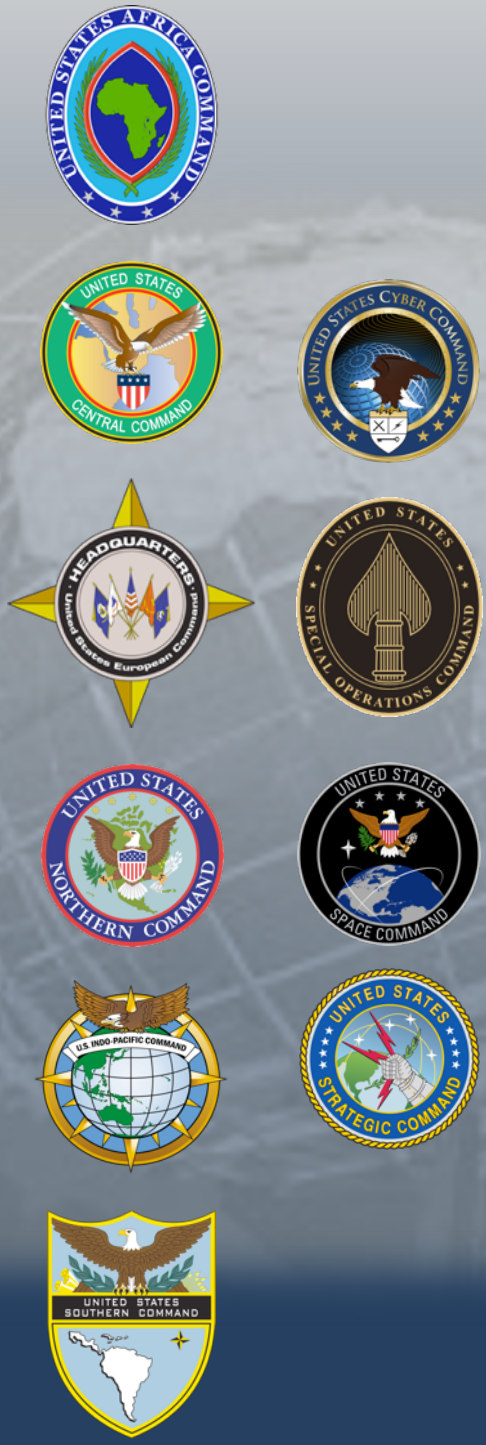
Emerging Strategic & Geopolitical Challenges: Operational Implications for US Combatant Commands

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

November 2022

APPROVED FOR PUBLIC RELEASE



SMA Perspectives

Emergent Issues for US 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 US government. Our hope is that the ideas presented in this series expand the readers' strategic horizons and inform better strategic choices.

Contributing Commands

USAFRICOM; USCENTCOM; USCYBERCOM; USEUCOM; USINDOPACOM; NORAD and USNORTHCOM; USSOCOM; USSOUTHCOM; USSPACECOM; 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, J39, 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 US Government. The purpose of this series is to expose a range of views and stimulate thinking on ways to address challenges that the US 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

In this report titled "Emerging Strategic & Geopolitical Challenges: Operational Implications for US Combatant Commands," ten military Combatant Commands provide overviews of the challenges they face in their respective areas of responsibility (AORs) and how they plan to ameliorate the risks and maximize the opportunities that these challenges present. The report provides the Commands a platform to articulate how they plan to manage the multiplicity of challenges they face. By doing so, it helps identify the types of capabilities and activities the Services must be able to plan for and field in defense of US interests in a competitive future international environment.

It is hoped that these viewpoints, when circulated among a wider public that includes academics and think tanks, etc., will help these communities prioritize their research efforts.

In her introductory section, Dr. Belinda Bragg, Principal Analyst at NSI, Inc., discusses concepts to establish and maintain stability in relationships that fluctuate between competition and cooperation. It highlights the clear need for a "new" security concept designed to maintain strategic stability and promote US national objectives; one that is a blend of legacy deterrence thinking, expanded thoughts on escalation management, and the concept of managing activities along a cooperation-competition-conflict continuum.

Brief Summary of Key Themes Articulated by the Commands

The following quote by USSTRATCOM Commander Admiral Charles Richard best exemplifies the security dilemma articulated by several Commands:

> *We face the difficulty of deterring two peer adversaries at the same time, who must be deterred differently, both possessing the ability to unilaterally escalate a conflict to any level of violence, in any domain, worldwide, at any time, with any instrument of national power.*

To meet the challenges from these adversaries, one must consider their global reach. Many of the biggest threats we face respect no borders or walls and must be met with collective action. All Commands advocate mutually beneficial partnerships and alliance architectures. This is best encapsulated by an African proverb provided by Robert Jones (USSOCOM): "If you want to go fast, go alone. But if you want to go far, go together."

Several Combatant Commands point out that approaches employed over the past 70 years are no longer sufficient to meet the great powers, non-state actors, and natural disasters that

threaten regional stability and US national objectives. To prevail, they argue that the Joint Force will need to "Think, Act, and Operate differently" so that the whole of US, allied, and partner interest emerges greater than the sum of its parts. In this vein, there is broad consensus regarding the need for integration of the instruments of national power to include military, economic, informational, and diplomatic power. They highlight that a key tenet of integrated deterrence is that it is not constrained by geography.

The challenge inherent in this multipolar environment is the different approach that each competitor takes. In this shift to multipolarity, the need for understanding the underlying structures of these geopolitical challenges is acute. While deterrence, and even containment, is a viable approach against a strategic challenger, relying on these approaches alone is not sufficient to protect vital US national interests when cumulative gains in day-to-day competition can shift the global distribution of power without war or the threat of war. Several Combatant Commands, particularly USSOCOM, make the point that there is a need to focus more on the roots of these problems to foster influence and enhance deterrence and resilience and less on pursuing elusive "defeats" of problematic symptoms.

The strategic impact of technology- and information-empowered populations is a game changer for great power competition. Advances in information technologies have served to shift the relative aggregate balance of power from governments to populations. These shifts are also rendering many traditional, control-based approaches to policy and security obsolete. In this dynamically changing environment, populations are the opportunity space. In this context, campaigning to gain an "information advantage" is vital, but achieving a "perception advantage" becomes paramount.

Deterrence must expand beyond preventing something from happening to preventing conflict from escalating beyond US strategic depth or capability to respond. This offers a way to address the escalation of many security challenges we face earlier in their development and risk profile. In doing so, it will broaden strategic options in terms of time, decision space, and approaches for our national decision-makers.

There is also the challenge for strategic deterrence and competition of countering contentious narratives and disinformation, especially about weapons of mass destruction (WMD), during conventional regional wars against a nuclear-armed adversary, as highlighted by Russia's "special military operation" in Ukraine. In this context, a distinction should be made between contentious narratives intended to influence US strategic deterrence and nonproliferation policies and overt and covert disinformation intended to disrupt those policies.

The section below briefly summarizes each of the contributions from the Combatant Commands. The summaries are primarily meant to entice the reader to read the full chapters, which have intentionally been kept short.

USAFRICOM

The USAFRICOM chapter opens with a statement by USAFRICOM Commander GEN Stephen J. Townsend: "Simply put, a secure and stable Africa is essential for America's security."

The authors emphasize the importance of the Continent by stating, "Africa has the potential for significant economic growth and development. It is home to the fastest growing economies and populations in the world and sits at the crossroads of international commerce and trade." They go on to succinctly state the Command objectives: "The Command advances US strategic objectives by focusing on strategic competition to maintain strategic access, prioritizing efforts that protect the homeland and US personnel on the continent, and by responding to regional crises across our area of responsibility."

They state, "Africa is a vast and diverse continent full of opportunity and promise, but also beset by challenges." They list several of these challenges.

- Violent extremist organizations (VEOs) remain a reality and continue to flourish in areas where governance is weak
- Poverty and food insecurity
- Fragile and failing states

They go on to discuss the challenges from China and Russia across the Continent, stating:

> *China and Russia's security assistance and arms sales to Africa prioritize their own gain, rather than building long-term African security capacity to strengthen governments and create political stability. Similarly, their investment activities often undermine government transparency and accountability, eroding human rights protections and US influence and access.*

They then discuss implications for US interests and national security.

- VEOs compromise security and economic investment
- Global prosperity and security require freedom of navigation
- The broader rules-based international order underwrites global prosperity and security and US influence
- Crisis response builds US reputation and influence

To address these challenges, they list key activities and capabilities.

- Security assistance and Counter-VEO (C-VEO)
- Partner training and joint exercises
- Military support to diplomacy and development
- Consistency and commitment

USCENTCOM

The chapter opens with a statement by the USCENTCOM Commander from the March 2022 posture testimony:

> *…with the recent withdrawal of U.S. forces from Afghanistan and conclusion of U.S. combat operations and transition to an advise, assist, enable mission in Iraq, many Americans may assume that CENTCOM's very reasons for being have drawn to a close. That could not be further from the truth.*

The authors—MajGen Scott F. Benedict and Ms. Christina Peters—go on to make some key observations. USCENTCOM's AOR remains one of the most dynamic places on earth and constitutes geostrategic key terrain that makes it a decisive theater for competition with major US strategic competitors. Some of the most immediate and credible threats to the US homeland continue to emanate from the USCENTCOM AOR. Therefore, when it comes to US national strategy, USCENTCOM advocates we should not constrain warfighting by domain or geography. National strategies should have global focus to address globally capable competitors, like China and Russia, anywhere they seek to undermine US national interests. A strategy that does not account for the importance of the Middle East is missing a key component required to successfully compete globally. They also highlight that a key tenet of integrated deterrence is that it is not constrained by geography.

The chapter goes on to raise two areas of concern with the current US national military and defense strategies.

- Focus on the two priority challenges (i.e., China and Russia) does not account for their global reach, which includes other geographic regions beyond USINDOPACOM and USEUCOM.
- The idea that 'assurance should not be gained through posture' conflates posture with forces; posture is a combination of forces, footprints, and agreements. They go on to state that, as we reduce force levels, we must find ways to preserve the other elements of posture. They emphatically state that maintaining a sufficient and sustainable presence in the central region is critical to preserving security relationships that will further our national interests. They also argue that mutually beneficial partnerships and alliance architectures are our greatest strategic advantage.

Additionally, they make the point that if we do not ensure effective and timely delivery of needed weapons to our security partners, it will inevitably lead to the US ceding its position as the partner of choice. They also state that delays in foreign military sales —combined with reductions in US capabilities across the region—exacerbates perceptions of wavering US commitment to security and stability in the USCENTCOM AOR. They advocate for continued resourcing of various defense-wide partner nation support programs and for increased emphasis on improving partners' collective defensive capabilities by building and maintaining

multilateral constructs. They highlight the threat posed by uncrewed aerial systems. They conclude by strongly advocating for USCENTCOM to be able to campaign and conduct combined operations and exercises forward, creatively employ multilateral constructs, retain appropriate manning and funding, and remain operationally ready to meet an uncertain and unstable future.

USCYBERCOM

In his opening paragraph, Mr. Mike Clark states,

> US Cyber Command (USCYBERCOM) directs, synchronizes, and coordinates cyberspace planning and operations to defend and advance national interests. The Command plans, de-conflicts, executes, and assesses cyberspace operations in coordination with, or in support of, other Combatant Commands (CCMD), allies and partners, and as directed, other entities across the full spectrum of competition to conflict.

He goes on to say that the security of the United States and our allies depends on international stability and global prosperity. Military superiority in the air, land, maritime, cyber, and space domains is critical to our ability to defend our interests and protect our values. Decades of misreading the cyber strategic environment placed the United States in a reactive posture and resulted in a policy of restraint and inaction. Today the United States risks preparing for a war that might never come while neglecting strategic gain being made by competitors and adversaries in the cyber domain. He goes on to say that while deterrence, and even containment, is a viable approach against a strategic challenger (as during the Cold War), relying on these approaches is insufficient to protect vital US national interests when cumulative gains in day-to-day competition can shift the global distribution of power without war or the threat of war. He concludes by stating that the Command's overarching goal is to posture its forces and capabilities to provide senior national leaders diverse, non-kinetic options throughout the entire spectrum of competition and conflict while simultaneously securing, operating, and defending the Department of Defense Information Networks (DODIN).

USEUCOM

The USEUCOM authors state unequivocally that the Command's primary mission is to compete, deter, and prepare to respond to aggression with the full weight of the NATO alliance. It is only by focusing on maintaining the NATO alliance, along with other key international bodies, and pursuing effective bilateral engagement that the United States can be successful at setting conditions where we can leverage the resources inherent in the USEUCOM AOR to mitigate the challenges the future will undoubtedly bring. They highlight the 50 countries and territories that constitute the US European Command AOR, which include

some of the key allies and partners that have ensured the post-World War II order. They go on to highlight several key challenges:

- Russia is a destabilizing challenge. Russia's nuclear arsenal and strike capability remain an enduring existential threat to the United States. It pursues malign activities, including military aggression aimed at undermining democracy and the rules-based international order, and it has a willingness to use force to achieve its aims.
- The second major challenge is an "increasingly assertive China" that seeks to increase its access, presence, and influence in Europe and globally. These activities provide Beijing with an avenue to assert influence at the expense of enduring US, allied, and partner interests.
- They highlight the challenge of successful VEO-inspired and organized attacks in Europe that complicate integration efforts, potentially isolating refugee and migrant communities and increasing the possibility of VEO recruitment. These attacks can then reinforce isolationist trends and distrust of international engagement.
- They next highlight the challenges brought about by climate change, which exacerbate risks to security as the physical impacts increase and geopolitical tensions mount on how to respond. They highlight that climate change will also affect the High North. As the Arctic ice sheet shrinks, it opens additional navigation routes as well as access to previously unreachable mineral resources.

USEUCOM finishes by emphasizing the importance of allies and partners in any security endeavor. Key points include: 1) that the strength of the NATO alliance is the "alliance" and 2) that their most concerning challenges are those that wear away and erode these organizations which, while seemingly reinforcing individual sovereignty, allow the cornerstones of European multilateralism to atrophy into ineffectiveness. This focus on working with allies and partners is nested within the interim national security guidance, which states, "[r]ecent events show all too clearly that many of the biggest threats we face respect no borders or walls and must be met with collective action." USEUCOM then concludes by stating that maintaining a capable US presence in Europe strengthens our national security by generating peace, unity, and cohesion among Europe's sovereign nations.

USINDOPACOM

In their opening statement, the authors describe the importance of the Indo-Pacific to the national security of the United States, stating that it is home to more than half of the world's population, responsible for nearly two-thirds of global economic output, and host to more members of the Joint Force than any other region aside from the United States itself. They also characterize the region as one that is critical to global prosperity moving forward: It is a region filled with promise: 58% of the world's youth population resides in the Indo-Pacific, and it is a region that is projected to account for two-thirds of global economic growth in the years ahead.

Yet the authors also characterize the USINDPACOM AOR as home to a broad array of threats: six of the world's nine declared nuclear powers, seven of the ten largest militaries on the planet, and four of the five primary threats identified in the Department of Defense's 2022 National Defense Strategy Fact Sheet: The People's Republic of China (PRC), Russia, North Korea, and violent extremist organizations (VEOs).

They note specific areas of concern with respect to each but devote much of their essay to describing the challenge presented by the PRC, the Department's "most consequential strategic competitor" and its "pacing challenge" with respect to planning, programming, budgeting, capabilities development, and force modernization. Beijing, they note, has pursued a decades-long program of reform and modernization intended to develop the power projection capabilities necessary to compel unification with Taiwan by force, enable the PRC to project power globally, and provide Beijing with the means to threaten the US Homeland.

Turning to how USINDOPACOM works to addresses these challenges, the authors note that the Command employs a broad array of posture initiatives, operations, exercises, security cooperation activities, and key leader engagements that are aligned toward common goals to prevent conflict by deterring US adversaries, and should deterrence fail, ensure that the Joint Force is prepared to fight and win. The authors then detail how each element of their approach contributes to this goal of preventing conflict and ensuring the Joint Force remains positioned to prevail should conflict break out.

NORAD and USNORTHCOM

To open, the authors—Mr. James M. Jenista and Mr. William J. A. "Joe" Miller—state that, in close "Tri Command" coordination with Canadian Joint Operations Command (CJOC), the Commands provide the full spectrum of defense and military support and cooperation for the US and Canadian homelands. They point to the non-native origins of the apex challenges and assert that, therefore, the best way to defend the homeland is to organize, resource, and compete (and, if necessary, fight) forward—indeed, globally. They go on to state the response must be globally integrated from the outset, in design, intent, and the distribution of resources, to achieve the strategic effects that will manifest in regional and local decisions and actions aligned to our interests and those of our allies and partners. In this vein, they state that our Commands, Services, Agencies, partners, and allies must synchronize and bring to bear our respective capabilities in a comprehensive, layered defense, one that integrates all forms of power, persuasion, and deterrence into a coherent whole. They conclude by stating that achieving those goals will mean unwavering national and collective will, singular mission focus, and leading-edge, mutually reinforcing technologies. The first steps in that direction, though still short of the stride we will eventually achieve, will signal our commitment to the task at hand.

USSOCOM

In his chapter, Mr. Robert Jones states that one of the great strengths of US Special Operations Forces (SOF) is the broad diversity of organizations, each with their own distinct culture and set of capabilities. He goes on to say that the challenge at USSOCOM, with the help of Special Operations/Low Intensity Conflict (SO/LIC), is to integrate, optimize, and direct those capabilities for new purpose. In this context, the Command vision is to create strategic, asymmetric advantages for the Nation in integrated deterrence as well as crisis and conflict. He lists the challenges and problems the US is facing and states that there is need to focus more upon the roots of these problems to foster influence and enhance deterrence and resilience and less on pursuing elusive "defeats" of problematic symptoms. He refers to previous documents that postulate how advances in information technologies had served to shift the relative aggregate balance of power from governments to populations. He states that the shifts driving quests for change were also rendering many traditional, control-based approaches to policy and security obsolete and that the rapid shifts in power driving change and fueling conflicts a century ago are vastly accelerated in this modern information age. We must reassess and reframe the problems we face and craft new solutions more appropriate for the world emerging around us. In this dynamically changing environment and for Joint SOF in particular, populations are the opportunity space. In this context, campaigning to gain an "information advantage" is vital, but achieving a "perception advantage" becomes paramount.

He refers to the *Joint SOF Operating Concept 2040*, which articulates a foundational supporting idea that strategic influence is through irregular warfare. He goes on to state that the strategic impact of technology- and information-empowered populations is a game changer for strategic competition. He makes a strong case for ensuring our deterrence efforts are fully integrated in every way, across all of the elements of government, across our vast network of allies and partners, across all of the traditional and emergent domains of activity, and across the spectrum of conflict and competition. He states that Joint SOF is uniquely suited to provide a new suite of highly effective, low-risk activities to help lower the threshold of deterrence and compress this gray space and, by campaigning for strategic influence, Joint SOF helps contribute to all aspects of advancing interests, deterring conflict, and posturing for success in myriad subtle ways. In facing one's revisionist opponents, who continuously test the limits of what they can accomplish short of war, he quotes an African proverb, which advises, "If you want to go fast, go alone. But if you want to go far, go together." In this context the US—working closely with the central states in the "Western" system—remains the best option for advancing and securing a stable world order.

