint, Interagency, Intergovernmental, and Multinational (JIIM) guidance, participation, and integration. DoD normally supports JIIM efforts in IW. Even when they are the lead agency, DoD still depends heavily on its JIIM partners.

Cyber-Space-SOF Triad as an Asymmetric Approach

One form of asymmetry is the recent emergence of the converging capabilities and effects of Cyber, Space, and SOF in the competitive security environment. As we move into the future, the combinations of these particular capabilities, orchestrated in a holistic fashion with relevant C2, will ensure greater redundancy, resilience, and influential power previously unseen on the battlefield. Together this triad of capabilities will offer new options for deterrence that will be compelling both in competition and conflict and could manifest in ways that were previously unseen and unanticipated by our adversaries.

An integrated Cyber, Space, and SOF Triad could certainly achieve greater strategic and operational impacts through campaigning for deterrence and preparing the environment for joint force action in crisis and conflict. The Triad components would be inherently trans-regional and could collectively better see, sense, understand, stimulate, and provide options to strike and assess across the physical domains synchronized with the information and cognitive dimensions. In employment, an interoperable Cyber, Space, and SOF Triad cross-functional team empowered with appropriate resources, authorities, and permissions could foreseeably converge cyber, space, and special operations capabilities to achieve unique trans-regional, multi-domain effects to impose costs on and create dilemmas for our toughest adversaries.

What Sort of Headquarters Should Conduct IW Campaigns?

For the future Joint Force, an IW-focused headquarters could be a viable option to conduct IW campaigns. The Transregional SOF Convergence Headquarters (SOF IW HQ) could coordinate, integrate, assess, and enable trans-regional strategic and operational level effects by converging multi-domain capabilities. It could create operational-level physical, information, and cognitive effects by campaigning across all domains throughout the operational continuum to support Army and Joint Force objectives and priorities though IW. This standing headquarters could command and control options for tailorable subordinate units. This new unit of action would be a standing headquarters modeled on the Special Operations Joint Task Force (SOJTF), which could selectively employ tailorable subordinate units.

Competition. On any given day, 2,000-4,000 ARSOF Soldiers are deployed in 70-80 countries. As each soldier is a sensor for information relevant to active campaigning, this posture could create a massive information network whose power increases exponentially through interaction with partner forces and surrogates. The SOF IW HQ has the ability to consolidate information from these forward forces in real time via state-of-the-art communication networks and could process it through artificial intelligence and machine learning (AI/ML) programs to determine meaning and discover hidden associations. Working with the Information Warfare Center (IWC) and a Military Information Support Operations Task Force

(MISTF) or Civil Military Operations Task Force (CMOTF) if formed, the SOF IW HQ could use this information to generate transregional IW Concepts of Operation (CONOPS) and options, converge special activities and information warfare, and impose costs and create dilemmas for adversaries via coercive means. With appropriate guidance, these options could be executed by a designated SOF Headquarters or by JIIM partners.

Crisis. In crisis, the network of SOF operators, partners, and surrogates can transition from a broad-spectrum external information gathering effort to a focused effort on select and/or regional problem sets. In this instance, a subordinate SOF Headquarters could command and control transregional operations targeted against specific adversaries. This employment model focuses existing networks built during IW campaigns to create transregional dilemmas for globally dispersed NDS threats using compelling means in an effort to return to competition. In preparation for potential escalation to conflict, SOF IW HQ could provide relevant target data to the Joint Force and a Multi-Domain Task Force (MDTF).

Conflict. In conflict, SOF units and partners forward positioned during IW will likely have the best situational awareness prior to and in the early phases of Joint Forcible Entry Operations (JFEO). A future SOF IW HQ could synchronize Joint SOF operations in deep areas to reduce enemy layered standoff by seeing, sensing, stimulating, and striking adversarial anti-access/area denial (A2/AD) systems. This would be accomplished through and with partners, surrogates, and guerilla forces and enabled by convergence of warfighting functions, information warfare, special activities, space, and cyber operations. These cross-domain operations could strike deep in the physical, information, and cognitive realms to create multiple 'fronts,' which present the enemy with compounding dilemmas and complicate the enemy's decision-making. They would simultaneously identify and categorize high value targets, degrade enemy combat power, disrupt the enemy's ability to command and control, delay the tempo of operations, attrition forces, obstruct reinforcement, destroy infrastructure and supplies, disrupt logistics, and ultimately break down the enemy's cohesion and morale.

Way Ahead

To move toward the future, a rigorous series of joint experimentation, simulations, and exercises is proposed to chart the way ahead, for several reasons. These series of events could serve as a means to validate or invalidate Army SOF's role in IW campaigning and subsequently develop supporting doctrine. Additionally, these events may reveal the need for future ARSOF units of action that could maximize the effectiveness of SOF in IW. This may also lead to a smaller modification of an existing unit (or units). Furthermore, these efforts could potentially lead to something entirely new, requiring DOTMLPF-P[4] analysis.

---

[4] Doctrine, organization, training, materiel, leadership and education, personnel, and facilities-policy

Conclusion

This article briefly explored a future concept for Irregular Warfare (IW) campaigning with Army Special Operations Forces (SOF) at the core of a Joint Force effort. It framed the discussion with four fundamental questions: 1) How could IW campaigning support Integrated Deterrence? 2) When should SOF lead in IW campaigning? 3) What is different about IW campaigning? and 4) What sort of headquarters should conduct IW campaigns? With purposeful experimentation and thoughtful reflection, the answers to these questions may provide a basis for future exploratory discussion and debate on an issue of vital importance to achieving Integrated Deterrence for the nation.

References

Church, B., Berlinger, J., Vogt, A, Sangal, A., Macaya, M., & Chowdhury, M. (2022, May 11). May 11, 2022: *Russia-Ukraine news*. CNN. https://edition.cnn.com/europe/live-news/russia-ukraine-war-news-05-11-22/h_534916cac5cc28cffd5507e5a04015f8

Headquarters, Department of the Army. (2019). *Army doctrine publication 3-0, Operations*. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf

Liddell Hart, B. H. (1991). *Strategy* [second revised edition]. New York, NY: Penguin Books.

National Intelligence Council. (2017). *Global trends, paradox of progress.* https://www.dni.gov/files/images/globalTrends/documents/GT-Main-Report.pdf

Office of the Secretary of Defense. (2022). *Fact sheet: 2022 National Defense Strategy*. United States Department of Defense. https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF

Steinbuch, Y. (2022, April 14). Ukraine claims it blew up bridge in ambush of Russian convoy. *New York Post*. https://nypost.com/2022/04/14/ukraine-claims-it-blew-up-bridge-in-ambush-of-russian-convoy/

United States Army Training and Doctrine Command. (2011). *TRADOC pamphlet 71-20-3 concept development guide.* United States Army. https://adminpubs.tradoc.army.mil/pamphlets/TP71-20-3.pdf

United States Army Training and Doctrine Command. (2018). *TRADOC pamphlet 525-3-1: The U.S. Army in multi-domain operations 2028*. United States Army. https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf

United States Department of Defense. (2021). *Dictionary of military and associated terms*. https://irp.fas.org/doddir/dod/dictionary.pdf

United States Department of Defense. (2018). *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American miltary's*

competitive edge. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

United States Joint Staff. (2016). *Joint operating environment 2035: The joint force in a contested and disordered world.* United States Department of Defense. https://apps.dtic.mil/sti/pdfs/AD1014117.pdf.

United States Joint Staff. (2017). *Joint Publication 1. Doctrine for the Armed Forces of the United States.* United States Department of Defense. https://urldefense.us/v3/ https:/vdocuments.net/jp-1-doctrine-for-the-armed-forces-of-the-united-states.html?page=1__;!!G2kpM7uM-TzIFchu!k4eB5P6H00XL4zCrlnNQA0Xj4FRKys1ZjKSMCh8MbP_hYo0nD9LqsLfd8Vxpax7ASq$

United States Joint Staff. (2020a). *Joint Publication 3-05: Joint doctrine for special operations.* United States Department of Defense.