USSOCOM appreciates how Joint SOF plays a unique and powerful role in helping lower the threshold of deterrence, reduce the likelihood of conflict, foster resilience, and help sustain an evolving world order. He ends his chapter by stating:

> *Now the task is to make those evolutionary changes. Now is the time to reframe and refine how we understand the challenges before us. Now is the time to craft new campaigns and to refine and rebalance the force for new approaches, new purposes, and new effects. This will be no easy task, but one fully embraced by the men and women of United States Special Operations Command.*

Dr. Robert Toguchi discusses an expanding role for Army Special Operations Forces (ARSOF) in deterrence. In an increasingly volatile environment where prevention may no longer be possible, he notes that deterrence must expand beyond preventing something from happening—to preventing conflict from escalating beyond the US strategic depth or capability to respond, in a manner consistent with our national values. Dr. Toguchi contends that an evolving concept of deterrence must consider thinking beyond high-end conventional or nuclear capabilities, and consider approaches such as irregular warfare across the spectrum of conflict. Although the pre-conflict space of global competition will continue to be led by the State Department, national guidance suggests that DoD support to a broader approach is needed. The DoD possesses unique capabilities to assess, sort, form a response, and rescale security threats before they escalate beyond the Nation's strategic depth and ability to respond. Further, Dr. Toguchi notes that deterrence can be defined as the prevention of adversary action through the signaling or use of credible physical, cognitive, and information capabilities that raise an adversary's perceived cost to an unacceptable level of risk relative to the expected benefit. To emphasize this line of thinking, Dr. Toguchi explores five broad conceptual lines of effort to strengthen deterrence, which include the following:

- Expanding the strategic start point
- Rethinking strategic power and reframing power projection with two sub-components, partner-based power and population-based power
- Gaining an information advantage
- Rethinking asymmetric approaches
- Expanding technology solutions for irregular warfare

In addition to these lines of effort, Dr. Toguchi highlights several emerging ARSOF conceptual initiatives in the areas of the SOF-Cyber-Space Triad: the need for a trans-regional convergence headquarters, advances in cognitive targeting, and new methods to achieve information advantage.

In their chapter, "Contentious narratives and disinformation about nuclear weapons in strategic deterrence and competition: A SOF perspective," the authors—Ms. Lesley Kucharski, Dr. Zachary Davis, and MAJ Trisha Wyman—discuss the challenge for strategic deterrence and competition of countering contentious narratives and disinformation about WMD during conventional regional wars against a nuclear-armed adversary, as highlighted by Russia's "special military operation" in Ukraine. They make a case for how SOF can contribute to strategic deterrence and competition objectives, specifically by countering adversary gray zone information efforts to alter regional security orders. In this context, they make a distinction

between contentious narratives intended to influence US strategic deterrence and nonproliferation policies and overt and covert disinformation intended to disrupt those policies. They define contentious narratives as being considered within the normative bounds of diplomacy, deterrence, and competition. The latter constitutes disinformation, which is outside the normative bounds of these traditional processes of statecraft, at least for democratic governments. Their analysis indicates Russia employs a mix of contentious narratives and disinformation about Ukrainian nuclear weapon ambitions across the global and local Russian-language information ecosystems. They suggest Moscow may have different strategic objectives for each audience. They go on to discuss a role for USSOCOM in addressing contentious narratives and disinformation about WMD. They point out that contentious narratives and disinformation about nuclear weapons and nuclear safety and security have global implications. They state contentious narratives and disinformation aimed at joint training of NATO and partner SOF forces, emergency preparedness exercises, or chemical, biological, radiological, and nuclear (CBRN) training could create confusion and controversy about SOF activities in Europe and beyond. In this context, they recommend three lines of effort:

- expand support of global multi-domain operations by standing up an Information Warfare Task Force on Weapons of Mass Destruction;
- establish mechanisms for quickly coordinating with other entities that have equities in countering contentious narratives and disinformation about WMD; and
- conduct information campaigns to counter contentious narratives and disinformation about WMD in coordination with WMD subject matter experts.

They conclude by stating USSOCOM can play a key role by creating synergies between its psychological operations (PSYOP) and counter-proliferation missions and coordinating with relevant stakeholders across the US Government (USG).

USSOUTHCOM

In his opening paragraph, the author states "Latin America and the Caribbean (LAC)—our shared neighborhood—is under assault from a host of cross-cutting, transboundary challenges that directly threaten our own homeland. Countering these threats requires greater US attention, commitment, and investment to reverse the current disturbing trends." He then focuses on several such challenges.

- The PRC continues its relentless march to expand its economic, diplomatic, technological, informational, and military influence in LAC and challenges US influence in all these areas. To date, 21 regional countries participate in the PRC's Belt and Road Initiative (BRI).
- Russia is expanding its influence in this region, engaging in extensive disinformation campaigns to influence key national elections throughout the region.

- Transnational Criminal Organizations (TCOs) operate nearly uncontested and blaze a trail of corruption and violence. TCOs create conditions that allow the PRC and Russia to exploit and threaten citizen security and undermine public confidence in government institutions.
- Regional authoritarian regimes (i.e., Venezuela, Cuba, Nicaragua, etc…) remain a regional corrosive influence, receiving political, military, and economic support from malign actors like China and Russia.
- Climate change is another regional challenge. Hurricanes, rising sea levels, flooding, and drought are worsening economic and food security and contributing to irregular migration in the region.

He goes on to describe how the Command is addressing these cross-cutting challenges by building partner nation capacity in counternarcotics, cyber, space, and counterterrorism. These include: annual exercises, security cooperation, building partnerships, cybersecurity, space cooperation, humanitarian assistance/disaster relief (HA/DR), maintaining the innovative edge, and climate defense. He discusses capabilities needed, such as intelligence, surveillance, and reconnaissance, as well as "Piercing the IO Space." He concludes by stating that to meet these challenges, we are putting integrated deterrence into action, using all available levers—assets, resources, and authorities—across the DoD, interagency, allies, partners, non-governmental organizations (NGOs), and private industry to fulfill our Enduring Promise to be the region's trusted partner—today, tomorrow, and always.

USSPACECOM

In their opening paragraph, Col (Ret) André Shappell and Lt Col Jean A. Purgason state emphatically that "Space is the 'eyes and ears,' and arguably the 'heart' of Integrated Deterrence." They point out the Command has a mandate "to protect and defend our national orbital assets and the space commons in general." They go on to state "Space plays a vital—and arguably the central—role in any strategy outlining the coherent use of all instruments of national and allied power to deter adversaries, assure allies, and protect strategic stability." As such, the Command's fundamental objective remains to "deter a conflict from beginning in or extending into space." They identify the Command's primary operational challenge as "gaining space superiority and the ability to maintain a comprehensive common operating picture of the space Area of Responsibility (AOR)." In this context, the Command's priority is to "enhance Space Domain Awareness (SDA) capabilities." They point out that SDA acts as a combat enabler to the terrestrial warfighter and that protecting decision space for national leaders through advanced indications and warning would prove decisive for effective mitigation and counteraction. Furthermore, "given the size of their AOR, there are limits to their ability to continuously monitor wide swaths of the domain" and that "constantly tracking objects in orbit is hard." Accordingly, the Command is looking for "new ways to expand sensor coverage by adding non-traditional SDA sensors currently used in other mission areas." They point out the pursuit of space superiority requires different approaches depending on where

the need is within the domain. Ensuring near real-time data to terrestrial users, especially in times of conflict, will be a deciding factor in an engagement or campaign. They mention instances where China has made technical advances and state that "without the US and allies developing similar capabilities will result in us ceding information superiority and likely space superiority to China." They stress the need to "continue building a range of options from which national leadership can choose to protect and defend space operations." In this context, they identify areas where advances are critically needed and state "the strategic space environment is evolving too rapidly to wait any longer." They state emphatically "the US, its allies and partners must invest their efforts and resources into ensuring we can gain and maintain space superiority in a time, place, and manner of our choosing."

They conclude by stating "robust space superiority places our coalition forces in a position of strength to deter adversaries from attacking our space assets and reduces the chances of in-domain escalation."

USSTRATCOM

In her chapter titled "The Challenge of a Multipolar World," Ms. Julie McNally quotes from a statement by USSTRATCOM Commander Admiral Charles Richard:

> *[W]e currently are operating under crisis deterrence dynamics, and the nation has received thinly veiled nuclear threats by the leader of a nuclear power. We face the difficulty of deterring two peer adversaries at the same time, who must be deterred differently, both possessing the ability to unilaterally escalate a conflict to any level of violence, in any domain, worldwide, at any time, with any instrument of national power.*

She goes on to state that there is persistent strategic competition across the diplomatic, information, military, and economic (DIME) levers of national power, presenting the quandary of deterring both Russia and China simultaneously. She asserts that the development of a spectrum of nuclear capabilities affords Russia the opportunity to threaten Europe with non-accountable nuclear weapons while holding the United States at risk with strategic nuclear weapons. She notes the lack of response options in US and NATO nuclear arsenals if Russia were to use a low yield nuclear weapon. In discussing the PRC, she draws attention to the combination of increasing nuclear capabilities and indications of the People's Liberation Army (PLA) reassessing their posture and doctrine that have implications for US strategic deterrence.

The challenges inherent in this multipolar environment are the different approaches that each competitor takes (opacity and fluidity of the PRC vs. clear and confrontational Russian messaging about capabilities development and doctrine) and the convergence or alignment of interests between the PRC and Russia per their strategic partnership. Chinese officials recently described this partnership as having "no limits" and signaled clear support for the Russian position against an expansion of NATO while receiving Russian support for the view

that the US involvement in the Indo-Pacific theater is illegitimate. In this shift to multipolarity, the need for understanding the underlying structures of these geopolitical challenges is acute.

She goes on to say that in recognition of these challenges, ADM Richard established an Analytic Agenda for the Command to identify key research needs and connect strategic deterrence researchers with the practitioners in USSTRATCOM. These research efforts pursue the understanding and modeling of the multipolar environment and the subsequent development of strategies for deterrence within it. The Command is also actively engaged in collaboratively developing the integrated deterrence framework and is working toward how to implement it. She concludes by stating that these cognitive efforts to address multipolarity through understanding nuclear risks, new and emerging problem sets, and ultimately developing new strategies for deterring multiple competitors are strong approaches to maintaining relative advantage in this era of strategic competition.

Conclusion

In his closing chapter, Lt Gen (Ret) Timothy Fay provides a Global Summary of Combatant Command Perspectives. He starts off by stating that all of the Commands represented in this paper did an excellent job communicating the perspective of their security environments and how they are working to deter, compete, and be prepared to win. He goes on to state that the convergence on the perception of the pacing threats and the implications for deterrence in this evolving security environment is a common theme best captured by the USSTRATCOM Commander, Admiral Charles "Chaz" Richards (quoted in the USSTRATCOM Chapter). He observes that when considered as a whole, the similarities and convergence are remarkable.

Specifically, he highlights the following areas of convergence:

- The two peer adversaries (Russia and China) must be deterred differently and at the same time, which requires deep knowledge and a cultural-level understanding of our adversaries. This is essential to our deterrence strategy. He observes that this emerging deterrence challenge requires significant and immediate intellectual investment.
- Both adversaries can escalate across domains, time, and space employing any and all instruments of their national power.
- The strategic advantage of our alliances and partnerships is a final common thread from all Commands. He states that the Commands identify this as not only a strategic advantage for the United States, but some consider it a potential weakness of our adversaries.

He does identify some notable differences. In one instance, he states that there may be some divergence on the primacy of the "ways" to best deter. Specifically, there was varied discussion with respect to the primacy of a force designed for current daily competition versus a force designed to deter and win a high-end conflict. The second difference involves the preponderance of force types. He states that it is likely that the cause of these minor

divergences is partially driven by the understandable tension between mission assigned and resources allocated.

He highlights the major element that was largely unaddressed has to do with the allocation of resources. In this context, he states that while the allocation of scarce resources relative to priority and risk was implicitly addressed by some in this discussion, there was not an explicit discussion.

He concludes by stating "…this collection of Command perspectives is remarkable. The level of convergence on threats, priorities and challenges is impressive. While there are divergences and omissions, they are minor and not strategic in nature."

Introduction

Dr. Belinda Bragg
NSI Inc.
bbragg@nsiteam.com

The Cooperation-Conflict Paradigm

The first SMA perspectives report in this series, Present and Future Challenges to Maintaining Balance Between Global Cooperation and Competition, discusses concepts to establish and maintain stability in relationships that fluctuate between competition and cooperation. It highlights the clear need for a "new" security concept that is a blend of legacy deterrence thinking, expanded thoughts on escalation management, and the concept of managing activities along a cooperation-competition-conflict continuum, with the purpose of maintaining strategic stability while promoting US national objectives.

Compatibility of interests is what differentiates cooperation from competition and conflict

In the 21st century, it is the strategic environment itself, rather than any ideological or political differences, that generates threats and conflict, particularly among major power competitors. Whether actors are at peace, in competition, or engaged in warfare at different times or simultaneously is a function of the interactions between their specific interests. These relationships can be described along a spectrum of increasing opposition, starting from zero, in which specific actor interests are complementary or "cooperative," in competition, or in conflict as the degree of opposition increases. As all actors have multiple interests, an important feature of this view is that the United States can simultaneously have cooperative and conflictual interests with the same actor. Thus, thinking of international actors only as perpetual "adversaries" or "friends" (on all issues) prematurely constrains and can undermine the effectiveness of US options.

If competition is a contest for advantage, leverage, and influence among relevant actors and populations to protect or advance their interests, the United States needs to build trust and strategic empathy with its allies and partners. Increasingly, US interest in promoting stability and maintaining the rules-based international order is challenged by the opportunistic behavior of its major power competitors. Successful deterrence in this context requires a deep understanding not only of the interests and intent of our competitors, but also of our allies and partners.

Competition below the level of armed conflict dominates the strategic environment

US competitors are increasingly willing and able to pursue aggressive policies and actions that are reshaping international security dynamics, while remaining relatively confident that they can manage the risk of great power armed conflict by staying below the United States'

threshold for military response. To be effective, the United States cannot reenact Cold War strategies but must find a better balance of activities defined by a refreshed perspective that takes stock of present dynamics and unique challenges on the horizon. Given competition is now a constant within the system, consistent engagement by the United States is necessary. Avoiding conflict and encouraging cooperation in today's environment will require communication and negotiation with even greater granularity than in the past, given the "shades of gray" in which international political, military, economic, social, and information activities will be conducted.

Managing Competition with China

The second SMA Perspectives report in this series, US versus China: Promoting 'Constructive Competition' to Avoid 'Destructive Competition', addresses the key challenges that the US must manage so that potential conflict between the United States and China stays below the level of destructive competition and armed conflict.

Constructive versus destructive competition

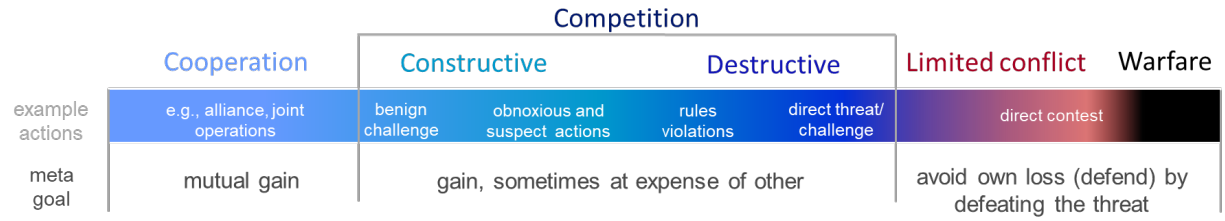


Figure 1. Expanded competitive continuum and meta objectives

Constructive competition is a "state in which actors see their interests on a particular issue to be in opposition but not a threat." Constructive competition is "tolerable and productive," and it is "the ideal mode in a dynamic global system, as it stimulates innovation and movement" (Astorino-Courtois, 2019). Cooperation between parties, where practical, promotes constructive competition because the parties see value in using competition to benefit their goals and objectives. Destructive competition, on the other hand, is a state in which actors see their interests on a particular issue to be in opposition and potentially (or actually) a threat to their interests. When vital interests are threatened, destructive competition has the potential to escalate to direct confrontation, which, left unchecked, could further escalate to a state of conflict (Astorino-Courtois, 2019; Astorino-Courtois, 2021).

Understanding interests can reduce the risk of escalation to destructive competition

The United States can encourage China to conduct activities that avoid escalation toward confrontation or conflict by enabling a range of alternative courses of action in which China can execute that offer the advantage of protecting the vital interests of the Chinese

government, the United States, and their partners. Cooperation in areas where the US and Chinese government have shared interests provides vehicles for communication that can foster "constructive competition," provide vehicles to control escalation, and reduce the potential for a rise in tensions leading to direct confrontation or even conflict.

The contributors hold various views on the scope for cooperation or constructive competition between the United States and China; however, US relative power advantage, especially military, is generally accepted as a source of threat to the CCP, and US policy to be inimical to China's achievement of its domestic and foreign policy goals.

While none of the contributors see a fundamental change in China's strategy or goals to be realistic, this does not make destructive competition or conflict inevitable. They offer several recommendations for managing competition:

- *understand* the interests that are driving China's actions so potential areas for constructive interaction (e.g., global governance) can be opened up, and the United States' ability to influence China's decision calculus is increased;
- *demonstrate* willingness to cooperate where and when US and Chinese interests align;
- *counter* the challenge of China's soft power through the development of a US soft power strategy;
- *signal* to allies and partners that the United States is able and willing to shield them from Chinese leverage across all domains (e.g., economic coercion, diplomatic isolation, cyber threats), not only military attack; and
- *frustrate* China's cyber activities and maintain an open internet rather than restricting Chinese telecommunications networks.

Initial management challenge: Careful analysis of the context, flexibility, and differentiation

When the United States and China compete over a specific issue, the first management challenge is to determine what is needed in order to compete on that issue. Is the competitive context such that promoting US interests can only be accomplished if the United States possesses greater influence relative to the issue than does China? Can US interests be served if US influence is equal to China's, or is it possible to promote US interests sufficiently even if the United States maintains inferior capability to influence the outcome? How the United States decides to see China's versus its own place in the world will condition which actions we think are appropriate competitive actions. If we decide that dominance on all domains is the best way forward, the United States must be prepared to enter into an arms race in the space or cyber domains. If we decide a balance of power or regional spheres of interest are the most desired states, substantial re-articulation of US policy vis-à-vis Taiwan and China's regional economic activities will emerge.

Anticipating the Future Operational Environment

Over the coming years, the Joint Force will operate in a strategic environment characterized by a wide-ranging and interdependent set of global "*apex" challenges* that US adversaries can exploit to pose direct threats to US and ally security. These include accelerating climate change, disease transmission, and other biological risks that kill millions and sow popular unrest; state fragility and the appeal of extremist ideologies; cyber threats that interfere with defensive signaling and can diminish the strength of US and ally deterrence; and increasing potential for rapid outbreak of global financial crises or use of economic coercion to "win without fighting."

Even in an environment of persistent competition, however, there is potential for cooperation. The broader our understanding of the operational environment, and the deeper our understanding of the interests that drive the actions of actors (both adversaries and partners) in that environment, the more likely we are to identify such opportunities.

The Army Training and Doctrine Command's (TRADOC G-2) work focusing on "Exploitation of Strategic Conditions 2035" identifies 24 conditions of the future operational environment that can be expected to affect threats to and opportunities for US national interests and security. How these general conditions manifest will vary between and among AORs, creating different challenges, opportunities, and areas of focus for the Commands.

TRADOC 24 Conditions	
Climate Change	Diverse Technology Actors
Competing Narratives	Dominance of Cities
Contested Spaces	Economic Inequalities
Erosion of the Liberal World Order	Effects of Urbanization
Multi-Polar World	Factionalized and Polarized Societies
New International Cooperation Models	Fragile and Failing States
Persistent State of Competition	Infrastructure Capacity Challenges
Crypto-Technology Use	Interconnected Economies
Information Communication Technology Ubiquity	Resource Competition
Technology-Reliant Societies	Specialized Economies
Demographic Pressures	Technology Access Gaps
Disease Evolution	Use of Proxies

This current report builds from previous work, presenting Command perspectives on the types of capabilities and activities the services must be able to plan for and field in defense of US interests in a competitive future international environment.

United States Africa Command (USAFRICOM)

"Simply put, a secure and stable Africa is essential for America's security"

GEN Stephen J. Townsend, USA, Commander USAFRICOM

Except where noted in the text, all of the material in this paper is drawn from official US Africa Command statements, primarily the January 30, 2020, and March 15, 2022 statements of General Townsend, Commander, USAFRICOM, before the Senate Armed Services Committee. The analysis was executed by Dr. Bragg and Dr. Cabayan to address the questions posed for this volume.

Background

Africa has the potential for significant economic growth & development. It is home to the fastest growing economies and populations in the world and sits at crossroads of international commerce and trade. Over half of the world's farming land is in Africa, and when effectively managed, Africa's population growth and rich natural resources can drive progress. However, a minimum-security threshold must be met for diplomacy to work, economies to flourish, and development efforts to take root. Currently, the activities and influence of VEOs threaten the security and stability of our African partners, our allies, US commercial and security interests, and US citizens. Enhanced security will foster development and investment. US initiatives such as the Millennium Challenge Corporation, Prosper Africa, and the Better Utilization of Investments Leading to Development (BUILD) Act encourage US companies to invest in Africa, providing a counterweight to China's increased economic engagement in the region.

Africa sits at crossroads of international commerce and trade and watches over the world's most important sea lines of communication. The United States plays a unique role in ensuring freedom of navigation for all along these strategic routes. Future US security, prosperity, and strategic access in times of crisis rests on free, open, and secure sea and air lines of communication around Africa.

US Africa Command Objectives

The Command advances US strategic objectives by focusing on strategic competition to maintain strategic access, prioritizing efforts that protect the homeland and US personnel on the continent, and responding to regional crises across our AOR. For US Africa Command, the countering violent extremist organizations (C-VEO) fight is a key component of strategic competition. Our experience, training, equipment, advice, and other unique capabilities support C-VEO efforts led by our allies and partners and—by addressing immediate partner needs—build relationships for the future.

African Continental Challenges

Africa is a vast and diverse continent full of opportunity and promise but also beset by challenges. Violent extremist organizations (VEOs) remain a reality and continue flourishing in areas where governance is weak. All are aided in their objectives by the prevalence of poverty and the lack of economic opportunity across much of the continent. These challenges persist despite Africa's natural resource wealth and pockets of fast economic growth, and they are amplified by the combined impact of climate change and demographic pressures.

Poverty and Food Insecurity

Although poverty levels in most African countries declined from 40 percent to 34 percent between 2010 and 2019, the COVID pandemic drove an increase in poverty, with 490 million people now estimated to live in poverty across the continent (United Nations Conference on Trade and Economic Development, 2021). Poverty and food insecurity are exacerbated by a constellation of conditions.

Climate change has already altered weather patterns, which have in turn affected crop production. In combination with natural resource degradation, climate change has also increased the prevalence of pathogens, and thus the likelihood of disease outbreaks. Lack of economic opportunity increases poverty and food insecurity directly and also increases the number of people who move within their country in search of a better life. Such internal displacement is itself both a direct cause and direct effect of poverty and food insecurity, and it creates competition and conflict over scarce resources. The combined result of these patterns has been an uptick in migration out of the region (especially to Europe) and the creation of a lucrative market for VEOs and criminal networks within Africa.

Looking to the future, these challenges are only set to be intensify as the population continues to grow. By 2050, Africa's population is projected to double, and more than a quarter of the world's inhabitants will live on the continent. By 2100, the population is expected to double again (United Nations Department of Economic and Social Affairs, 2019). Climate change is projected to trigger more extreme weather events and further sea level rise, creating more challenging conditions for agricultural production. If left unaddressed, these two conditions (climate change and population growth) will drive ever-increasing rates of poverty and food insecurity across the region.

Fragile and Failing States

Violent extremist organizations (VEOs) are expanding at a rapid pace in much of Africa, enabled in large part by weak governance. In general, African governments regard VEOs as near-term threats to their governing capacity. VEO violence exacerbates despair and hopelessness, stoking communal conflicts and undermining trust in local governments and militaries. VEO violence also depresses economic activity and investment, further weakening governing and military capacity and driving political instability.

ISIS and other spoilers look to exploit long-simmering grievances and gaps in governance within the region. Fragile and failing states are the ideal environment for VEOs; the security vacuums created by regional conflicts, such as the civil war in Libya, present powerful opportunities for VEOs to expand their influence. As state power recedes, VEOs can move in to fill security and public service voids while expanding their radical ideology.

While al-Shabaab is most dangerous for US interests today, ISIS is rapidly franchising VEOs in all corners of Africa. Furthermore, in the Sahel and Lake Chad, Al Qaeda and ISIS networks are working together to exploit weak regional governance and overextended militaries, as well as marginalized populations and porous borders. VEO violence in Burkina Faso, Mali, and western Niger has increased 250 percent since 2018. Having quickly spread from northern Mali, Al Qaeda's JNIM, ISIS-aligned groups, and other VEOs are now operating throughout the Sahel region.

The massive population growth projected for Africa in the following decades will further strain resources and governing services. Unless regional governments can respond adequately and create economic opportunity, surges in migration to Europe and elsewhere are likely, as are increased political instability, communal conflict, trans-regional terrorism, and the further marginalization of already vulnerable populations.

The Challenge from China and Russia

China and Russia's security assistance and arms sales to Africa prioritize their own gain, rather than building long-term African security capacity to strengthen governments and create political stability. Similarly, their investment activities often undermine government transparency and accountability, eroding human rights protections and US influence and access.

China and Russia, recognizing the strategic and economic importance of Africa, continue to exploit opportunities to expand their influence across the continent.

China and Russia are in a position of advantage in central and southern Africa. In the Central African Republic, Russia is deploying private military companies (PMCs), extracting minerals, and attempting to buy influence. China continues to invest heavily in African infrastructure, which brings some benefit to the continent through improved transportation hubs and market access, though many of its projects appear to prioritize Beijing's desire to increase its influence and military reach. China seeks to open more bases, and its unprofitable seaport investments in East Africa and Southern Africa track closely with involvement by Chinese military forces. In contrast, the US believes in investing in and fortifying our African partners to enable "African solutions to African problems"—the bedrock of long-term self-sufficiency, security, and development.

China, in particular, has also made significant efforts to increase its diplomatic presence in the region and currently maintains 52 embassies in Africa—three more than the United States and a 24 percent increase since 2012. China also leads its G20 partners in head-of-state and senior

leadership visits to the continent over the last decade. Despite their rhetoric emphasizing cooperation and mutual development, Chinese and Russian activities on the continent have been destabilizing. Their activities have also promoted a disregard for human rights and inclusive economic growth that threatens to upend the progress the Continent has seen in the last ten years.

Implications for US Interests and National Security

VEOs Compromise Security and Economic Investment

There has not been durable progress made by the international community or regional groups to contain priority VEOs in Africa. This is largely because of insufficient coordination of military activities and an imbalance between military and non-military investments. If the United States steps back from Africa, VEOs will be able to grow unchecked. Not only will we lose opportunities for increased trade and investment in Africa's fast-growing economies, but these organizations also pose a more direct threat to US interests and security. Most VEOs in Africa seek to strike at the United States in the region, and some aspire to strike the US homeland. In November 2019, al-Shabaab's leadership publicly identified Americans and US interests worldwide as priority targets—mirroring Usama bin Laden's declaration of war on the United States in 1996.

Global Prosperity & Security Require Freedom of Navigation

Located at the crossroads of the world, Africa watches over strategic choke points and sea lines of communication, including the Mediterranean Sea and the Strait of Gibraltar on NATO's southern flank, the Red Sea and the Bab al Mandeb Strait, and the Mozambique Channel. These strategic pathways are essential to global commerce: African, US, and global prosperity depend on unhindered access to these waters. The United States plays a unique role in ensuring these strategic routes remain open to all, and they are critical to the operations of most of our geographic and functional combatant commands. Our future security, prosperity, and strategic access in times of crisis rely upon free, open, and secure sea and air lines of communication around Africa.

The Broader Rules-based International Order Underwrites Global Prosperity and Security and US Influence

Africans recognize that the existing rules-based international order (RBIO) offers people everywhere the best hope for safe, secure, and prosperous lives. However, today our regional partners face increased pressure from China and Russia, who seek to weaken US influence by undermining the RBIO and increase their own influence through exploitative and ineffective economic and security assistance.

Crisis Response Builds US Reputation and Influence

Responding to regional crises across our area of responsibility is one way the United States can demonstrate the benefits of a strong, US-led RBIO. As we saw with US Africa Command support to the US Agency for International Development (USAID) for Cyclone Idai relief, recovery efforts can also open the door for future security cooperation opportunities.

Addressing These Challenges: Activities and Capabilities

Security Assistance and C-VEO

C-VEO assistance is a key tool in US Africa Command's strategic competition toolkit, especially in countries where US interests are greatest. Our principal means for applying pressure is working with our African and international partners to increase African security capabilities and information operations. Only when necessary do we use military force. We have unique experience and capabilities to support allies' and partners' C-VEO efforts, as well as provide training, equipment, and advice. By addressing immediate partner needs in this way, we also build enduring relationships; this is a distinct advantage that our competitors cannot match.

Partner Training and Joint Exercises

US-facilitated exercises offer some of the best return on investment. They provide our African partners with exposure to American values, expertise, and professionalism and advance our force readiness. US Africa Command and its component commands conduct engagements and exercises throughout the region, which are designed to strengthen key partnerships and improve partner capabilities in basic military skills, maritime security, C-VEO efforts, counter-trafficking, humanitarian assistance, disaster relief, and control of key infectious diseases. These programs improve partners' capabilities, encourage self-sufficiency, and develop opportunities for burden sharing over the long term.

Military Support to Diplomacy and Development

US Africa Command's security activities are designed to directly complement Department of State and USAID work to reduce the spread of harmful ideologies, strengthen governments' capacity to protect their citizens, and promote good governance, economic success, and stability and security. Our persistent focus on ISIS-Libya, in coordination with our interagency and African partners—and at low cost in terms of Department of Defense resources—continues to disrupt ISIS freedom of action as a regional terrorist threat. We will remain vigilant in order to counter VEO reconstitution efforts.

Consistency and Commitment

The effectiveness of our specific security assistance and training efforts is mediated by the consistency of our engagement. As strategic competition for influence in Africa continues to ramp up, building partnerships will require consistent US engagement and strong signaling of commitment. If the United States steps back, Russia and China will fill the void, for—as one

African leader recently shared—"a drowning man will accept any hand." US Africa Command's strategic approach is whole-of-government across three themes: We partner for success, compete to win, and maintain pressure on malign networks. Following our national strategic guidance to achieve US foreign policy goals, US Africa Command applies a partner-centric, interagency-based approach, dating back to the inception of the Command in 2007. We must Partner for Success with a diverse network that includes African nations, strategic allies, US government agencies and departments, and multinational coalitions in order to prevent, address, and mitigate conflict in Africa, as well as protect and further US interests and security.

References

United Nations Conference on Trade and Development. (2021). *Economic development in Africa report 2021* [Press release]. https://unctad.org/press-material/facts-and-figures-7

United Nations Department of Economics and Social Affairs. (2019). *World population prospects Highlights, 2019 revision Highlights, 2019 revision*. https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf

United States Central Command (USCENTCOM)

MajGen Scott F. Benedict
Director, USCENTCOM, CCJ5
scott.f.benedict.mil@mail.mil

Ms. Christina Peters
Communication Strategy, CCJ5
christina.l.peters20.civ@mail.mil

The USCENTCOM Commander stated in the March 2022 posture testimony:

> *…with the recent withdrawal of U.S. forces from Afghanistan and conclusion of U.S. combat operations and transition to an advise, assist, enable mission in Iraq, many Americans may assume that CENTCOM's very reasons for being have drawn to a close. That could not be further from the truth.*

USCENTCOM's area of responsibility (AOR) remains one of the most dynamic places on earth and constitutes geostrategic *key terrain* that makes it a decisive theater for competition with major US strategic competitors. Therefore, when it comes to US national strategy, USCENTCOM advocates we should not constrain warfighting by domain or geography. National strategies should have *global* focus to address *globally capable* competitors, like China and Russia, anywhere they seek to undermine US national interests. A strategy that does not account for the importance of the Middle East is missing a key component required to successfully compete globally.

USCENTCOM's AOR includes land and maritime borders with USINDOPACOM, USEUCOM, and USAFRICOM, making it an essential region to not only US national interests and security, but also to our allies. It contains three strategic maritime transit points for energy and trade that guard the flow of the global economy. One-third of the world's oil production transits the Strait of Hormuz daily, meaning health of the global economy rises and falls with the region's stability. Besides being a crossroads for global commerce, the region is also a global epicenter for violent extremism. Some of the most immediate and credible threats to the US homeland continue to emanate from the USCENTCOM AOR, reinforcing the necessity to degrade terrorist threats from violent extremist organizations.

To focus on priority challenges, the 2022 National Defense and National Military Strategies seek to limit deployment of US assets to the USCENTCOM region. While USCENTCOM concurs with the direction of the national strategies and priorities, there are two main areas of concern.

1) Focus on the two priority challenges (i.e., China and Russia) does not account for their global reach

A key tenet of integrated deterrence is that it is not constrained by geography. Both the National Defense and National Military Strategies are sub-regionally vice globally focused, and do not consider that *global competition* means *global*—which includes other geographic regions beyond USINDOPACOM and USEUCOM. China and Russia continue to aggressively pursue their national interests in the Middle East and Central and South Asia. However, due to the impulse to compensate for a perceived overinvestment in the USCENTCOM region over the past 21 years, critical capabilities are being redeployed from the USCENTCOM AOR at a rate that is causing concern among our closest partners and allies. This creates opportunities for China and Russia to expand their influence.

The bisection of the Eurasian landmass by the central region provides key terrain and a dominant position for the US to strategically compete with China and Russia through a range of security cooperation ventures including border security, counter narcotics, counter weapons of mass destruction, counter terrorism, and defense institution building—activities that allow us to maintain status as *"partner of choice"* in the region. However, posture reductions are severely diminishing our ability to conduct these critical activities, providing expansionist China and a resurgent Russia the opportunity to shift alliances and gain influence, access, and key resources to support their national objectives.

While USCENTCOM's force posture draws down, China continues to expand its presence through its Belt and Road Initiative, debt trap infrastructure investments, military basing, and proliferation of 5G technology that provides opportunities for political coercion and military exploitation of US partners and allies. Similarly, Russia continues to reinforce its enduring military and economic presence in Syria, expand its economic and defense relationship with regional countries, and increase influence over regional energy resource and transit routes. Ultimately, China and Russia are positioning themselves to expand their influence to replace the current international order with a multipolar order that is more amenable to Chinese and Russian national interests.

2) The idea that assurance should not be gained through posture

This premise conflates posture with forces: posture is a combination of forces, footprint, and agreements. USCENTCOM's longstanding relationships are supported by years of physical presence. As we reduce force levels, we must find ways to preserve the other elements of posture. We must also consider that how we establish our limited enduring presence is being analyzed by both our regional and global partners. Nations are making long-term decisions about our reliability based on the actions we take today. Reductions have already eroded our relationship with key regional partners and allies who are foundational to our collective ability to address challenges presented by strategic competitors in the region. As we continue to reduce our forces, we must set conditions to mitigate the impact, or we risk undermining the

confidence of our partners and allies. This could compromise our ability to leverage longstanding relationships and wield influence, which will further push our partners and allies toward our adversaries.

Maintaining our influence and safeguarding US interests requires a whole-of-government approach, and that we establish the conditions (i.e., footprint) to rapidly receive dynamic force opportunities. We must also acknowledge that we cannot contend with complex and interconnected challenges alone. Mutually beneficial partnerships and alliance architectures are our greatest strategic advantage; they are the center of gravity in our national strategies. Therefore, we must establish agreements with both regional and international partners to increase confidence and set expectations. This increased emphasis on partnerships and assurance should begin with security cooperation initiatives to include foreign military sales (FMS), defense-wide partner nation support, and multilateral constructs.

Countries in the USCENTCOM AOR use FMS to purchase a security relationship with the US. However, since US FMS processes are lengthy and bureaucratic, our position with key regional partners and allies is deteriorating to the point where they are turning to our adversaries to meet their security requirements. USCENTCOM is hindered in its ability to achieve effective and economical collective security by delays in FMS to partners and allies, which—combined with reductions in US capabilities across the region—contributes to the perception of wavering US commitment to security and stability in the USCENTCOM AOR. This false narrative provides an opportunity for strategic competitors to exploit. Countering this narrative requires credible assurance and reliable demonstrations of US commitment to our regional security partners. It also calls for us to recognize the importance of our security assistance enterprise and our defense industry's ability to support our partners' defensive needs in a timely manner.

We cannot afford to re-posture US defensive capability while simultaneously failing to deliver the weapons our partner and allies need to defend themselves. Not only do we need to leverage FMS to counter the perception that the US is abandoning the region, but we cannot expect to advance our regional security objectives and achieve integrated deterrence—which depends heavily on our network of partnerships and alliances—without ensuring our partners and allies are equipped with the tools and training they need to be successful. If we do not prioritize FMS, we will not only lose interoperability with our partners, but we foresee our partners limiting access, basing, and overflight that we have relied on for decades. Additionally, if we do not ensure effective and timely delivery of needed weapons to our security partners, we will have to rely on rhetoric alone to achieve US vital national interests in the region. This will inevitably lead to the US ceding its position as partner of choice.

USCENTCOM also advocates for continued resourcing of various defense-wide partner nation support programs. A prime example is the Border Security Program, which will provide up to $370 million of support to Jordan, Lebanon, Egypt, Tunisia, and Oman in fiscal year 2022. Enhanced border security will help constrain the movement of foreign terrorist fighters and disrupt supply and equipment shipments to various extremist organizations. These programs

provide invaluable assurance to our key partners in the region, and support security and stabilization efforts in this highly volatile region. There are other programs and authorities, like Defense Support for Stabilization, that hold enormous potential for the USCENTCOM region, but lack dedicated appropriated funds. With the end of the supplemental Overseas Contingency Operations funding in fiscal year 2022, it is vital that these programs receive dedicated funding so they do not compete with other baseline priorities.