United States Joint Staff. (2020b). *Joint publication 5-0: Joint planning.* United States Department of Defense. https://irp.fas.org/doddir/dod/jp5_0.pdf

United States Strategic Command (STRATCOM)

Mr. Richard McManus
DAFC, USSPACECOM, recently of USSTRATCOM
Richard.a.mcmanus.civ@mail.smil.mil

USSTRATCOM's view of integrated deterrence relies upon two assertions. The first is that observations of past and present security environments led senior leaders to conclude deterrence must be holistic and must underpin our nation's defense strategy. The second is that in order to transition deterrence theories into Department of Defense (DoD) best practices, a shared deterrence framework is critical. Therefore, the initial section of this article examines how observations led to the revival of "integrated deterrence." The second section addresses the need for a DoD-wide accepted integrated deterrence framework and proposes essential characteristics of any emerging deterrence framework.

Observations of Past and Present Security Environments

Deterrence works. The concept of deterrence gained notoriety, or better yet was immortalized, due to the successful avoidance of nuclear Armageddon during the multi-decade Cold War. During this period, both the United States and the Soviet Union developed and fielded nuclear arsenals capable of thermonuclear annihilation casting nuclear shadows over any, and all, military employment decisions. Fierce nationalism and/or demonizing propaganda fostered a mutual hatred of opposing ideologies. Despite this, restraint prevailed. Political, economic, cultural, and even military clashes, while frequent and often tense, never escalated to direct conflict or thermonuclear war. In this regard, deterrence was successful.

Deterrence implementation via coordination. Throughout the Cold War, U.S. leaders across the government developed policies, messages, operations, exercises, and supporting defense budgets to implement national security strategies with deterrence as the cornerstone. They coordinated these both internally (e.g., between U.S. agencies) and externally with NATO and other key allies. Deterrence was integrated across contributors and benefactors, across domains (air, land, sea, and space), across geographic regions, and across the spectrum of conflict. We collectively acted proactively day-to-day and prepared for both imaginable and unimaginable contingencies.

Previous deterrence integration practices atrophied. By the late 1990s, the threats of nuclear Armageddon or a Fulda Gap invasion seemed threats of the past. Without these looming, the predominance of deterrence in national strategy eased and need for national leaders to focus on deterrence as a tool of statecraft dissipated. Routine integration between political and military apparatuses and the associated coordination mechanisms atrophied. Deterrence efforts bifurcated into two forms: nuclear and conventional. The former (nuclear) enhanced

strategic stability, assured allies of U.S. commitment to extended deterrence, and enabled the nation to confront challenges with limited fear of strategic escalation. The latter (conventional) became the realm of combatant commanders where deterrence was implemented by portraying regional dominance to deter limited-aim conflicts and resolve potential crises on terms favorable to the U.S. and its allies.

The security environment requires effective deterrence. Today, China and Russia perceive themselves victims of a U.S.-dominated international system and are intent on challenging this liberal construct. They spent decades observing the U.S. ways of war and building modern military forces, developed and positioned to exploit time/distance advantages. Simultaneously, they expanded and diversified their nuclear arsenals to deter interventions in crises, which they view as sovereignty issues. Russia uses military force overtly to manage its perceived sphere of influence while China welds a combination of diplomatic, economic, and military power to expand its hegemonic power. For the first time in history, the U.S. and its allies must apply deterrence to two aggressive nations capable of contesting military dominance and capable of escalating aggression with any instrument of power or in any domain. This is the security environment that drove the revival of integrated deterrence.

A Shared Integrated Deterrence Framework

The state of integrated deterrence. On 30 April 2021, U.S. Secretary of Defense Lloyd J. Austin III first uttered the phrase "integrated deterrence" at a U.S. Indo-Pacific Command ceremony in Pearl Harbor, Hawaii. It was a new phrase—but not a new concept. In June 2021, at a Carnegie Mellon address, Undersecretary of Defense for Policy, Dr. Colin Kahl, expanded on what was meant by integrated deterrence. He highlighted the need to integrate deterrence efforts across 1) the government agencies, 2) allies and partners, 3) geographic areas, 4) all-domains, 5) time, and 6) the spectrum of conflict. These two speaking engagements initiated the first effort in decades in which the DoD would examine deterrence holistically. The Office of the Secretary of Defense (OSD) then took on the task of codifying "integrated deterrence" in the National Defense Strategy (NDS). As of late July (2022), OSD is on the cusp of releasing an unclassified NDS. Now the department faces the daunting task of transitioning integrated deterrence from theory to practice.