In addition to improving our FMS processes and maintaining support to defense-wide nation support programs, we must also place increased emphasis on improving partners' collective defensive capabilities by building and maintaining multilateral constructs that they can sustain for years to come. Currently, individual nations' defense is largely based on their bilateral relationship with the US. However, it is folly to think that through our bilateral relationships, nations will be able to increase their capability to a level where they can sufficiently respond to regional contingencies and reduce our competitors' ability to hold key geographic and logistical lines of communication at risk. This is particularly true when it comes to the persistent and evolving challenge of uncrewed aerial systems (UAS).

State and non-state actors are rapidly growing their UAS capabilities, which presents a direct threat to the US and our regional partners and allies. Our adversaries seize the opportunity to acquire and weaponize relatively cheap commercial and military grade UAVs, then use them to attack military and civilian infrastructure and probe our capabilities and air defenses in the region—providing them the operational ability to surveil and target US and partner facilities. The growing threat posed by these systems, coupled with our lack of dependable, networked capability to counter them is the most concerning tactical development since the rise of the improvised explosive device in Iraq. The strategic answer to effectively counter UAS threats is to combine our efforts, with regional partners and allies, through regional constructs.

USCENTCOM will compensate for capability reductions through regional constructs; we will shift bilateral relationships to multilateral frameworks. Many of our key regional partners and allies have already joined our multilateral initiatives because they understand that controlling the air domain and securing the maritime commons is essential to our collective success in future operations. Lack of coordination presents seams that can be exploited along our borders, airspace, and in international waterways. However, by increasing our security cooperation and interoperability, we can deny our adversaries that opportunity.

Finally, winning strategies do not over-exert, reallocate, or redesign force posture below the threshold of preparedness. Maintaining a *sufficient and sustainable* presence in the central region is critical to preserving security relationships that will further our national interests. Failing to do so will cause further erosion to relationships with key partners and allies. In addition to losing the trust and confidence of our partners and allies, further reductions to our force posture could dramatically degrade or even completely cede US access and influence in the region, creating a void for globally capable competitors to exploit.

USCENTCOM must be able to campaign and conduct combined operations and exercises forward, creatively employ multilateral constructs, retain appropriate manning and funding, and remain operationally ready to meet an uncertain and unstable future. This will enable us to sustain placement and access to deter aggression, while providing the capability to disrupt VEOs and compete with global competitors. It will also allow us to influence and help secure three of the world's most vital transit choke points to ensure free flow of navigation, resources, and commerce. Ultimately, we must continue demonstrating the values, commitment, and capability that makes us the *partner of choice* in not only the region, but throughout the world.

References

Posture statement, 117 Cong. (2022). (Testimony of General Kenneth F. McKenzie, Jr. Commander, United States Central Command). https://docs.house.gov/meetings/AS/AS00/20220317/114523/HHRG-117-AS00-Wstate-McKenzieK-20220317

United States Cyber Command (USCYBERCOM)

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

Background

US Cyber Command (USCYBERCOM) directs, synchronizes, and coordinates cyberspace planning and operations to defend and advance national interests. The Command plans, de-conflicts, executes, and assesses cyberspace operations in coordination with, or in support of, other Combatant Commands (CCMD), allies and partners, and as directed, other entities across the full spectrum of competition to conflict. USCYBERCOM's three lines of operation are to

- direct the security, operation and defense of the Department of Defense Information Network (DODIN), including the Department of Defense's (DoD) critical infrastructure to enable DoD mission assurance;
- deter, defend, and defeat cyberspace attacks against the United States and its national interests; and
- assist Combatant Commanders (CCDR) to achieve their campaigning and warfighting objectives in and through cyberspace.

USCYBERCOM directs operations through subordinate headquarters. These include the Cyber National Mission Force-Headquarters (CNMF-HQ), Joint Force Headquarters-DoD Information Network (JFHQ-DODIN, the commander for which is dual-hatted as the Director of the Defense Information Systems Agency) and Joint Task Force Ares. They work with our Joint Force Headquarters elements, the commanders for which are dual-hatted with one of the Services' cyber components (Army Cyber Command, Marine Corps Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/16th Air Force, and Coast Guard Cyber Command). The Command's assigned forces currently comprises 133 teams across the Cyber Mission Force (CMF) with approximately 6,000 Service members, including National Guard and Reserve personnel on active duty—the majority of the forces that secure and defend the DODIN. The CMF is due to grow by 14 teams over the next five years.

In addition to the authorities all CCMDs have, USCYBERCOM also exercises Service-like authorities previously unique to US Special Operations Command (USSOCOM) under 10 USC §167b. Examples of these authorities include developing strategy, doctrine, and tactics; monitoring promotion of cyberspace operations forces (COF) and coordinating with the military departments on the assignment, retention, training, professional military education (PME), and special and incentive pay; Joint Force Provider (JFP) and Joint Force Trainer (JFT) for the COF, and preparing and submitting program recommendations and budget proposals for manning, training, and equipping the COF. Recently delegated budget oversight requires USCYBERCOM to submit its first Program Objective Memorandum (POM) in FY24 for the CMF

and Joint Cyberspace Warfighting Architecture (JCWA). Collectively, these authorities enhance the Command's ability to organize, train, equip, and employ COF to meet mission requirements.

Strategic Context

The security of the United States and our allies depends on international stability and global prosperity. Military superiority in the air, land, maritime, cyber, and space domains is critical to our ability to defend our interests and protect our values. The spread of information technology and communications enables new ways for adversaries to undermine US power by operating routinely in and through cyberspace. The locus of global competition shifted to cyberspace, where adversaries and competitors produce outcomes negatively affecting the US society, economy, government, and critical infrastructure, all while remaining below the traditional threshold of armed conflict.

Decades of misreading the cyber strategic environment placed the United States in a reactive posture and resulted in a policy of restraint and inaction. The open access internet model, in place for decades, has conferred enormous benefits for the global community as well as huge costs. Cyberspace has become a haven and playground for criminals who prey on victims around the world, imposing security costs on everyone who connects online. That situation might in time be mitigated, but at present this background noise of criminality distracts users and governments from more insidious and dangerous state actors seeking to erode the relative power of democratic states.

State and non-state actors now see cyberspace as a space for political maneuver, information campaigns, intellectual property theft, ransomware attacks, supply chain manipulation, and on occasion, destruction. Some governments support cyber criminals who advance state interests on their behalf. Today the United States risks preparing for a war that might never come while neglecting strategic gain being made by competitors and adversaries in the cyber domain. While deterrence, and even containment, is a viable approach against a strategic challenger (as during the Cold War), relying on these approaches is insufficient to protect vital US national interests when cumulative gains in day-to-day competition can shift the global distribution of power without war or the threat of war. 2018 was a watershed year for the nation when it was recognized that adversary military forces were threating our democratic institutions, and law enforcement or diplomatic responses solely were inadequate. This resulted in new laws, strategies, and policies that improved the DoD's ability to respond.

In summary, changes to the cyberspace strategic environment have trended negatively: malicious cyberspace activity swelled, malware proliferated, campaigns below the level of armed conflict expanded, and state and non-state adversaries now routinely use cyberspace to advance their economic, political, and strategic objectives.

Challenges

Russia's invasion of Ukraine demonstrated their determination to violate Ukraine's sovereignty and territorial integrity, forcibly impose its will on its neighbors and challenge NATO. Russia's military forces are employing a range of cyber capabilities to include espionage, offensive cyberspace operations, and operations in the information environment to support its invasion and to defend Russian actions.

China is the DoD's pacing challenge, and consists of both a sprint and a marathon in the cyber domain. China's military modernization and buildup over the past several years threatens to erode deterrence in the western Pacific and requires immediate steps to address. Simultaneously, China is a long term, enduring strategic challenge that is now global in scope. It is exerting influence worldwide and threatening the established world order through its rising economic, military, diplomatic, and informational power.

Iran and North Korea are cyber adversaries growing in both sophistication and willingness to act. Iran is increasing ransomware operations, targeting critical infrastructure, and information campaigns. North Korea uses malicious cyberspace activity to generate revenue through criminal enterprises such as criminal hacking for hire and theft of cryptocurrency.

The scope, scale, and sophistication of adversary threats in cyberspace continues to grow. The United States faced major cybersecurity challenges in recent years consisting of cyberspace attacks, criminal activity, and espionage directed against US citizens and private businesses, the US Government and associated democratic processes, critical defense and commercial infrastructure, and intellectual property.

Opportunities

USCYBERCOM's principal method for implementing the 2022 National Defense Strategy (NDS) is contributing to integrated deterrence by campaigning and building enduring advantages.

Integrated Deterrence. At its core, deterrence dissuades adversaries and competitors from committing aggression and other acts that are harmful to US interests by changing their perception of costs and benefits. Integrated deterrence, described in detail in the NDS, entails the Joint Force working seamlessly across military domains, theaters, the spectrum of conflict, other instruments of national power, and alliances and partnerships. It combines existing and novel concepts, capabilities, and emerging technology in new ways to shape both the information environment and adversary decision calculus about the benefits and costs of action or inaction. Cyberspace operations themselves do not replace nuclear or kinetic options, but they do fill an important and expanding role particularly during competition.

Campaigning. While securing, operating, and defending the DODIN, USCYBERCOM enhances deterrence and gains military advantage through campaigns by conducting and sequencing logically linked military activities, day after day, to achieve defense objectives over time. First described in the 2018 NDS as great power competition, campaigning involves iterative actions

undertaken by the operational approach of persistent engagement. Engaging competitors and adversaries below the level of armed conflict yields intelligence and accesses to support achieving Joint Force commander objectives. Through persistent engagement, USCYBERCOM forces observe, react and train, and create friction and uncertainty while reducing the risk of strategic surprise.

Building Enduring Advantages. Many nations rely on cyberspace to perform the day-to-day functions associated with the governance and operation of a modern society. The DoD's reliance on cyber, which underpins many critical Joint Force functions, requires proactive action to build and maintain advantages in the cyber domain. The Department is adopting a zero trust architecture, which is a security model based on continuous monitoring, assessment, and verification of user access to data. This approach, when coupled with modernized encryption and cryptography, will allow the DoD to operate the DODIN and trust information even when competitors and adversaries penetrate DoD networks. Increasing readiness of the CMF, creating new and reinforcing existing partnerships, and improving recruitment, training and retention are also key objectives to building enduring advantages.

Summary

USCYBERCOM views 2022 and beyond as a significant period for mitigating challenges posed by competitors and adversaries and for fulfilling opportunities for the Joint Force. The Command's overarching goal is to posture its forces and capabilities to provide senior national leaders diverse, non-kinetic options throughout the entire spectrum of competition and conflict while simultaneously securing, operating and defending the DODIN. The point of contact for this paper is Mr. Michael Clark, US Cyber Command Director of Cyber Acquisition and Technology, email michael.a.clark67.civ@mail.mil, or phone number 443-654-2573.

United States European Command (USEUCOM)

Emerging Strategic and Geopolitical Challenges: Operational Implications for USEUCOM

USEUCOM Staff
POC: Mr. Jimmy Krakar
Academic Coordinator, USEUCOM
james.n.krakar.civ@mail.mil

All geographic combatant commands are unique, and the 50 countries and territories that constitute the US European Command (USEUCOM) area of responsibility (AOR) include some of the key allies and partners that have ensured the post-World War Two security order for over the last 80 years. The Interim National Security Strategic Guidance (INSSG) articulates how a free and prosperous Europe remains foundational to US national security in a competitive geopolitical environment. Europe boasts of some of the world's most advanced nations politically and economically. While US defense is critical for the region, the region as a whole is an exporter of global peace and security. The advanced nature of the USEUCOM AOR lends itself to a whole of government approach that works with our allies and partners across a spectrum of challenges both bilaterally as well as through some of the most developed alliances and international organizations in the world.

This advanced level of democratic political organization, sufficient economic resources, and forward thinking governance posture the majority of the countries in the USEUCOM AOR to have a relatively high degree of resilience for individual apex challenges. The issue is when these apex challenges are leveraged and exploited by various state and non-state actors to further their own agenda, which often involves destabilizing and marginalizing the importance of alliances such as the North Atlantic Treaty Organization (NATO) and the European Union (EU).

The INSSG lays out Russia as a destabilizing challenge. Russia's nuclear arsenal and strike capability remain an enduring existential threat to the United States. Russia pursues malign activities including military aggression aimed at undermining democracy and the rules based international order, and has a willingness to use force to achieve its aims. Russia employs gray area activities to maintain its purported sphere of influence while attempting to coerce neighboring sovereign nations and to form fractures between allies at NATO. They use tactics ranging from disinformation campaigns to malicious cyber activities to the manipulation of energy markets to support Moscow's effort at political subversion and economic intimidation. These tools and others are intended to coerce, weaken and divide our allies and partners in the European theater and beyond. In the Baltics, the Russian government actively targets ethnic Russian population with extensive propaganda and malign influence operations, while conducting cyber operations to weaken alliance resolve.

The second major challenge laid out by the INSSG is an "increasingly assertive China." The Peoples Republic of China (PRC) seeks to increase its access, presence, and influence in Europe and globally. They engage in aggressive and subversive economic and diplomatic activities in the USEUCOM AOR not only to build markets to strengthen the Chinese economy but also to establish presence at key transportation nodes and increase their political influence. China's foreign direct investment, government backed business ventures, and infrastructure deals not only secure the PRC's advantage in global trade, market access, and technological standards, but also provide Beijing with an avenue to assert influence at the expense of enduring US, allied, and partner interests.

The PRC focuses on seizing the "high ground" in critical and emerging technology sectors with military application, including artificial intelligence, advanced robotics, quantum technologies, and hypersonic systems, and at the same time it seeks to export its national technology standards globally. The PRC's efforts to expand 5G networks throughout Europe via state-backed firms, such as Huawei and ZTE, pose significant security risks to the interests and military forces of the US, allies, and partners. These networks place intellectual property, sensitive information, technology, and private personal information at heightened risk of acquisition and exploitation by the Chinese government. The PRC continues to invest significantly in European ports and transportation nodes, as well as other critical infrastructure in Europe.

In the Western Balkans, Russia—and now the PRC—use malign influence to roil existing ethnic tensions and seek to foster instability. Russia uses social and political pressures to impede these countries' Euro-Atlantic alignment and integration. The PRC's emergence as an alternative patron for economic and defense cooperation, under suspect terms, further disrupts the region.

Two additional challenges that influence the USEUCOM AOR are violent extremist organizations (VEOs) and climate change. Successful VEO-inspired and -organized attacks in Europe complicate integration efforts, potentially isolating refugee and migrant communities and increasing the possibility of VEO recruitment. These attacks can then reinforce isolationist trends and distrust of international engagement.

Climate change will exacerbate risks to security as the physical impacts increase and geopolitical tension mount on how to respond. Increasing physical effects such as droughts, ice melts, sea level rise, and extreme weather events will strain national governance, budgets, and stability in Europe. For populations most vulnerable to climate change, migration can serve as a form of adaptation, further challenging international stability and governance as migration increases from vulnerable areas.

Climate change will also effect the High North. As the Arctic ice sheet shrinks it opens additional navigation routes as well as access to previously unreachable mineral resources. As part of the global ocean, the Atlantic and Arctic Oceans must remain open and free to facilitate commerce between Europe, North America, and other international markets. Again the key is

operating within existing multilateral organizations. Of the eight member states of the Arctic Council five are members of NATO, while two additional are NATO Partners for Peace. The existing rules-based international order benefits all Arctic nations by facilitating sustainable economic development, fostering cooperation, and promoting a stable, conflict free region.

It is key to remember that as is often said in NATO, the strength of the alliance is the alliance. The NATO alliance, and the European Union are both predicated on their members adhering to the principles of liberal democracy, rule of law, and participation in the post-World War Two liberal world order. The most concerning challenges are those that wear away and erode these organizations that, while seemingly reinforcing individual sovereignty, allow the cornerstones of European multilateralism to atrophy into ineffectiveness.

In Europe, malign activity and direct military aggression, energy competition, and forced migration stress the rules-based international order and strain the resources of the state. Strategic competitors use all instruments of national power to exploit these conditions to gain advantage and create instability. This nexus challenges governments and institutions like NATO and the European Union to develop coordinated and complementary policies to counter malign activity. As the INSSG states, "Recent events show all too clearly that many of the biggest threats we face respect no borders or walls and must be met with collective action."

Europe and the United States remain the foundation for upholding a free and open international order. USEUCOM's unique geographic location enables global operations for access basing and overflight permission with Europe. We work within a whole of government framework to maintain essential access and permissions under bilateral agreements and to resist Russian and Chinese strategic investments. Absent these agreements, the United States could not meet treaty obligations or effectively protect vital national interests. The shared ideals, values, trust, and longstanding relationships we have in Europe enable the United States to generate coalitions for worldwide operations in support of shared national interests.

Maintaining a capable US presence in Europe strengthens our national security by generating peace, unity, and cohesion among Europe's sovereign nations. Russia and China present formidable, enduring challenges to preserving a free and peaceful Europe. Nevertheless, the West is more united that it has been in years. NATO is stronger, not weaker, and we are ready to respond decisively. Our strategy addresses the dynamic security environment by ensuring we effectively compete for long-term sustainable advantage, deter attacks from potential aggressors, and prepare our allies and partners to respond decisively.

USEUCOM's primary mission is to compete, deter, and prepare to respond to aggression with the full weight of the NATO alliance. It is only by focusing on maintaining the NATO alliance, along with other key international bodies, and pursuing effective bilateral engagement that the United States can be successful at setting conditions where we can leverage the resources inherent in the USEUCOM AOR to mitigate the apex challenges that the future will undoubtedly bring.

United States Indo-Pacific Command (USINDOPACOM)

USINDOPACOM Strategic Planning & Policy Directorate
PACOM.J56.All@pacom.mil

The Region

As articulated in the *Indo-Pacific Strategy of the United States*, released by the White House in February 2022, the Indo-Pacific region is vital to the national security of the United States. It is home to more than half of the world's population, responsible for nearly two-thirds of global economic output, and host to more members of the Joint Force than any other region aside from the United States itself. It is a region filled with promise: 58% of the world's youth population resides in the Indo-Pacific. It is also one projected to become more critical to global growth and prosperity over time: The region is projected to account for two-thirds of global economic growth in the years ahead.

However, the Indo-Pacific is also home to a broad array of potential threats: It hosts six of the world's nine declared nuclear powers, seven of the ten largest militaries on the planet, and four of the five primary threats identified in the Department of Defense's *2022 National Defense Strategy Fact Sheet*: the People's Republic of China (PRC), Russia, the Democratic People's Republic of Korean (DPRK), and violent extremist organizations (VEOs).

The PRC

The Department of Defense has identified the PRC as its "most consequential strategic competitor" and its "pacing challenge" with respect to planning, programming, budgeting, capabilities development, and force modernization. DoD's assessment that the PRC is pursuing a broad-based effort using all elements of national power to challenge the rules-based international order and reshape global governance to better suit its authoritarian preferences resulted in this designation.

The competitor designation given to the PRC is further driven by the evolution of the People's Liberation Army (PLA), which has undertaken an accelerated and comprehensive military modernization program intended to position itself as the region's dominant military by 2027. The PRC has pursued a decades-long program of reform and modernization intended to develop the power projection capabilities necessary to compel unification with Taiwan by force, enable the PRC to project power globally, and provide the PRC with the means to threaten the US Homeland.

The PRC has also demonstrated a willingness to employ other elements of national power alongside its military to undermine state sovereignty, democratic governance, and human rights at home and throughout the Indo-Pacific. It has employed brute force to press its territorial claims against India along the border that India and the PRC share, systematically dismantled democratic governance in Hong Kong, continued to expand military infrastructure

in the South China Sea while pressing expansive and unlawful maritime claims, and engaged in broad-based economic coercion against states that question its actions with respect to Taiwan, Hong Kong, or COVID-19. At home, the PRC continues to actively suppress, detain, and torture ethnic and religious minority groups, including the predominantly Muslim Uyghur population in the PRC's far western provide of Xinjiang, practices the Department of State concluded in 2020 constitute both genocide and crimes against humanity.

Russia

Alongside the challenges presented by the PRC, Russia maintains an ability to threaten the US Homeland, as well as the interests of US allies and partners in the Indo-Pacific. Moscow has long evidenced a desire to diminish the global influence of the United States and demonstrated a willingness to employ all elements of national power to undermine free, open, and democratic societies worldwide. While Russia's unprovoked and unjustified invasion of Ukraine most directly affects Europe, the Russian military maintains significant military capabilities in the Pacific and routinely conducts high-end naval exercises and strategic air patrols in the vicinity of the sovereign territory of the United States and its allies in the Pacific, such as Japan. Against the backdrop of a recently announced PRC-Russia comprehensive "strategic partnership," an increased drive by the Russian military to increase interoperability with the PLA and a willingness by Moscow to broadly support PRC attempts to undermine free, open, and democratic societies worldwide, it has become increasingly clear that Russia's efforts to challenge US leadership and threaten US security interests transcends Europe.

The DPRK

The Pacific is also home to the Democratic People's Republic of Korea (DPRK), which continues to threaten the United States, the Republic of Korea, Japan, and others through reinvigorated efforts to develop a nuclear weapons program and suite of conventional and ballistic missiles. The DPRK has conducted over 60 such launches since 2019, including seven in January 2022 alone. These efforts are expected to continue, as the Kim regime views them as essential to ensuring its own survival, extracting badly needed economic and humanitarian assistance from the international community, and posing a credible threat to the United States—a goal the DPRK's leadership has stated in public. The DPRK continues to undermine international law as it routinely violates U.N. Security Council Resolutions (UNSCR) by means of illegal ship-to-ship petroleum imports.

VEO

As DOD turns its focus to strategic competition with nation states, USINDOPACOM remains mindful that the threat presented by VEOs remains ever- present.

Climate Change

The Command also appreciates the threat presented by climate change, which is acute in the Indo-Pacific: A majority of the population in the USINDOPACOM area of responsibility lives in coastal regions that are particularly vulnerable to sea level rise and extreme weather events.

Climate change is expected to place agricultural productivity and access to fresh water at risk, dynamics that will exacerbate instability throughout the Indo-Pacific, particularly as nations struggle to escape the current period of pandemic-induced economic hardship.

USINDOPACOM's Approach

In light of these challenges, the Secretary of Defense tasked the Department to "defend the homeland, deter our adversaries, and strengthen our allies and partners." USINDOPACOM works toward these goals in the Indo-Pacific through a broad array of posture initiatives, operations, exercises, security cooperation activities, and key leader engagements that are aligned toward common goals, sequenced in execution, synchronized with the other elements of US national power, and executed across warfighting domains in close coordination with US allies and partners. Collectively, these efforts are intended to prevent conflict by deterring US adversaries and, should deterrence fail, ensure that the Joint Force is prepared to fight and win.

Posture

Today's arrangement of forces, footprints, and agreements in the USINDOPACOM area of responsibility reflects the geopolitical reality that existed at the end of World War II and the strategic and operational imperatives that drove DoD planning throughout the Cold War. It is weighted heavily toward northeast Asia, concentrated in a handful of locations, and predicated upon the assumption—true for much of the past few decades—that the Joint Force would operate in environments where forces, command and control, and logistics would flow uncontested into the Indo-Pacific theater in time of need. That assumption is being challenged.

The Joint Force now finds itself faced with the potential for a high-end warfight against a near-peer adversary in a contested environment. Subsequently, any force flow, communications, and logistics will be heavily contested. Potential adversaries have developed the ability to strike with ever greater speed and capability, as well as at increasing distances. USINDOPACOM is therefore intently focused on modernizing Joint Force posture in the Indo-Pacific to support a combat-credible, all-domain force that is distributed, resilient, and forward deployed west of the International Date Line.

Such a posture enables a forward, persistent pattern of operations inside the First Island Chain and enhances the Joint Force's ability to exercise and operate with allies and partners in peace time. This posture will help the DoD re-establish a general baseline of deterrence, forestall conflict, and ultimately provide the Department with better options to fight and win in a crisis scenario.

Operations

Persistent and synchronized coalition and joint operations linked over time and space across the western Indo-Pacific contribute to the Joint Force's ability to deter conflict.

USINDOPACOM conducts such operations to bolster interoperability, reassure allies and partners, build partner capacity, and normalize Joint Force operations throughout the Indo-Pacific. A consistent, persistent presence also demonstrates the enduring nature of US commitment and provides recurring opportunities for the Joint Force to remain familiar with the Pacific operating environment.

Exercises

USINDOPACOM's program of complex, multi-domain exercises demonstrates US commitment to the security of our allies and partners. These exercises build interoperability and, together with a robust program of experimentation, help the Joint Force develop the concepts and capabilities needed in a high-end warfight.

Security Cooperation

While USINDOPACOM's exercise program aims to enhance the ability of the Joint Force to operate together with allies and partners, security cooperation provides our counterparts with the tools required to do so. Security cooperation also better enables allies and partners to protect and defend their interests across the warfighting domains: DoD security cooperation activities in the Indo-Pacific are helping improve maritime domain awareness, increase cyber readiness, facilitate the exchange of intelligence, and increase the warfighting capabilities of armies, navies, and air forces throughout the Indo-Pacific.

Key Leader Engagements

Key leader engagements accentuate USINDOPACOM's other efforts. The Joint Force cannot deter our adversaries without allies and partners prepared to work alongside us. Critical to building this unity of purpose and effort are the discussions between our senior leaders that socialize security concerns, build consensus, develop concepts and capabilities, and refine war plans.

Conclusion

The diverse array of challenges that exists in the Indo-Pacific requires a comprehensive, agile, and resilient solution. USINDOPACOM recognizes that the traditional way of operating practiced for more than 70 years is no longer sufficient to meet the great power, non-state, and natural disaster threats that imperil regional stability and US national objectives. The Commander of USINDOPACOM has challenged his team to "Think, Act, and Operate" differently in order to address the threats that face the United States, as well as our regional allies and partners. This change has manifested in our pursuit to enable, facilitate, and deliver Integrated Deterrence in accordance with Secretary Austin's vision of a whole-of-government solution to today's security challenges. USINDOPACOM is grounded in the reality of the mission to deter aggression, counter gray zone activity, and, if deterrence fails, be prepared to win in conflict. The five ways of campaigning outlined above describe how the Command's time, money, and resources will be prioritized over the next five years to achieve the objectives laid out in the National Defense Strategy.

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

Mr. William J. A. "Joe" Miller
Director, NORAD & USNORTHCOM J7
william.j.miller116.civ@mail.mil

It is counterintuitive to assert a NORAD and USNORTHCOM position that the best way to defend the homeland is to organize, resource, and compete (and, if necessary, fight) forward—indeed, globally. Yet, that is exactly the stance taken in this chapter. To support the argument, consider a (simplified) historical perspective.

The structure of the Department of Defense that organizes forces by Service and then again by functional and geographic combatant command has developed, applied, and refined the Joint Force concept to execute its mission set over the several decades since Goldwater-Nichols in 1986. From its inception, this approach has been rooted in the assumption that the United States could contain most conflicts and reach decision by campaigning and fighting forward, containing action within a given area of responsibility (AOR) or theater of conflict. In that period, however, our competitors around the world have recognized our nuclear and conventional force strength and subsequently learned to avoid direct combat and instead work to advance their operational and strategic interests, globally, through actions calculated to remain below the threshold of armed conflict with the United States. Those actions have included both regional and global initiatives and have spanned the spectrum of competition, from cooperation with the United States where interests are aligned to armed intervention in third party conflicts with impacts counter to US interests.

Regional actions notwithstanding, our competitors have generated effects with global implications, compounded by the pace of technological change and the emergence of the apex challenges identified in the two previous SMA Perspectives volumes. The measure of success in competition, then, must be taken in a global context. It behooves the Department to accelerate its shift to a global—and globally integrated—approach to operations, one that will consistently build advantage independent of geography or domain and leveraged, when the opportunity presents, to advance our interests or, where necessary, to temper the adventures of our competitors.

The apex challenges are themselves deeply interdependent, often with cross-domain effects leading to potentially rapid amplification and resulting in global consequences. For example,

cryptocurrencies, though not inherently "cyber threats," certainly inhabit primarily the cyber domain and yet, because their existence belies a lack of trust and confidence in traditional monetary systems, they may in fact present as a "financial crisis" to a "fragile state," where the disruption escapes localized containment efforts and suddenly has repercussions in the global market. Or a virulent disease spreads rapidly via the globally networked transportation system, in spite of coordinated societal efforts to prevent it, and disproportionately destabilizes those nation-states less capable of weathering a sustained outbreak.

But none of the apex challenges originate in the homeland! Whether the effect in the homeland is environmental, cyber-specific, or financial, the source is elsewhere. Even in the case of violent extremism, the inspiration is external. And for the narrower case of "homegrown" violent extremism, the appropriate response is under the jurisdiction of law enforcement.

Each apex problem defines its own operating space and seldom matches our organizing constructs. Apex challenges, by their very nature, simply do not respect our artificially constructed boundaries, whether geographic or domain, and thus must be considered global if we are to build and leverage advantage for competitive gain. The Department of Defense, no less so than the whole of government and the private sector, must take on the challenges from that perspective. It is not enough to synchronize initiatives among the Combatant Commands' respective AORs; the effort must be globally integrated from the outset, in design, intent, and distribution of resources, to achieve the strategic effects that will manifest in regional and local decisions and actions aligned to our interests and those of our allies and partners.

Without boundaries that limit their effects in both space and time, addressing the apex challenges cannot rely on an AOR-centric approach, nor even a confederation of AOR-based strategies. Every Combatant Commander in his or her assigned AOR or functional area, every sensor and weapon system operator in every domain, and the full complement of our partners and allies must recognize the global environment, acknowledge that the competitive arena is global, and commit a priori to a globally integrated campaign. Our Commands, Services, Agencies, partners, and allies must synchronize and bring to bear our respective capabilities in a comprehensive, layered defense, one that integrates all forms of power, persuasion, and deterrence into a coherent whole. To do so means to align organizational structure, personnel, and funding to the global campaign, sustained across administrations and even across generations, in service and defense of our shared and enduring common interests.

What then, are those enduring interests, generalized enough to span the vicissitudes of operational thrust, parry, and feint in competition, crisis, and conflict, and yet specific enough to provide clarity of purpose and mission for individuals and organizations dedicated to those interests as each inherits the mantle of responsibility from one generation to the next? What do we have? What do we value?

The rules-based order (RBO) is one such value, having delivered relative peace and security for some seven-plus decades compared to the previous centuries and millennia. The RBO offers an opportunity for stability among nation-states around the world, reducing the incentive for manmade threats to the environment, sovereignty, cyber communications, and financial systems. It is strengthened through active, adherent participation by the greatest number of nation-states, and thus it is in our national interest—and that of our allies and partners—to advocate for and facilitate increased participation, as well as to encourage self-compliance on the part of each participating nation. The RBO is a catalyst in promoting prosperity, which in turn supports unilateral and collective resiliency to endure occasional cycles of economic decline or short periods of political instability. The Department of Defense has a vested interest in preserving the RBO in competition and restoring it in de-escalation from crisis or conflict; the force should be aligned and resourced to support this goal.

Conversely, it is also in our interest, and within the Department's mission set, to discourage and dissuade nations whose behavior violates or, indeed, never subscribes to the tenets of the rules-based order. Once established among a critical mass of participating nations, the RBO confers the advantage of greater alignment of participants' national interests, reducing competition between participants and incentivizing the cooperative application of, say, economic leverage to influence nonparticipating nations. This concept has played out in the West's near-unanimous application of sanctions to Russia in response to its incursion in Ukraine, where the primary influence is intended for Russian leadership and a secondary influential effect is seen in China's hesitation to support the Russian military operation. To date, the Department of Defense has supported this effort through application of its own resources and capabilities, determinedly below the level of direct armed conflict with Russia. And while much of the materiel has been supplied in the region surrounding Ukraine, the integrated, coordinated effort is from a globally based perspective.

Regional crises and conflicts, though, tend to invite regionally focused containment strategies, a habit that risks myopia and fails to adequately posture for the global nature of the apex challenges. The interconnectivity of the world means that localized events, especially apex-related ones, have the potential to spin into ones with global consequence and, in particular, affect the homeland. Incrementally and episodically addressing various manifestations of any and all of the identified apex challenges, it ultimately becomes apparent this is not a problem set with a defined solution, and indeed likely defies complete eradication. To establish a lasting commitment across military command tours, political administrations, and societal generations, the US whole-of-community and the Department of Defense need an iconic "moonshot"—the singular application of will, focus, and technology that relentlessly moves toward removing threats and eliminating vulnerabilities—that "solves" the essentially unsolvable suite of challenges, apex or otherwise, by building a series of consistent successes in a dynamic environment of perpetual change.

Achieving and sustaining globally integrated operations and their supporting defense architecture must be embarked upon and pursued with the purpose and zeal of a national

strategy as compelling as the Apollo Program, necessarily enduring in concept, structure, and resource. This strategy should be informed by new regional threats and domain-centered challenges, to be sure, but always from the perspective that the unified, global application of leveraged advantage will yield the most efficient and consistently influential effects. This means unwavering national and collective *will*, singular mission *focus*, and leading-edge, mutually reinforcing *technologies*. Our first step in that direction, though still short of the stride we will eventually achieve, will signal our commitment to the task at hand.

NORAD and USNORTHCOM, committed to Homeland Defense, join the effort.

United States Special Operations Command (USSOCOM)

Special Operations at a Crossroads: Thinking Strategically at United States Special Operations Command

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

It is not enough to provide the Joint Special Operations Force (JSOF) the nation wants. In this decisive period of transition, United States Special Operations Command (USSOCOM) must also provide the Joint SOF the nation needs. This is a subtle, yet significant evolution, demanding nuanced refinements in how we understand the challenges we face and how we best contribute to the solutions our national security and the advancement of our vital interests demands.

On 11 April 2022, General Richard Clarke and Assistant Secretary of Defense Christopher Maier released the current Special Operations Forces Vision and Strategy (United States Special Operations Command, 2022). It is significant that both USSOCOM and the Office of Special Operations and Low-Intensity Conflict (SO/LIC) combined to craft and approve this document. This is reflective of the growing partnership that continues as *Joint SOF Operating Concept 2040* nears completion.[1]

The Operating Concept 2040 builds upon this vision and strategy, incorporating guidance from the latest National Defense and Military Strategies (NDS/NMS) from the Office of the Secretary of Defense and the Chairman of the Joint Staff, respectively. This operating concept also incorporates inputs from across the USSOCOM enterprise. One of the great strengths of US SOF is our broad diversity of organizations, each with their own distinct culture and set of capabilities. The challenge at USSOCOM, with the help of SO/LIC, is to integrate, optimize, and direct those capabilities for new purpose.

Command Vision

> *"Create strategic, asymmetric advantages for the Nation in integrated deterrence, crisis and conflict"*

Strategic Environment

Most perspectives on the strategic environment focus on the apparent complexity and ambiguity of a rapidly changing environment, coupled with the growing frustrations and

[1] The *Joint SOF Operating Concept 2040* is currently in flag officer review

concerns over an array of problematic actors/threats. These threats range from China on the high end as the "pacing challenge" as a rising state with both the will and growing capability to challenge the United States in her role as leader of a rules-based order, to the "acute threat" posed by Russia, to the other challenges presented by Iran and North Korea. Meanwhile, far larger and more distributed than on 9/11 despite over 20 years of aggressive pursuit, remains the continuing challenge presented by Violent Extremist Organizations (VEOs) such as Al Qaeda and the Islamic State. USSOCOM fully appreciates the challenges unique to each of these threats. Now there is need to focus more upon the roots of these problems to foster influence and enhance deterrence and resilience—and less on pursuing elusive "defeats" of problematic symptoms.

In 2015 General Joseph Votel signed a strategic appreciation subtitled *Finding Balance in A Shifting World* (Votel, 2015). The premise of the document was that threats were largely naturally occurring symptoms of larger dynamics taking place. These problems could be disrupted or deterred but were not solvable through military action alone. The authors postulated how advances in information technologies had served to shift the relative aggregate balance of power from governments to populations. They saw how governments everywhere were struggling to manage the friction associated with this shift, employing some blend of efforts to ignore, suppress, or stay in step with the rapidly evolving expectations of the populations they affect—both at home and abroad. The authors recognized that similar shifts in relative power were occurring between states. They predicted that friction would continue to grow between rising powers seeking privilege equal to their elevated positions, while declining states would seek to maintain what they held. The same forces shaping this contest between revisionist and status quo powers were also serving to erode the efficacy of long-held positions and approaches.

The shifts driving quests for change were also rendering many traditional control-based approaches to policy and security obsolete. It is worth noting that very similar dynamics occurred at the height of the Industrial Age, resulting in nearly a century of unprecedented warfare and insurgency (also the end of colonial empires and a vast expansion of democracy). The advent of nuclear weapons, and more importantly, nuclear deterrence through the credible threat of their use, has served to curb the high end of warfare. However, proxy war and insurgency persist, as do the modern variations we characterize as "Gray Zone Competition" and "Transnational Terrorism" (USSOCOM, 2015; Brown, 2022). As Joint Special Operations University (JSOU) President Dr. Ike Wilson points out, these powerful dynamics, along with other factors, combine to create the Compound Security Threats (CST) characterizing modern security challenges (Irwin & Wilson, 2021).

The rapid shifts in power that drove change and fueled conflicts a century ago are vastly accelerated in this modern information age. These forces are working to elevate the threshold of deterrence and increasing the frequency, scope and scale of illegal, and often violent, competition. These rapid changes are outpacing more than just the governance they affect. They are also outpacing doctrinal solutions and long-held understandings of the problems we

seek to resolve. While the instinct is to simply work harder and faster as old approaches fall short, the reality is that we must reassess and reframe the problems we face, and craft new solutions more appropriate for the world emerging around us.