Relearning integration. To implement integrated deterrence holistically, the DoD must learn to overcome both lexical and cultural differences between the various deterrence contributors and benefactors. Consider the lexical challenge first: the phrase "deterrence by denial." For military members, denial equates to defeating operational forces physically. For their diplomatic counterparts, the phrase more commonly equates to denying the objective of the aggression—not necessarily through military defeat. Diplomats often prefer to deny objectives through manageable political or economic methods and view the alternative of military defeat as a high-risk/last-resort option. Second, consider cultural challenges. Just within DoD, deterrence responsibilities are distributed across eleven Combatant Commands, six services, and numerous combat support agencies, each of which view the world from their own vantage

point. The organizational breadth creates a massive challenge to maintaining deterrence unity of effort. Over the last decade, defense exercises and wargames sought the solution to internal cultural barriers through the championing of "global integration." Those events revealed centralized deterrence is too slow for the pace of modern crises/conflict, and decentralized deterrence is easily undermined in a global multi-domain security ecosystem. A shared deterrence framework provides a first step to overcoming cultural (and lexicon) differences.

Characteristics of any adopted integrated deterrence framework. To transition deterrence theories (or concepts) as outlined in defense strategy into practice, the nation must recognize the need for and develop a shared integrated deterrence framework. Any emerging deterrence framework must have the following features:

- *Orient on decisive influence of decision maker perceptions.* Deterrence is the art of deliberately influencing the perceptions that motivate leaders to consider military aggression. This orientation requires an in-depth understanding of those perceptions and a recognition of which are subject to influence. An aggressor's escalation decision factors are formed by perceptions of: 1) the need to act, 2) the opportunity to act, 3) the military capability to act, 4) the military opposition they must overcome to succeed, 5) the political opposition they must absorb if successful, and 6) their ability to sustain gains. Preparing for proactive deterrence requires a shared agreement on which perceptions to track and assess, a baseline assessment of these perceptions, and an articulated path to influence these perceptions in a way that encourages restraint.
- *Recognize distinct deterrence periods.* Across the spectrum of conflict, two key variables significantly impact deterrence approaches. First is the immediacy and priority of deterrence objectives. Second is the means and authorities available to pursue those deterrence objectives. Consider four distinct deterrence periods: day-to-day, crisis, intra-war, and post-strategic escalation (e.g., attacks on U.S./allied homelands, chemical/biological weapons use, nuclear attacks, etc.). In the day-to-day deterrence period, immediacy is given to deterring initial aggression, while priority remains on deterring strategic escalation. Except in extreme circumstances, deterrence operations in this period would require restraint from kinetic force employment as a means to sustain deterrence. In crisis, immediacy would be given to deterring armed conflict, and means/resources might be expanded to include force employment. In the intra-war period, immediacy would be given to deterring strategic escalation. Following adversary strategic escalation, the nation would face strategic choices, and the aperture for what/how to employ force would likely broaden. Recognizing these periods as unique enables the Department to prepare deterrence approaches tailored to anticipated circumstances and to explore those options with national decision makers beforehand. Preparing for each is necessary to address deterrence "across the spectrum of conflict."
- *Combine critical deterrence logics.* While many deterrence practitioners demonstrate a bias to a single deterrence logic (e.g., cost imposition, denial, etc.), any one of these single logics will be insufficient by itself given the nature of threats. For example, the

efficacy of operational denial (in the cases of China or Russia) is challenged by time/space advantages and years of calculated modernization. In many cases, military denial is not credible. Similarly, the efficacy of a pure cost imposition approach is stressed by the adversaries' ability to match escalation (e.g., they retain the ability to escalate). Additional deterrence logics also enhance deterrence. For example, ambiguity regarding current and future U.S./allied military capabilities can alter decision makers' confidence in predicting the costs and benefits. For each distinct deterrence period, a tailored combination of deterrence logics must be applied to increase the likelihood of deterrence success.