To that end:

- the compulsion for change favors the revisionist, who is more likely to see opportunity in a situation, while a status quo actor is more apt to focus on the threat. But there are opportunities for both.
- identifying threats is helpful to prioritize resources and drive change, but to fixate on threats results in missed opportunities and potential exhaustion or war.
- lastly, that for JSOF in particular, populations are the opportunity space.

Campaigning for Influence

As early as 2008, USSOCOM postulated that the United States was embroiled in "a competition for influence." As I frequently heard Admiral Eric Olson point out, one's narrative is "80% what one does, and only 20% what one says." The current Commanding General, General Rich Clarke, is working to bring the imperative of influence forward through the fielding of the Joint MISO WebOps Center (JMWC) to address the opportunities and risks of the global information space and enhance the synergy of these efforts across agencies.

Strategic influence, however, is not only about conducting influence operations; it's also about *operating for influence*. It is worth pointing out that one phrase currently gaining traction is that of campaigning to gain an "information advantage;" this includes the critical notion of *perception advantage*. The character of one's actions is far more essential to achieving durable, desired strategic effects than the content of one's words. Designing campaigns to communicate strategic narratives through their execution is an essential aspect of strategic influence.

Historically, the pursuit of interests by great powers has demanded exercising degrees of control over the places, populations, and governments where those interests are perceived to exist. In bygone eras such approaches could be implemented at reasonable cost and any resultant friction either suppressed or deterred. But resistance is natural. Valid rationale for action and the character of one's approach can still mitigate the degree of the resistance effect created but cannot negate it entirely. For example, the US approach to Afghanistan was far more valid and less provocative than that of the Soviets a generation earlier, yet it provoked powerful resistance all the same.

The dynamics of the current strategic environment have combined to frustrate US post-9/11 Middle East policy, and now Russia is being taught the same hard lessons in Ukraine and Syria. The strategic impact of technology- and information- empowered populations is a game changer for great power competition. Integrating population-based activities into a comprehensive scheme of deterrence is an essential component to securing interests and

creating the time and space necessary for policy and governance to adjust to new realities for the application of power and the advancement of interests.

Strategic influence (Jones, 2021) is a concept fully recognizing that in the current strategic environment, the positive influence one can foster is far more valuable, less expensive, and less provocative than the *control* one can exert. How one operates to foster one's own positive influence, while at the same time posturing to leverage the provocation of adversaries, is both a challenge and an opportunity for Joint SOF campaigns.

Integrated Deterrence

Emerging strategic guidance is built around the central premise of traditional US deterrence becoming inadequate to the task (Cronk, 2021). A wide range of empowered state and non-state threats increasingly act out in the pursuit of their interests and in ways that are detrimental to the rules-based order and to the interests of the US, our allies, and partners. China is foremost on this list of actors, then Russia, Iran, and North Korea; VEOs are labelled a threat, but the threat with which the United States will take risk. Therefore, we must make our deterrence more effective. The way we do that is by ensuring our deterrence efforts are fully integrated in every way; across all of the elements of government; across our vast network of allies and partners; across all of the traditional and emergent domains of activity, and across the spectrum of conflict and competition.

USSOCOM has been studying the confluence of gray zones and growing deterrence challenges for the past decade (Jones, 2019). When a state actor incrementally violates the laws of the one whose sovereignty is being challenged in order to expand the sovereignty of the challenger, we call that a "gray zone" activity. The problem with most traditional approaches to deterrence is that they create a high risk of escalation if ever employed in the gray zone. Our opponents appreciate full-well the parameters of this gray space lying between what we say our "rules" are and what they believe we will actually enforce or against which we will enable our partners and allies to push back. The gray zone is really describing coercive, illicit, immoral, or illegal activities to incrementally advance one's interests within this "say-do" gap. Policy efforts to close this gap are essential to effective integrated deterrence in the aggregate and over time. In the meantime, Joint SOF is uniquely suited to provide a new suite of highly effective, low-risk activities to help lower the threshold of deterrence and compress this gray space.

Ultimately, the problem is not one of simply integrating lines of deterrent capabilities more effectively within recognized domains. We must also identify new approaches to expand deterrence below the current threshold and into the gray zone (Jones, 2020). These linked papers offered a few important insights.

First, modern gray zone competition, while disruptive and often illegal, is a natural occurrence in an era of rapidly shifting power. This means that while the most problematic actions of our competitive adversaries may be deterred, most adversaries cannot be dissuaded in the belief

these actions are necessary to achieving interests. It is also best to make any policy adjustments from a position of power.

Second, in these revolutionary times, the autocratic regimes we deem most dangerous to our interests keep a watchful eye on the sentiment and stability of their populations. China and Russia, for example, are often more fearful of the populations their governance negatively affects, both at home and abroad, than they are of the threat of economic sanctions or potential conflict with Western militaries.

To illustrate the nuance of this form of competition, we can point to the actions of violent extremist organizations. The non-state actors we brand as violent extremist organizations have little to hold at risk and therefore cannot be deterred. However, by adopting a more accurate understanding of the problem, there are opportunities to improve our strategic effects. By appreciating the nature of the Unconventional Warfare (UW) campaigns waged by VEOs, we realize they are reliant upon the political grievance of the populations they leverage and support—or at least a sufficiently large portion of a population to enable them to have sufficient space within which to plan and act. *VEOs are essentially conducting support to resistance*. This means we must do far more than simply attempt to "defeat" or "disrupt" their narratives and networks. As a whole, we must also actively campaign to *outcompete* VEOs for influence. This includes being a champion for more inclusive governance, less provocative policies, and the evolution of governance in general. This is not a problem one can simply "counter."

Joint SOF, particularly Army SOF, is uniquely suited to identifying and shaping disruptive political grievance, in the context of great power competition, in the places it matters most. In such restive times, it is often necessary to work with partners and allies to foster resilience and effectively immunize a population from the UW efforts of others. Equally, when that political grievance is directed toward an adversary, there is opportunity to foster and communicate credible threats of UW. This is perhaps the area where Joint SOF can make a great contribution—fostering stability and threatening instability as necessary, while at the same time posturing for potential conflict or crisis response. By campaigning for strategic influence, Joint SOF helps contribute to all aspects of advancing interests, deterring conflict, and posturing for success in myriad subtle ways.

Revolutionary Thought, Evolutionary Action

One inherent disadvantage of being a status quo actor dedicated to preserving a rules-based order is that one's own actions are constrained by those rules, while one's revisionist opponents will continuously test the limits of what they can accomplish short of war. The character of our status, coupled with our duty to coordinate within and between agencies, as well as within and between our network of partners and allies, is both our greatest strength and our greatest weakness.

While thoughts on change can be revolutionary in their character and speed, true change is evolutionary at best, as it grinds against multiple forces of inertia. Autocratic revisionist regimes do not suffer this problem. As the African proverb advises, *"If you want to go fast, go alone. But if you want to go far, go together"* (Whitby, 2020). Ultimately, the real question is, how do we slow down these fast-moving revisionists, steering them away from actions most dangerous to our interests, while creating the decision time and space necessary for our own policy leaders and those of our allies and partners to adjust?

The US-led rules-based order has the potential to go very far indeed. We must, however, be intellectually honest about the problems at hand. These revisionist actors are not out to get us as an end in itself; we simply stand in the way of their ambitions. While the United States has had its own struggles in this rapidly evolving strategic environment, one thing has become increasingly clear over the past two years: The United States—working closely with the central states in the "Western" system—remains the best option for advancing and securing a stable world order. USSOCOM appreciates how Joint SOF plays a unique and powerful role in helping lower the threshold of deterrence, reduce the likelihood of conflict, foster resilience, and help sustain an evolving world order. This tumultuous era demands the United States be a leader our partners and allies can trust to lead this delicate evolution of governance, policies, and relationships. This demands equal evolutions in how we campaign for integrated deterrence.

While new strategic guidance is fairly clear as to what must be done, how it is to be done is a much vaguer space, and one left to each agency, Service, and component to resolve. Those who optimize emergent domains of space and cyber will have tremendous advantages, and USSOCOM certainly looks to fully integrate both into our future approaches. However, the opportunity space most relevant to Joint SOF in general, and particularly Army SOF, is among the restive and empowered populations of the planet. This is a space where one's actions can either foster influence and resilience or create grievance and provocation. Those who understand and optimize this space best will have the decisive advantage in this growing competition. Joint SOF is uniquely suited to campaign effectively throughout this space, fostering influence, resilience, and stability where desired, and posturing to leverage grievance where necessary to deter or coerce. It is also through these strategic influence campaigns that Joint SOF sets the conditions for effective Crisis Response (CR) and Counter Weapons of Mass Destruction (CWMD) operations, as well as setting the theater for the larger Joint Force, should contingencies arise.

"How" is always the most difficult question. We've put a great deal of thought into "why" these modern challenges exist. Now the task is to make those evolutionary changes. Now is the time to reframe and refine how we understand the challenges before us. Now is the time to craft new campaigns and to refine and rebalance the force for new approaches, new purposes, and new effects. This will be no easy task, but one fully embraced by the men and women of USSOCOM.

References

Brown, K. E. (2022, March 28). Transnational terrorism. *E-International Relations.* https://www.e-ir.info/2022/03/28/transnational-terrorism-2/

Jones, R.C. (2021). *Strategic Influence: Applying the Principles of Unconventional Warfare in Peace.* Department of Defense, Joint Staff J3, Strategic Multilayer Assessment. https://nsiteam.com/strategic-influence-applying-the-principles-of-unconventional-warfare-in-peace/

Cronk, T. M. (2021). *DOD official outlines 2022 National Defense Strategy in CNAS forum*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/2869837/dod-official-outlines-2022-national-defense-strategy-in-cnas-forum/

Irwin, W., & Wilson, I. I. (2022). The fourth age of SOF: The use and utility of special operations forces in a new age. *Joint Special Operations University.* https://jsou.libguides.com/ld.php?content_id=65814810

Jones, R. C. (2019). Deterring "competition short of war": Are gray zones the Ardennes of our modern Maginot Line of traditional deterrence? *Small Wars Journal*. https://smallwarsjournal.com/index.php/jrnl/art/deterring-competition-short-war-are-gray-zones-ardennes-our-modern-maginot-line

Jones, R.C. (2020). Conceptualizing the future of US special operations. *Small Wars Journal.* https://smallwarsjournal.com/jrnl/art/conceptualizing-future-us-special-operations

United States Special Operations Command. (2022). Special Operations Forces Vision and Strategy. https://www.socom.mil/sof-vision-and-strategy.

United States Special Operations Command. (2015). *White paper: The gray zone.* https://www.soc.mil/swcs/ProjectGray/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf

Votel, J. (2015). Finding balance in a shifting world. *United States Special Operations Command. https://nsiteam.com/social/wp-content/uploads/2022/04/Strategic-Appreciation-Signed-9-Mar-2016.pdf*

Whitby, A. (2020, December 25). Who first said: if you want to go fast, go alone; if you want to go far, go together? *Andrew Whitby.* https://andrewwhitby.com/2020/12/25/if-you-want-to-go-fast/

Army Special Operations Forces' Expanding Role in Deterrence

Dr. Robert M. Toguchi
USASOC
robert.toguchi@socom.mil

Introduction

The recent war between Russia and Ukraine emerged in a scope and scale unprecedented since the Second World War. On February 24, 2022, Russia launched a five-prong military invasion of Ukraine with large-scale conventional forces. Although Russian President Vladimir Putin called it a "special military operation," the roots of this large-scale conflict go back to 2014, when Russia invaded and annexed Crimea while Russian-supported separatist forces seized parts of the southeastern Donbas region.

In 2022, conventional deterrence experienced challenges. In the wake of the Russian invasion, the US military recognized the foundational importance of strengthening deterrence at the strategic and operational levels to prevent future wars of aggression. In the emerging operational environment, deterrence cannot be limited to operational forces only designed for high-end military conflict. Today, deterrence may come, in many forms, to include the application of Special Operations Forces through irregular warfare to ensure that all elements of national power are implemented to the fullest capacity prior to the next large-scale invasion.

Framing ARSOF's Expanding Role in Deterrence

In an era of competition between great powers, the premise of this evolving concept is that the focus must now be on deterrence. Where multiple threats are altering the global security environment to the extent that prevention is no longer an option, shaping or spoiling actions, or at a minimum preventing threat actions from escalating beyond our strategic depth and ability to respond, is an emerging requirement. Our underlying hypothesis can be summarized as follows: *In the emerging security environment, deterrence must expand beyond preventing something from happening, but also about preventing conflict from escalating beyond US strategic depth or capability to respond, in a manner consistent with our National values.*

In a world characterized by increased volatility, an evolving concept of deterrence recognizes the need to expand deterrence thinking beyond high-end conventional or nuclear capabilities and consider threats to national security across the spectrum of conflict. Although the pre-conflict space of global competition will continue to be led by the Department of State, national guidance suggests the DoD support to a broader approach is needed. The DoD possesses unique capabilities to assess, sort, form a response, and rescale security threats long before they escalate beyond the nation's strategic depth and ability to respond.

In consideration of security threats and capabilities across the operational continuum, *deterrence can be defined as the prevention of adversary action through the signaling or use*

of credible physical, cognitive, and information capabilities that raise an adversary's perceived cost to an unacceptable level of risk relative to the expected benefit.

With an emphasis on pre-conflict force posture and readiness, this chapter will explore five broad conceptual lines of effort to strengthen deterrence, which include: 1) Expanding the Strategic Start Point, 2) Rethinking Strategic Power and Reframing Power Projection with two sub-components, Partner Based Power and Population Based Power, 3) Gaining an Information Advantage, 4) Rethinking Asymmetric Approaches, and 5) Expanding Technology Solutions for Irregular Warfare.

Expanding the Strategic Start Point

The totality of the security challenges facing the United States and its allies and the evolving character of these threats require an operational framework to win early to prevent these challenges from scaling beyond the nation's strategic depth and ability to respond. Such an operational framework begins with an earlier Strategic Start Point for campaigning. The framework for this approach centers on forward basing in and around the people with deep knowledge of the environment to generate decisive situational awareness to better inform the proper strategic start point for campaigns where the "Win" can occur at a much lower level of effort. An earlier "Strategic Start Point" requires new thinking about the traditional military Phase 0 and new thinking about when "Left of Phase 0" campaigns can begin. Re-framing the Strategic Start Point requires us to consider how we assess, sort, form a response and rescale security challenges to win early and preserve strategic depth and decision space for our national decisionmakers. An example of this approach can be seen in the early investment of US SOF trainers and advisors over many years to ensure the relative combat effectiveness of Eastern European SOF formations and employment of advanced technology capabilities.

Rethinking Strategic Power and Reframing Power Projection

Traditional considerations of power projection generally center on long-range stand-off or rapid expeditionary capabilities. Rethinking strategic power to address security challenges emanating from the gray zone, below the level of armed conflict, considers power beyond traditional warfighting capabilities to examine the full range of national, allied, partner, and population-based power. Reframed power projection envisions leveraging bilateral capabilities through a focus on extant partner and population-based power in and around the operational area, in support of persistent campaigns below armed conflict, to mitigate threats early in their development and risk profile. In an era of persistent unrest and global insecurity, the application of indigenous mass is a fundamental component of power projection. The effectiveness of recent Ukraine defenses comprised of military, security forces, and population-based defenses attests to the power of these approaches.

Partner-Based Power

Partner-based power is a vital component of ARSOF's emerging role in deterrence and centers on leveraging persistent forward presence to shape, develop, enable, and integrate indigenous

governments, militaries, and security forces into a broad framework of strategic power. Partner-based power focuses on developing and accessing host nation capabilities to produce credible power in the operational area to achieve relative superiority over the physical, cognitive, and information security environments of key populations and locations. At its core, partner-based power is centered on operating "with and through" foreign governments, militaries, security forces, and non-governmental organizations[1] to support local, regional, and global deterrence efforts. Operations in Northern Iraq, Colombia, El Salvador, and the Philippines offer compelling examples of effective partner-based power.

Population-Based Power

Population-based power is also a vital component of ARSOF's emerging role in deterrence and centers on persistent influence to shape, develop, enable, and integrate local perceptions, attitudes, behaviors, decision-making processes, and actions that support a broad framework of strategic power. Population-based power relies upon influence over time to address trends in competition and to achieve relative superiority over the physical, cognitive, and/or information security of key personas, groups, and populations. Population-based power includes actions and/or messaging to encourage desired behavior in targeted populations, such as support to legitimate governments, countering malign activities, etc. In semi-permissive or denied environments, population-based power leverages select populations to facilitate a resistance movement than can deny adversary regime objectives and policies or, in extreme cases, facilitate regime change. Population-based power enhances resilience. It also focuses on operating "with and through" relevant persons and populations, both of which are designed to create indigenous mass forward in the operational area to support local, regional, and global deterrence efforts.

Gaining an Information Advantage

An information advantage is key to deterrence in the gray zone. ARSOF require persistent forward presence working with partners and allies to establish and improve US placement, access, and influence. ARSOF must have the ability to converge all-domain effects to coordinate, synchronize, and campaign globally in the gray zone.

Transregional Fusion Headquarters

To coordinate special operations across geographic, political, and military boundaries, ARSOF may need a transregional C2 capability that can fuse all-domain capabilities to achieve US deterrence objectives. The purpose of a transregional fusion headquarters is to facilitate the rapid and continuous integration and convergence of capabilities in all domains, the electro-magnetic spectrum (EMS), and the information environment. This enables the Joint Force to optimize effects and raise an adversary's estimate of the perceived cost of action to an

[1] The U.S. Army defines mass as: "Concentrate the effects of combat power at the decisive place and time." See Headquarters of the Department of the Army (2004).

unacceptable level of risk across human-imposed boundaries—it eliminates gaps and seams across the operational space. The special operations component commander would have a tool to employ special forces, civil affairs, and psychological operations capabilities from across all geographically oriented SOF commands, partnered with capabilities from cyber, space, and other JIM partners.

Cognitive Targeting as an Enabler

Cognitive Targeting consists of employing culturally aware and regionally attuned ARSOF to influence the perception and behavior of relevant audiences through the low-signature application of lethal and non-lethal actions. ARSOF coordinates actions and messaging with the DoD and other JIM partners to accomplish US strategic objectives. For example, ARSOF may leverage personal relationships and messaging influence over an adversary's troops to remain in their barracks prior to a joint forcible entry operation. Cognitive targeting may also entail an information plan to influence religious leaders to condemn ethnic cleansing by an adversary government.

Rethinking Asymmetric Approaches

Joint Publication 1-02 defines asymmetry in military operations as "the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent's strengths while exploiting his weaknesses" (Joint Staff, 2014). In a competitive environment, asymmetric approaches can be advantageous to optimize forces, capabilities, and relationships to achieve a relative positional advantage over our toughest adversaries.

SOF-Cyber-Space Triad as an Asymmetric Approach

One form of asymmetry is the recent emergence of the converging capabilities and effects of SOF, Cyber, and Space 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 SOF Cyber Space 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.

Expanding Technology Solutions for Irregular Warfare

Forward presence and proximity with populations is paramount to maintaining a competitive advantage in Irregular Warfare. To that end, technology-based deterrence solutions have long been a key element in the national security calculus. During the Cold War, deterrence required a new level of technological sophistication to counter the former Soviet Union and roll back the spread of Communism. In the 1970s, Secretary of Defense Harold Brown and Under Secretary William Perry implemented a plan to emphasize advanced technology solutions to deter the former Soviet Union and gain technical superiority but this time focused on stealth capabilities, precision strike weapons, and improved command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) (Martinage, 2014).

The emerging operating environment requires technology solutions for Irregular Warfare. Social, political, informational, and economic trends in international competition are converging among state actors, non-state actors, and others for relative superiority over key populations. Such technologies may include enhanced cyber-enabled collection and analytical capabilities leveraging open-source information and a robust reachback to subject matter expertise to conduct social media exploitation and analysis, AI-enabled data fusion, human terrain mapping, sentiment analysis, trend analysis, pattern-of-life analysis, and predictive analytics.

Conclusion

State and non-state actors are increasingly employing combinations of conventional, irregular, and hybrid strategies across the conflict continuum to achieve their objectives. Russia's actions in Eastern Europe, China's activities in the South China Sea and the rise of non-state actors are contemporary examples that suggest a need to re-examining deterrence thinking and to define what a "Win" looks like in the gray zone.

ARSOF's role in deterrence considers deterrence across the entire operational continuum to confront low- and high-end competitors in the early 21st century security environment. It offers a way to address the escalation of many security challenges we face earlier in their development and risk profile. In doing so, it will broaden strategic options in terms of time, decision space, and approaches for our national decision-makers.

References

Headquarters of the Department of the Army. (2004). *FM 1-02: Operational terms and graphics*.

Joint Staff. (2014). *Joint publication 1-02: DOD dictionary of military and associated terms.* http://www.dtic.mil/doctrine/dod_dictionary/index.html

Martinage, R. (2014). *Toward a new offset strategy: Exploiting U.S. long-term advantage to restore U.S. global power projection capability* [PowerPoint slides]. Center for Strategic and Budgetary Assessments

Contentious narratives and disinformation about nuclear weapons in strategic deterrence and competition: A SOF perspective

Ms. Lesley Kucharski
Analyst Lawrence Livermore National Laboratory
Kucharski2@llnl.gov

Maj. Trish Wyman
US Army
trisha.e.wyman.mil@socom.mil

Dr. Zachary Davis
Senior Fellow, Center for Global Security Research, Lawrence Livermore National Laboratory
davis126@llnl.gov

Russia's "special military operation" in Ukraine demonstrates the challenge for strategic deterrence and competition of countering contentious narratives and disinformation about weapons of mass destruction (WMD) during conventional regional wars against a nuclear-armed adversary. Moscow uses both tailored, contentious narratives and targeted disinformation about WMD in Ukraine to influence and disrupt local and global perceptions in support of its deterrence and competition objectives vis-à-vis the United States and NATO. Since December 2021, Moscow has made a focal point of chemical, biological, radiological, and nuclear weapons in its efforts to establish a permissive environment for its military build-up on the border with Ukraine and then its military intervention.

These information tactics also demonstrate an opportunity for US Special Operations Forces (SOF). They are a case study for considering how SOF can contribute to strategic deterrence and competition objectives, specifically countering adversary gray-zone information efforts to alter regional security orders.[1] Such a role is in line with the 2022 Special Operations Forces Vision and Strategy, which provides a framework for the evolution of SOF into "a force capable of creating strategic, asymmetric advantages for the nation as a key contributor of integrated deterrence" (United States Special Operations Command, 2022).

This paper briefly examines this strategic challenge and SOF opportunity, focusing narrowly on the distinction between contentious narratives and disinformation about nuclear weapons and the role of SOF in countering these gray-zone information tactics. The nuclear dimension of Moscow's contentious narratives and disinformation in the "special military operation" is of particular interest because it demonstrates the distinction between strategic efforts to

[1] For a thoughtful discussion about the roles SOF can play in supporting US strategic deterrence objectives, see: Roberts 2021.

influence and *disrupt* local and global perceptions in Moscow's favor. This distinction between influence and disruption is less clear with Russia's contentious narratives and disinformation about chemical and biological weapons in Ukraine, as disinformation about these two types of WMD appears to overwhelm contentious narratives. We believe this distinction is useful for policymakers and warfighters responsible for countering gray-zone information tactics because it provides a framework for crafting tailored responses to contentious narratives and disinformation about nuclear weapons and other WMD. The chapter concludes with a discussion of efforts that could be undertaken by SOF in cooperation with other relevant stakeholders to address this aspect of adversary gray-zone information tactics.

A conceptual framework for identifying contentious narratives and disinformation

Our analysis makes a distinction between contentious narratives intended to influence US strategic deterrence and nonproliferation policies, and overt and covert disinformation intended to disrupt those policies (See Figure 1 for a graphical representation of the difference between influence and disruption). Under this framework, contentious narratives do not qualify as disinformation unless they were articulated and used for the purpose of bluntly undermining declared US policies. Put differently, we make a distinction between subjective and differing yet plausible threat perceptions and strategies, and objectively false and malicious information. The former informs contentious narratives that are considered within the normative bounds of diplomacy, deterrence, and competition. The latter constitutes disinformation, which is outside the normative bounds of these traditional processes of statecraft, at least for democratic governments. Both approaches have deep roots in the Russian theory and practice of information confrontation (*informatsionnoye protivoborstvo*, or *IPb*) (Defense Intelligence Agency, 2017, p. 37).

Table 1: Ends-ways-means framework for understanding the difference between influence and disruption. According to this framework, disruption is a subset of influence, and influence is not always disruption.

Ends	Ways	Means
Influence	Contentious narratives (benign or malicious)	Diplomacy, competition, deterrence
Disruption	Disinformation (malicious)	Information warfare

This conceptual framework is useful for understanding adversary threat perceptions and can help policymakers and warfighters craft tailored responses to adversary influence and disruption efforts. Russian gray-zone information tactics in the "special military operation" in Ukraine are an illustrative case study.

Analyzing Russian claims about Ukrainian nuclear weapon ambitions

Analysis of Russian claims about Ukrainian nuclear weapon ambitions using our conceptual framework leads to three key judgements:

1. Russia employs a mix of contentious narratives and disinformation about Ukrainian nuclear weapon ambitions across the global information ecosystem and the local Russian-language information ecosystem.
2. Russian claims appear to be tailored to each information ecosystem despite eventual overlap as the claims proliferate, suggesting that Moscow may have different strategic objectives for each audience. While Moscow appears to target global and local audiences with contentious narratives about Ukrainian nuclear ambitions to influence perceptions in Moscow's favor, Moscow appears to target local Russian-speaking populations with overt and covert disinformation to disrupt anti-war narratives (Watts, 2021).
3. High-level Russian officials appear to refrain from proliferating at the global level the same nuclear disinformation that is promoted in the local Russian-language information ecosystem. This starkly contrasts with high-level Russian statements about other WMD in Ukraine, most notably biological weapons.

Contentious narratives about Ukrainian nuclear weapon ambitions preceded the "special military operation," emerging on 21 February 2022 at the highest political level from President Putin (Putin, 2022a) and Defense Minister Shoigu (Shoigu, 2022) in response to remarks made by President Zelensky at the Munich Security Conference on 19 February 2022. In his speech, Zelensky stated that "Ukraine will have every right to believe that the Budapest Memorandum is not working and all the package decisions of 1994 are in doubt" if consultations within the framework of the Memorandum do not happen or do not result in improvements in Ukraine's security environment (Zelensky, 2022).[2] Moscow seized this part of the statement and immediately made it a focal point in its narrative about cooperation between NATO and Ukraine. Moscow claims that the statement revealed Kiev's nuclear weapon ambitions, and it emphasizes that a nuclear-armed Ukraine would be unacceptable for Russian security. It appears that Moscow uses this contentious narrative about Ukrainian nuclear ambitions to influence global and local perceptions and cultivate a permissive environment for the "special military operation."

Two hypotheses could explain Russian motivations for this contentious narrative about nuclear weapons. First, this contentious narrative might represent genuine threat perceptions and therefore would fall within the realm of *strategic deterrence and stability signaling*. Moscow could believe that Kiev desires to acquire nuclear weapons and that it is in a position to do so, especially if it has the backing of the United States and NATO. A Ukraine with an

[2] The Budapest Memorandum on Security Assurances of 1994 provided Ukraine, Belarus, and Kazakhstan security assurances from Russia, the United States, and United Kingdom when the three former Soviet Republics joined the NPT as Non-Nuclear Weapon States (NNWS).

independent nuclear force or under the protection of US or NATO extended nuclear deterrence guarantees appears to be a genuine threat perception, judging by the content and quantity of public statements from high-level Russian officials, although technical analysis casts severe doubt on the idea of an indigenous Ukrainian nuclear weapons capability.[3] Nevertheless, President Putin repeated the narrative in his address to the nation that marked the start of the "special military operation" on 24 February (Putin, 2022b), and he has continued to repeat this narrative throughout the operation, expressing anxiety about perceived Transatlantic support for (or lack of Transatlantic criticism of) Zelensky's remarks in Munich (Putin, 2022c).

This narrative is tied to Moscow's perception that the United States and NATO, backed by nuclear weapons, are using Ukraine as a foothold for aggression against Russia. Moscow sees Western support for Kiev as a direct threat to Russian security. If this threat perception about Ukrainian nuclear ambitions is genuine, then the implications for possible Russian actions to prevent such a scenario suggest a greater willingness to escalate the conflict. Additionally, Moscow may assess that this confusing rhetoric about Ukrainian nuclear weapon ambitions, in combination with its own explicit nuclear signaling, conveys its high stake in the conflict and enhances its deterrence posture vis-à-vis the United States and NATO.

A second hypothesis is that this narrative about Ukrainian nuclear weapons ambitions does not represent genuine threat perceptions but falls into the realms of contentious *diplomacy and strategic competition.* Under this scenario, the narrative is an opportunistic and convenient focal point for the "special military operation" that emerged in response to the remarks made by President Zelensky in Munich. Creating confusion and anxiety about Moscow's nuclear rhetoric might also create a permissive environment for conflict escalation, possibly even laying the groundwork for Moscow to use nuclear, chemical, or biological weapons. From this perspective, Moscow is "flooding the zone" with influence operations that do not necessarily reflect actual threat perceptions but are seen as advantageous to its military efforts.

Starting on 03 March, the SVR and Russian state media began supplementing contentious narratives about Ukrainian nuclear ambitions with overt and covert disinformation about Ukrainian nuclear capabilities and facilities. On 03 March, the head of the SVR, Sergei Naryshkin, announced that the SVR had evidence that Ukraine was developing nuclear weapons, and that the United States knew about this but did nothing to stop Ukraine (RIA Novosti, 2022a). On 04 March, the scientific community at the Kurchatov Institute[4] issued a statement in support of the "special military operation," recognizing, among other things, the "danger of new types of weapons that are being developed in laboratories bordering Russia" (Kurchatov Institute, 2022). While this statement appears to fall within the realm of nuclear

[3] An indigenous nuclear weapon program would require Ukraine to acquire highly enriched uranium or plutonium, presumably diverted from its civil nuclear power program, which is under full scope safeguards by the IAEA in accordance with Ukraine's obligations as a NNWS under the NPT.

[4] The Kurchatov Institute played a foundational role in the development of the Soviet nuclear weapons program.

influence, Russian state media refers to it in the context of nuclear, chemical, and biological disinformation about Ukraine. On 06 March, an unnamed "representative of an authoritative Russian government agency" told RIA Novosti that Kiev was using the Chernobyl Exclusion Zone to make dirty bombs and nuclear weapons, intentionally blurring the distinction between nuclear weapons and radiological devices (RIA Novosti, 2022b).

This stream of nuclear disinformation appears to have originated in the Russian information ecosystem several days after the contentious narrative about Ukraine's nuclear weapon ambitions and at lower levels of government through the SVR and Russian-language news outlets and talk shows, suggesting that Moscow may be targeting Russian-speaking populations in Russia and Ukraine with disinformation. Moscow may be using disruptive *disinformation* to *reactively shape public opinion* away from supporting the pro-Western regime in Kiev and shift the focal point in discussions about responsibility for the nuclear safety and security concerns stemming from military activity at Ukrainian nuclear facilities (International Atomic Energy Agency, n.d.).

While the line between these contentious narratives and disinformation about Ukrainian nuclear ambitions may be blurry, the distinction can help guide US policy responses. This analysis suggests that the United States should exercise restraint when responding to contentious narratives that reflect Russia's genuine threat perceptions and instead seek to shape Russian behavior and degrade Russian resolve with other explicit and tacit means of deterrence.[5] This analysis also suggests that the United States should compete for narrative dominance in response to opportunistic narratives and disinformation, as neither reflect genuine threat perceptions.[6]

A role for USSOCOM in addressing contentious narratives and disinformation about WMD

This analysis has implications for USSOCOM. Contentious narratives and disinformation about nuclear weapons and nuclear safety and security in Ukraine are not confined to Russia and Ukraine but flow into NATO countries and beyond, where concerns and confusion about nuclear issues can affect efforts to support Ukraine and reinforce allied deterrence and defense. Longstanding USSOCOM support for US allies could become the target of Russian disinformation, as has been the case for Defense Threat Reduction Agency support for public health research laboratories in Ukraine and across the post-Soviet space (Defense Threat Reduction Agency, n.d.). Contentious narratives and disinformation aimed at joint training of NATO and partner SOF forces, emergency preparedness exercises, or chemical, biological, radiological, and nuclear (CBRN) training could create confusion and controversy about SOF activities in Europe and beyond.

---

[5] For a discussion of explicit and tacit means of deterrence, see Schelling (1960), pp. 5, 21, 54.

[6] For a discussion about the potential objectives of strategic competition, see: Durkalec et al., 2018.

We have explored a wide range of possible SOF roles in the digital domain in a volume written for USSOCOM entitled *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* (Davis et al., 2021). Several chapters offer operational concepts for SOF to integrate a broad variety of cyber and social media tools into USSOCOM practice. In this paper, we focus on the specific challenge of supporting US strategic deterrence and competition objectives by countering contentious narratives and disinformation that target US nuclear policies and cooperative CBRN threat reduction support systems.

As the lead coordinator for counter-proliferation and owner of psychological operations (PSYOP) forces (United States Special Operations Command, n.d.), USSOCOM is uniquely positioned to both counter WMD and conduct influence operations on behalf of the USG (Lin & Wyman, 2021). SOF are regularly positioned around the world, alongside US diplomats, often in austere, high-risk locations. SOF are also enabled to conduct CONUS-based operational support (CBOS) (1st Special Forces Command – Airborne, 2021) meaning that SOF physically located in the United States can execute digital influence missions and global operations in the information environment with the right authorities, permissions, and as directed (United States Department of Defense, 2016). Such missions could highlight the contributions of cooperative threat reduction and international nonproliferation institutions such as the IAEA and Organisation for the Prohibition of Chemical Weapons (OPCW) to global security. Positive narratives could proactively inform and influence public perceptions on a wide range of nuclear safety and security topics. Nuclear, chemical, and biological themes could document the dangers of conducting military operations at nuclear installations and the risks of using or threatening to use WMD. Specialized efforts could extend the influence of these narratives to reach a broad array of non-English speaking audiences. Country teams are adept at crafting appropriate narratives and targeting local media outlets.

USSOCOM could pursue three lines of effort. First, expand and normalize CBOS in support of global multi-domain operations by standing up an Information Warfare Task Force on Weapons of Mass Destruction (IWTF-WMD) that reports to the Principal Information Operations Advisor (U.S. House Committee on Armed Services, 2021). This task force could be positioned at Fort Bragg, North Carolina, which provides direct access to global PSYOP experts within the 4th and 8th PSYOP Groups who can rotate in and out of these missions, and it could be led by senior PSYOP and Army Nuclear and Counterproliferation officers. The IWTF-WMD could be modeled on the Theater Special Operations Commands that serve as one-stop shopping for regional commands to access and coordinate with USSOCOM. This concept would allow the highest priority issues to be addressed quickly without delaying or restricting operations at the strategic level.

Second, establish a mechanism within the IWTF-WMD for quickly coordinating with other entities that have equities in supporting US deterrence and competition objectives by countering contentious narratives and disinformation about WMD. The list of entities should include USSTRATCOM and USCYBERCOM (Lin & Wyman, 2021, p. 349); stakeholders across

the US interagency, such as the State Department and the National Nuclear Security Administration; and other relevant allied and partner stakeholders. This coordination mechanism could facilitate a more unified, proactive, and timely response to contentious narratives and disinformation in peacetime, crisis, and war.

Third, direct the IWTF-WMD to conduct information campaigns to counter contentious narratives and disinformation about WMD in coordination with WMD subject matter experts. For example, USSOCOM could use the IWTF-WMD to do the following:

1. Develop and disseminate factual information about US and allied WMD policies as well as competitive counter-narratives that expose and counter disinformation (Lin & Wyman, 2021, p. 346).
2. Use AI/ML technology to inform counter-narrative development and dissemination by proactively sampling, binning, and analyzing contentious narratives and disinformation about WMD (Scharre, 2021). This should entail efforts to determine, track, and measure the impact of adversary targeting and messaging.
3. Identify key and central influencers within the relevant information ecosystems and scale their online social networks to increase the size of accessible audiences, while targeting to increase or reduce dissemination as appropriate (Mislove et al., 2007; Lin & Wyman, 2021, p. 347).

Conclusion

Countering gray-zone information warfare tactics involving contentious claims about WMD in conventional regional wars with a nuclear-armed adversary is a new challenge for US strategic deterrence and competition objectives. Efforts to counter these tactics benefit from an analytical framework that distinguishes between contentious narratives and disinformation. This analytical framework suggests that the United States can develop flexible and tailored responses. USSOCOM can play a role in this process by creating synergies between its PSYOP and counter-proliferation missions and coordinating with relevant stakeholders across the USG.

References

Davis, Z.; Gac, F.; Rager, C.; Reiner, P.; & Snow, J. (2021). *Strategic latency unleashed: The role of technology in a revisionist global order and the implications for special operations forces.* Lawrence Livermore National Laboratory. https://cgsr.llnl.gov/content/assets/docs/StratLatUnONLINE.pdf

Defense Intelligence Agency. (2017). *Russia military power report.* https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf

Defense Threat Reduction Agency. (2022, April 11). *Disinformation aimed at DTRA* [Press Release]. https://www.dtra.mil/News/Countering-Disinformation/

Durkalec, J., Gasser, P., & Shykov, O. (2018, November 13-14). *Multi-domain strategic competition: Rewards and risks.* 5th Annual LLNL Deterrence Workshop. United States. https://cgsr.llnl.gov/content/assets/docs/Deterrence_Workshop_Summary_Final2018.pdf

International Atomic Energy Agency. (n.d.). *Nuclear safety and security in Ukraine.* https://www.iaea.org/nuclear-safety-and-security-in-ukraine

Lin, H., & Wyman, T. (2021). Special operations forces and cyber-enabled influence operations. In Z. Davis, F. Gac, C. Rager, P. Reiner, & J. Snow (Eds.), *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* (pp. 333-351). Lawrence Livermore National Laboratory. https://cgsr.llnl.gov/content/assets/docs/StratLatUnONLINE.pdf

Mamontov, A. (2022, January 22). *The Andromeda strain. Documentary by Arkady Mamontov* [Video]. YouTube. https://m.youtube.com/watch?v=pA0JRyxH1GM

Mislove, A., Marcon, M., Gummadi, K. P., Druschel, P., & Bhattacharjee, B. (October 2007). *Measurement and analysis of online social networks*. Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. New York, NY, United States.