- *Allow for the scaling of deterrence to the appropriate level of violence.* It is possible and necessary to scale deterrence activities, recognizing that either excessive or insufficient assertiveness can undermine deterrence. Consider four levels of deterrence activities. First is investing in and testing deterrence capabilities. This level includes activities necessary to prepare for deterrence and/or combat operations across the spectrum of conflict. Most activities of this sort can be conducted with minimal risk to stability. Second is the messaging and information operations. Think of this as the words (not actions) used to communicate to deterrence stances. Third is demonstrating. This entails demonstrating through posturing, forming or exercising alliances, and revealing capabilities with the intent of influencing escalation decisions. Fourth is employing force. This level involves physically affecting the opponent's systems or forces. Articulating these levels allows combatant commanders (CCDRs) to scale deterrence activities in accordance with policy guidance—a necessary characteristic for implementing deterrence strategies.

- *Drive dynamic, and often competing, global and regional priorities.* The complexity of the security environment will require that throughout the spectrum of conflict, simultaneous execution of defense-critical missions is necessary. Each mission contributes to deterrence in some manner, and each is the responsibility of a different combatant commander. Perhaps the most essential aspect of a deterrence framework is defining with clarity who does what, when, and with what capabilities to achieve the nation's deterrence objectives throughout the spectrum of conflict. Arguably this will be dynamic.

In conclusion. The revival of integrated deterrence is necessary based on changes in the security environment. The development of a DoD-wide shared integrated deterrence framework is necessary for coordination both within the Department and externally with government agency and alliance partners. Ultimately, the United States and its allies seek to deter armed crisis and armed conflict by convincing potential adversaries they can resolve disputes without force, military aggression will not achieve their desired aims, and the consequences of pursuing military solutions are unacceptably costly. If we do find ourselves embroiled in armed conflict, particularly with a nuclear peer, we must be prepared to double down on even more vital deterrence objectives: deter attacks on the homeland and deter

nuclear escalation. It is time to transition the concept of integrated deterrence from theory to practice.

Biographies

Dr. Belinda Bragg

Dr. Belinda Bragg is a Principal Research Scientist for NSI. She has provided core support for DoD Joint Staff and STRATCOM Strategic Multilayer Analysis (SMA) projects for the past nine years. She has worked on projects dealing with nuclear deterrence, state stability, U.S.-China and U.S.-Russia regional relations. Dr. Bragg has extensive experience reviewing and building social science models and frameworks. She is one of the two designers of a stability model, (the StaM) that has been used analyze stability efforts in Afghanistan, state stability in Pakistan and Nigeria, and at the city-level to explore the drivers and buffers of instability in megacities, with a case study of Dhaka. She was also part of the team that designed the pathways model and implemented it for a study of the likelihood of fragmentation in Pakistan. More recently she participated in projects focusing on the grey zone, space, Afghanistan and North Korea. Dr. Bragg is also responsible for writing final integration reports for all SMA projects.

Dr. Hriar "Doc" Cabayan

Dr. Hriar "Doc" Cabayan is currently a member of the Office of Defense Coordination at the Lawrence Livermore Laboratory. He joined the laboratory in 1977 and worked on nuclear weapons effects, Strategic Defense Initiative related efforts, and directed energy programs. In 1997 he joined the Joint Staff/J-39 where he managed the Strategic Multilayer Assessment (SMA) Program. In 2007, he received the Joint Meritorious Civilian Service Award from the Office of the Chairman, Joint Chiefs of Staff in 2007 and again in 2019. He returned to Lawrence Livermore Laboratory in October 2019.

Mr. Nathan Heath

Nathan Heath is an Analyst specializing in Strategic Multilayer Assessment (SMA) research and writing in support of government clients. He regularly contributes to report-writing and modeling for SMA projects, including for the USAF HQ A3, USAFRICOM, and USSTRATCOM. He holds an M.A. in Law and Diplomacy from The Fletcher School of Law and Diplomacy, Tufts University, as well as B.A.'s in International Relations and Music from Wheaton College (IL). Prior to joining NSI, Nathan worked in various roles across government, private law, and nonprofit organizations. In his spare time, he enjoys music, hiking, running, and cycling.

Ms. Michele Wolfe

Michele K. Wolfe is a senior civilian employee at the United States Africa Command. As the Senior Operations Research Systems Analyst (ORSA), she functions as the subject matter expert for analysis and strategic assessments for the Command, to include crafting and influencing far-reaching strategic actions, affecting Africa, Europe, and the United States.

Ms. Wolfe recently graduated from the Defense Senior Leader Development Program (DSLDP), the Department of Defense's premier program to develop 21st century senior executive leaders. She began the 28-month DSLDP in January of 2020, with leadership seminars and a preparatory course at the Army War College before devoting a year to intensive study at the Naval War College, earning a Master's degree in National Security and Strategic Studies (with Distinction) with an additional graduate certificate in Ethics in Emerging Military Technology in June 2021. Ms. Wolfe then accepted the present overseas billet to gain Joint and Combatant Command Experience at some of the highest levels.

Prior to the DSLDP, Ms. Wolfe served as Headquarters, Department of the Army G-8's ORSA, Requirements Integration Synchronization Officer (RISO), and the Army Requirements Oversight Council's Secretariat Branch Chief. She led requirements and analysis reviews of Joint Capabilities Integration and Development System (JCIDS) documents and studies, at times writing guidance, and at other times, championing programs through the approval systems and integrating them into the Planning, Programming, Budgeting and Execution (PPBE) cycle. Ms. Wolfe worked with aviation and missile portfolios, but focused on engineering, to the point where the Corps of Engineers awarded her the Bronze Order of the DeFluery just before she departed for the Naval War College.

Prior to her work at the Pentagon, Ms. Wolfe spent nearly a decade at the TRADOC Analysis Center leading crucial Army and Joint Analysis of Alternatives (AoA) studies. Key programs included the Ground Combat Vehicle AoA, the Lower Tier Air and Missile Defense AoA, and

the Advanced Threat Detection System AoA. During these studies, Ms. Wolfe led multi-organization teams through risk, trade-off decisions, and requirements analysis, presenting insights that influenced billion-dollar acquisition programs, some of which the Army is procuring today.

Among her awards, Ms. Wolfe earned the Bronze Order of the DeFluery, the Department of the Army Achievement Medal for Civilian Service, the Commander's Award for Civilian Service, the NATO Science and Technology Organization Award, and a publication in the Journal of Asia-Pacific Affairs for her article "The Next War to End All Wars," from the Naval War College.

Ms. Wolfe spends her free time with her husband, "Air Force" Andy, two gorgeous daughters, an old poodle, and a grumpy cat.

Dr. Michael Warner

Dr. Michael Warner serves as Command Historian at U.S. Cyber Command. He has written and lectured on intelligence and cyber history, theory, and reform. His latest book, *The Use of Force for State Power: History and Future*, was co-authored with John Childress (Palgrave Macmillan, 2020). He also wrote *The Rise and Fall of Intelligence: An International Security History*, published by Georgetown University Press (2014). Recent writings include: "The Military Instrument in Cyber Strategy" (with Emily Goldman), *SAIS Review of International Affairs* 41:2 (Summer-Fall 2021); "A Brief History of Cyber Conflict," in *Ten Years In: Implementing Strategic Approaches to Cyberspace*, an anthology he co-edited with Emily Goldman and Jacqueline Schneider (Naval War College Newport Paper 44, 2021); and "US Cyber Command's First Decade," (Stanford/Hoover Aegis Series, 2020).

Dr. Emily Goldman

Dr. Emily Goldman serves as a strategist at U.S. Cyber Command and a thought leader on cyber policy. She was cyber advisor to the Director of Policy Planning at the Department of State, 2018–19. From 2014 to 2018 she directed the U.S. Cyber Command/National Security Agency Combined Action Group, reporting to a four-star commander and leading a team that wrote the 2018 U.S. Cyber Command vision, "Achieve and Maintain Cyberspace Superiority." She has also worked as a strategic communications advisor for U.S. Central Command and for the Coordinator for Counterterrorism at the State Department. She holds a doctorate in Political Science from Stanford University and was a Professor of Political Science at the University of California,

Davis, for two decades. Dr. Goldman's most recent book, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, with Michael Fischerkeller and Richard Harknett, was published by Oxford University Press in 2022.

Mr. Michael A. Clark

Michael Clark, a member of the Senior Executive Service, serves as the U.S. Cyber Command (USCYBERCOM) Director for Acquisition and Technology (J9). Mr. Clark provides leadership, advice, and technical guidance on development and integration of cyberspace capabilities as part of the Joint Cyber Warfighting Architecture Portfolio exceeding $4B. He leads technology transition efforts with strategic government and academic partners. He provides leadership to the maturity of the command's Innovation Strategy. He is responsible for the development and execution of all USCYBERCOM acquisition system policies and procedures.

Mr. Clark retired from active duty Air Force in 2001, after 24 years of service as an Intelligence professional. He served in numerous duty positions to include tours with the RC-135, SR-71, and U2-R collection platforms; as an all-source intelligence analyst at the Intelligence Center Pacific; as Flight Commander at the 6920th Electronic Security Group, Misawa Air Base, Japan; and as the first Commander of Detachment 1, 692nd Intelligence Wing, Andersen AFB, Guam. He was the first Air Force officer assigned as a CLASSIC WIZARD Operations Officer at the Naval Computer and Telecommunications Area Master Station in the Western Pacific. His final active duty assignment was to Headquarters Air Force (HAF) where he held positions as the Intelligence Briefer to the Chief of Staff and Secretary of the Air Force, Functional Manager for Air Force Information Warfare Programs, and as HAF Integrated Joint Special Technical Operations Planner.

Mr. Clark joined Syracuse Research Corporation (SRC) in Chantilly, Virginia in 2001 as a Senior Intelligence and Information Operations Engineer, developing a Computer Network Operations (CNO) enabling-technology for the National Reconnaissance Office. Mr. Clark was the first SRC employee to be assigned as an Intergovernmental Personnel Act (IPA) detailee and lead the Executive Agency Office for Headquarters Air Force, providing oversight of two Defense Intelligence programs. In 2006, he joined the Joint Functional Component Command Network Warfare at Fort Meade, Maryland and held positions as a CNO Planner (J5), Deputy Director for Operations (J3), Director for Manpower, Personnel, and Security (J1), Deputy Director for Plans and Policy (J5), and most recently, Director for Acquisition and Technology (J9). He has been with USCYBERCOM since its inception in 2010.

Mr. James M. Jenista

James "JJ" Jenista is an Air Force civilian in the Joint Training, Exercise, and Wargaming Directorate (J7) at North American Aerospace Defense Command (NORAD) and United States Northern Command (USNORTHCOM). In the combined Headquarters for the two Commands, JJ provides contract management and acquisition support across eight Divisions and a host of external partners. He is a planner with USNORTHCOM and has assisted in the planning and execution of a variety of Joint and National Level Exercises.

JJ holds Bachelor and Master of Science Degrees in Aerospace Engineering from the University of Notre Dame, where he enrolled on a Naval ROTC scholarship and was subsequently commissioned into the Navy. He flew the A-6 Intruder and the F-14 Tomcat during a 20-year naval career that also included stints teaching NROTC at Notre Dame and facilitating Naval Leader Training Courses in Coronado, CA. He was a 4-time Navy Astronaut Candidate, was on duty in the NORAD Command Center on 9/11, and is completing a master's degree in Homeland Security through the Center for Homeland Defense and Security under the auspices of the Naval Postgraduate School.

Mr. Robert C. Jones

Robert Jones is a retired U.S. Army Special Forces Colonel, a former Deputy District Attorney, and the senior strategist at U.S. Special Operations Command. Currently serving within the USSOCOM J5-JSOU Donovan Integration Group, Mr. Jones is responsible for leading innovative thinking on the strategic environment and how it impacts factors critical to national

security, such as the evolving character of conflict, all aspects of irregular warfare, deterrence in competition, societal stability, and implications for SOF. He also serves as a Strategic Advisor to the Director of Plans, Policy, and Strategy.

Mr. Jones is a featured lecturer for the JSOU Enlisted Academy, as well as the USAJFKSWCS Officer Course on strategy, the evolving character of conflict, impact on viability of solutions, and implications for SOF. He is currently promoting a proactive campaigning construct of *strategic influence* that is rooted in the fundamentals of insurgency and unconventional warfare and intended to inform SOF operationalization of the National Defense and National Military Strategies. His focus is the pursuit of understanding and the provision of context.

"**If war is the final argument of Kings, then revolution is the final vote of the people.**" RCJ

Mr. Howard R. Simkin
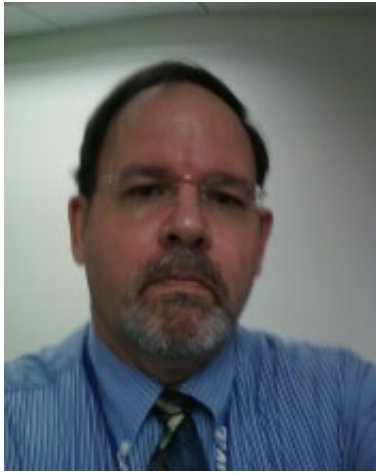
Howard R. Simkin is a Senior Concept Developer in the DCS, Capability Development and Integration Directorate (CDID), U.S. Army Special Operations Command. He has over 40 years of combined military, law enforcement, defense contractor, and government experience. He is a retired Special Forces officer with a wide variety of special operations experience. Within the CDID he analyzes and defines the future operating environment and required capabilities Army Special Operations Forces (ARSOF) in support of future concepts development. His subject matter expertise includes analyzing and evaluating historical, current and emerging technology as well as Combined, Joint, Multi-Service, Army and ARSOF organizational initiatives, trends, and concepts to determine the implications for ARSOF units. Mr. Simkin holds a Masters of Administrative Science from the Johns Hopkins University. He is certified both as a TRADOC Mad Scientist and as a Project Management Professional. He has written several articles that have been published in Naval History Magazine, Small Wars Journal, the TRADOC Mad Scientist Blog or on the Strategic Multilayer Assessment Forum.

Mr. Richard McManus

Richard McManus served as a senior technical advisor and defense strategist at United States Strategic Command for over ten years where he championed integrated deterrence as a crucial component of our nation's defense. He is responsible for developing and coordinating innovative deterrence strategies designed to preserve U.S. and allied military advantages while managing escalation risk. Richard, more commonly know as "Lefty," recently accepted a position as the Deputy Director of the Force Design Integration Office at the Space Warfighting Analysis Center in Colorado Springs, Colorado.

Richard holds degrees from University of West Florida, University of Notre Dame, and Air University. He is a graduate of Army Command General Staff College and Air Force School of Advanced Air and Space Studies.

Strategic Multilayer Assessment
Joint Staff, Deputy Director of Global Operations (DDGO)

E stablished in 2000, Strategic Multilayer Assessment (SMA) provides planning and decision support to combatant commands and other U.S. government (USG) departments and agencies.

SMA's mission is to enable decision makers to develop more cogent and effective strategy and doctrine, bridging the gap between the academic research community and operators and planners.

SMA addresses complex operational or technical challenges that transcend typical department boundaries and lie outside the core competencies or expertise of a single command or agency. SMA executes projects that require mixed method, multidisciplinary approaches and creates teams combining expertise from across the USG, academia, international partners, and the private sector. SMA is agnostic to outcome, emphasizing scientific rigor and thorough examination and analysis. SMA does not write policy, plans, or doctrine and does not perform intelligence analysis.

SMA mission areas include, but are not limited to: information operations, counterproliferation, fragile state dynamics, countering violent extremism, gray zone, strategic and great power competition, warfighter technology gaps, and 21st century deterrence.

SMA Outreach & Events

SMA built and sustains a community of interest comprising over 5,000 individuals and has ties to 175 U.S. universities, 20 foreign universities, 14 major think tanks, and eight foreign military organizations. To join the SMA email listserv and receive notifications regarding SMA reports and upcoming events, please send your name, email address, and organization to Ms. Mariah Yager (mariah.c.yager.ctr@mail.mil).

SMA holds weekly speaker series events featuring leading experts discussing emerging national security challenges facing the combatant commands, the Joint Force, U.S. allies, and the world. Access the event archives, which include audio or video recordings when available, written summaries of presentations, and speaker bios and briefing materials, at https://nsiteam.com/sma-speaker-series/

SMA Publications

Available on the open Internet: https://nsiteam.com/sma-publications/

Available on NIPR (IntelDocs) requiring CAC/PIV certificate: https://go.intelink.gov/QzR772f

For any questions, please contact Ms. Mariah Yager, JS J3, SMA (mariah.c.yager.ctr@mail.mil).