Putin, V. (2022, February 22). *Presidential address*. President of Russia. http://kremlin.ru/events/president/news/67843

Putin, V. (2022a, February 21). *Presidential address*. President of Russia. http://kremlin.ru/events/president/news/67828

Putin, V. (2022b, February 24). *Presidential address*. President of Russia. http://kremlin.ru/events/president/news/67843

Putin, V. (2022c, March 5). *Meeting with flight crew representatives of Russian airlines.* President of Russia. http://kremlin.ru/events/president/news/67913

RIA Novosti. (2022a, March 3). Naryshkin announces SVR has proof that Ukraine was developing nuclear weapons. https://ria.ru/20220303/oruzhie-1776346303.html

RIA Novosti. (2022b, March 6). Source reveals Ukraine's motivations for using the Chernobyl NPP. https://ria.ru/20220306/chaes-1776880399.html.

Roberts, B. (2021). Special forces and strategic deterrence. In Z. Davis, F. Gac, C. Rager, P. Reiner, & J. Snow (Eds.), *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces,* (pp. 51-60). Lawrence Livermore National Laboratory, https://cgsr.llnl.gov/content/assets/docs/StratLatUnONLINE.pdf.

Scharre, P. (2021). Artificial intelligence: Risks and opportunities for SOF. In Z. Davis, F. Gac, C. Rager, P. Reiner, & J. Snow (Eds.), *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* (pp. 333-351). Lawrence Livermore National Laboratory. https://cgsr.llnl.gov/content/assets/docs/StratLatUnONLINE.pdf

Schelling, T. (1960). *The strategy of conflict.* Cambridge, MA: Harvard University Press.

Staff of the Kurchatov Institute National Research Center. (2022, March 4). *For scientists of Russia.*

Kurchatov Institute. http://nrcki.ru/product/press-nrcki/press-nrcki--44871.shtml?g_show=43519

Shoigu, S. (2021, December 21). *Expanded meeting of the defence ministry board*. President of Russia.
http://en.kremlin.ru/events/president/news/67402
Shoigu, S. (2022, February 21). *Security council meeting.* President of Russia.
http://kremlin.ru/events/president/news/67825
U.S. House Committee on Armed Services. (2021). *National Defense Authorization Act for Fiscal Year 2022: Report of the Committee on Armed Services, House of Representatives on H.R. 4350 together with additional and dissenting views.*
https://www.govinfo.gov/content/pkg/CRPT-117hrpt118/html/CRPT-117hrpt118.htm
United States Department of Defense. (2016). *Strategy for operations in the information environment.* https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf
United States Special Operations Command. (2022). *Special Operations Forces vision & strategy.* https://www.socom.mil/sof-vision-and-strategy
United States Special Operations Command. (n.d.). *Core activities.*
https://www.socom.mil/about/core-activities
Watts, C. (2021. April 28). Russia's disinformation ecosystem. *Homeland Security Today*. 28.
https://www.hstoday.us/subject-matter-areas/infrastructure-security/russias-disinformation-ecosystem-a-snapshot/
Zelensky, V. (2022, February 19). Full speech at 2022 Munich Security Conference. *The Kyiv Independent.* https://kyivindependent.com/national/zelenskys-full-speech-at-munich-security-conference/
1st Special Forces Command – Airborne. (2021). *A vision for 2021 and beyond.*
https://www.soc.mil/USASFC/Documents/1sfc-vision-2021-beyond.pdf

United States Southern Command (USSOUTHCOM)

USSOUTHCOM Staff

POC: Mr. Leland M. Lazarus
Special Assistant/Speechwiter, Command Action Group
leland.m.lazarus.civ@mail.mil

Introduction

As current national strategic direction states: "Today, more than ever, America's fate is inextricably linked to events beyond our shores." Nowhere is this more evident than right here in Latin America and the Caribbean (LAC). This region—our shared neighborhood—is under assault from a host of crosscutting, trans-boundary apex challenges that directly threaten our own homeland. Countering these threats requires greater U.S. attention, commitment, and investments to reverse the current disturbing trends.

The People's Republic of China (PRC)

The PRC continues its relentless march to expand its economic, diplomatic, technological, informational, and military influence in LAC and challenges U.S. influence in all these areas. Over the past year the PRC and its state-owned enterprises (SOEs) continued to target, recruit, and bribe officials at all levels in the AOR to expand their economic, political, and military influence throughout the region. PRC activities include investments in strategic telecommunication and space infrastructure, systematic technology and intellectual property theft, disinformation and propaganda campaigns, illegal, unreported, and unregulated fishing, and malicious cyber activity – all with the goal of expanding long-term access and influence in this hemisphere. As in other regions of the world, the PRC uses its economic might to co-opt and coerce countries to fulfill its strategic goals. To date, 21 regional countries participate in the PRC's Belt and Road Initiative (BRI) which provides PRC-backed loans for key infrastructure such as ports, telecommunications, roads and bridges, agriculture cultivation, and mining projects to satisfy the PRC's own growing domestic demand and pursuit of a continued monopoly of critical minerals. PRC SOEs are increasingly involved in developing facilities and other infrastructure near strategic maritime choke-points such as the Panama Canal and the Strait of Magellan. In Asia, Africa, and the Middle East, the PRC has abused commercial agreements at host country ports for military functions; our concern is that they are attempting to do the same right here in this region, close to our homeland.

Russia

In February 2022, the world witnessed Vladimir Putin's brazen aggression against Ukraine, a blatant violation of the international rules-based order established after World War II. But

Russia is also engaging in extensive disinformation campaigns to influence key national elections throughout the region this year. Russia is expanding its influence in Venezuela, Cuba, and Nicaragua, countries that allow Moscow to expand its air and sea access to project military power throughout the region. Agreements with Venezuela, Nicaragua, and Brazil allow Russian warships to make port calls on short notice. Russia seeks inroads in the hemisphere by providing security training through $2.3 billion in weapons and military equipment sales in the last 10 years, to include direct sales to Venezuela.

Transnational Criminal Organizations

TCOs blaze a trail of corruption and violence, threaten citizen security, and undermine public confidence in government institutions. They are trafficking opioids, cocaine, and other deadly drugs into U.S. neighborhoods, fueling both the drug overdose epidemic and drug-related violence.

Tragically, more than 100,000 Americans died from drug overdoses within a 12-month period, representing an almost 30% increase over the same period the previous year. Beyond drugs, TCOs traffic in humans (some "coyotes" charge between $15,000 and $20,000 per person to get illegal migrants to the U.S.), arms, illegal logging and mining, and other illicit products. Many TCOs have larger budgets and more personnel than the security forces trying to stop them.

Regional Authoritarian Regimes

Venezuela has become one of the worst humanitarian crises this hemisphere has ever seen and poses a significant security threat to the region. As a result of the regime's rampant corruption and gross mismanagement, the Venezuelan people lack basic services like clean water, food, and health care. More than six million Venezuelan refugees and migrants were displaced globally (more than 20% of the overall population). The Maduro regime actively engages in narcotrafficking and harbors regional terrorist groups like FARC and ELN within its borders. Regimes in Cuba and Nicaragua also remain a regional corrosive influence, receiving political, military, and economic support from malign actors like China and Russia.

Climate Change

Hurricanes, rising sea levels, flooding and drought are worsening economic and food security and contributing to irregular migration in the region. In August 2021, a 7.2 magnitude earthquake struck Haiti, killing more than 2,000 people and damaging thousands of homes. Communities in Central America are still recovering from the Category 4 hurricanes Eta and Iota that made landfall in 2020, destroying thousands of homes, decimating livestock and essential crops like rice, corn, and beans, and displacing nearly 600,000 people in Honduras, Guatemala, and Nicaragua. About 8 million people suffer from food insecurity due to drought in the Dry Corridor—a 1,000-mile-long geographic zone that runs through Mexico, El Salvador, Honduras, Nicaragua, and Costa Rica.

Hurricanes and drought also further exacerbate an already difficult malnutrition context and food insecurity, with Guatemala, Honduras, and Nicaragua having a combined 1.3 million children under 5 years old experiencing stunting which is a prevalence of 43, 20, and 14 percent, respectively, in each of those countries. South America is suffering extreme drought not seen since the 1940s, hampering the flow of hydroelectric dams and river transport for Paraguay and Brazil. In April 2021, a volcano erupted in St. Vincent and the Grenadines, displacing thousands. These natural disasters, along with the economic fallout of COVID-19, violence fueled by TCOs, corruption, and a perceived change in U.S. immigration policy, have driven thousands of migrants to embark on long and dangerous journeys to the U.S. border.

SOUTHCOM's Plan of Action

To address these apex challenges, SOUTHCOM is using all possible "levers" at our disposal to integrate seamlessly with other Combatant Commands, the Joint Force, allies and partner nations, Congress, the U.S. inter-agency, non-governmental organizations, and the private sector. In this fight, our regional partners are our best defense. We're building partner nation capacity in counter narcotics, cyber, space, and counter-terrorism to address these cross-cutting apex challenges.

Annual Exercises

Our annual exercises such as PANAMAX (defense of the Panama Canal), UNITAS (maritime security), and TRADEWINDS (Caribbean disaster response) build readiness and enhance our partners' capabilities, interoperability, and domain awareness. USSOUTHCOM personnel also frequently participate in our partner nations' annual exercises, including Salitre in Chile, Angel de los Andes in Colombia, and CRUZEX in Brazil.

Security Cooperation

Our security cooperation program focuses on building our partners' capacity to conduct ground and maritime interdiction, defend their cyber networks, secure their borders and sovereignty, and maintain domain awareness. The Near Coastal Patrol Vessel (NCPV) program is a USSOUTHCOM initiative to address selected Caribbean and Central American partners' requirements for a maritime patrol vessel with the capacity to conduct sustained Maritime Interdiction Operations. To date, we have fielded NCPVs in the Dominican Republic, Panama, El Salvador, and Honduras to increase interoperability and counter regional threats. Panama deployed its NCPV in December and in one month used it to conduct two successful search and rescue operations near the Gulf of Panama. We are also working closely with partners in Guatemala to strengthen their professional military intelligence capabilities, and Colombia to help them establish a secure communication network that is interoperable with the DoD.

Partners in the Fight

Years of sustained security, cooperation with our partners throughout our hemisphere is really paying dividends – we have helped build the capability of these nations to operate with us to

disrupt drug shipments before those loads enter the homeland. In 2021, Colombia led Operation Orion, which encompassed two multi-national, all-domain, operations that disrupted 217 metric tons of cocaine and captured 7 aircraft, 106 vessels, and 8 low profile vessels. The U.S. provided maritime patrol aircraft (MPA) and analyst support to these operations. This is just one example of the large return on investment gained by combining a willing and able partner with a committed

U.S. presence in the Western Hemisphere. Another example is Operation Kraken, conducted in coordination with Colombia, Panama, and inter-agency partners. Due to this joint and combined effort, the U.S. and partners seized 65 metric tons of cocaine, 22,000 pounds of marijuana, and 43 illegal vessels; destroyed 42 cocaine labs; and detained 129 drug traffickers.

Cybersecurity

SOUTHCOM helps prepare our partner nations to defend themselves against a variety of cyber threats including from malign state and non-state actors, hackers, criminal groups, and terrorist organizations. Our Joint Cyber Center continues to conduct security cooperation through our Joint Combatant Command Cyber Assistance Teams and Subject Matter Expert Exchanges to share expertise, best practices, and cyber threat indicators to assist partner nations with incident response to cyberattacks, and to further harden and secure their networks. Separately, the SOUTHCOM Joint DoDIN Operations Center (SCJDOC) monitors for malicious cyber activity in the AOR 24/7.

Space Cooperation

USSOUTHCOM is working with U.S. Space Command and the U.S. Space Force to expand military space engagement with LAC countries. Our partners in the AOR are quickly becoming space-faring nations and USSOUTHCOM is engaged to increase future opportunities for combined operations to counter regional threats. For instance, we've increased Space Domain Awareness data sharing partnerships with Brazil, Colombia, Peru, and Chile. Air Forces-Southern (AFSOUTH), our air component, works with these same partners throughout the year to advance combined space operations. In November 2021, USSOUTHCOM worked with Joint Task Force Space Defense (JTF-SD) and the Chilean Air Force on the U.S. – Chile Sprint Advanced Concept Training (SACT) Space Domain Awareness (SDA) experiment, the first of its kind in South America. The SACT connected the US Air Force Academy Falcon Telescope located at the University of La 18 Serena in Chile with JTF-SD's commercial SDA operation at Catalyst Campus in Colorado Springs, to improve safety of orbital flight for all countries. We are standing up a Space Component Command for USSOUTHCOM, with personnel focused on space cooperation, sharing open-source satellite data to help partners better track and target illegal activity happening within their borders, and signing more space cooperation agreements with partner nations.

Humanitarian Assistance/ Disaster Relief (HA/DR)

SOUTHCOM's HA/DR projects show how we can leverage flexible, responsive funding to save lives. Since the start of the pandemic, USSOUTHCOM used CARES Act funding to make over 500 humanitarian assistance donations valued at over $74 million to 28 countries. These donations included field hospitals, personal protective equipment, ventilators, and medical supplies and immediately offset the delivery of substandard vaccines from the PRC and Russia. When a devastating earthquake struck Haiti last year, USSOUTHCOM supported the U.S. Agency for International Development's humanitarian response to save lives. After 21 days of around the clock teamwork with all our Component Commands, the National Security Council, the Department of State, NGOs, and Haitian authorities, our team assisted and rescued 477 people and delivered nearly 590,000 pounds of food, water, medical equipment, and other supplies. As we continue to provide HA/DR support, we will work more closely with regional emergency management organizations to coordinate our HA/DR responses.

Maintaining the Innovative Edge

SOUTHCOM can also serve as an innovative test bed for DoD, inter-agency, private industry, and academia to develop new technologies to maintain our innovative edge over the PRC, Russia, and other adversaries. We're working on several prototypes to include an expeditionary 3D concrete printer that significantly reduces the carbon footprint. We're also leaning forward on deploying alternative flight technologies that support our missions while reducing emissions.

Climate Defense

New ideas, tools, and technologies are force multipliers, as is our technical assistance. For example, the U.S. Army Corps of Engineers continues to provide vital support to our Latin American and Caribbean partners. USACE is helping Ecuador assess and mitigate the erosion caused by a faulty PRC-built dam, Panama with a multi-billion-dollar Canal water management program, Honduras with flood control; Dominican Republic with port upgrades; Brazil with watershed development; and Colombia and Peru with military base infrastructure. Through these USACE projects, SOUTHCOM is offering viable alternatives to PRC-funded infrastructure projects; and they represent the highest standards of transparency, financial sustainability, labor protections, and environmental preservation.

Capabilities We Need: ISR and Strategic Messaging

Though we have promising levers that can make a real difference as we campaign to out-compete threats in the region, many of the programs and processes we have in place are not designed to move swiftly enough to out-compete our adversaries. Our most acute shortfalls are in Intelligence, Surveillance, and Reconnaissance (ISR), which is critical to our ability to defend against threats in our neighborhood before they impact the homeland.

Another crucial area is competition in the information space. Our adversaries are aggressive in information operations, amplifying their assistance to partners in the region and spreading disinformation to diminish U.S. credibility. We must more effectively "pierce" the information space, using all the tools available to us— traditional media, radio, TV, social media, and podcasts—to amplify our own story, shape local perceptions, and expose malign actors and their disinformation. We must highlight the value of our neighborhood in defense of our homeland and the role it plays in the global campaign for integrated deterrence. We have a great story to tell: the

U.S. is the region's trusted partner because of the values we share and the alignment of our activities to create mutual gains toward greater resilience, peace, and prosperity in the AOR.

Conclusion

The safety of our homeland is directly linked to resilience, stability, and security of our Latin American and Caribbean partners. The U.S. and our regional partners are on the front line of strategic competition, and we share crosscutting threats that we must confront together. As Secretary of Defense Lloyd Austin stated, "our allies and partners are a force multiplier and one of the greatest strategic assets we have in protecting our nation…we will act together…making us stronger as a team than the sum of our individual parts." We at SOUTHCOM believe this wholeheartedly, and we are committed to work shoulder to shoulder with our partners, maximizing our efforts where their priorities align with our own national interests. To meet these challenges, we are putting integrated deterrence into action, using all available levers—assets, resources, and authorities—across the DoD, inter-agency, allies, partners, NGOs, and private industry to fulfill our Enduring Promise to be the region's trusted partner—today, tomorrow, and always.

United States Space Command (USSPACECOM)

USSPACECOM's Apex Challenge: Ensuring US and Allied Space Superiority

Col. (Ret.) André G. Shappell
USAF
andre.shappell.1.ctr@usspacecom.mil

Lt Col Jean A. Purgason
USSF
jean.purgason@usspacecom.mil

Space is the "eyes and ears" and arguably the "heart" of Integrated Deterrence; there is no integration in deterrence without space. The same rationale employed in the development of the nation's Integrated Deterrence concept also illustrates the logic and justification for establishment of United States Space Command: a new, multipolar security environment; new forms of military competition in a growing number of domains; competition for military applications of emerging and potentially disruptive technologies; the renewal of conventional military balances of power; and the exponential growth in civil and commercial activity in space. Space plays a vital—and arguably *the central*—role in any strategy outlining the coherent use of all instruments of national and allied power to deter adversaries, assure allies, and protect strategic stability. Along with cyber, space enables capabilities in all of our levers of national power.

United States Space Command's mission is to protect and defend US and allied interests in space. Within the framework of our Unified Command Plan missions and responsibilities, the Command's fundamental objective remains to deter a conflict from beginning in or extending into space. Our key task is to provide space operations options to the National Command Authority within the context of the United States' Integrated Deterrence approach to national security.

The unique problem is that we do this in an Area of Responsibility (AOR) that *begins* 100 kilometers above the earth and extends outward indefinitely. Achieving and maintaining domain superiority—the ability to operate freely in the domain when and where we want to and for how long we need to—in that large of an AOR is our apex challenge.

The primary operational difficulty for gaining space superiority in an environment with virtually no human presence and daunting physical operating characteristics is the ability to maintain a comprehensive common operating picture of the space AOR. This is why US Space Command's first priority is to enhance our Space Domain Awareness (SDA) capabilities. We use SDA in multiple ways to support both the terrestrial warfighter and USSPACECOM's *supported* operations in the space domain.

SDA acts as a combat enabler to the terrestrial warfighter. Ever since Operation Desert Storm, coalition forces have relied on position, navigation, and timing data for troop movements and precision-guided munitions, as well as satellite communications to ensure unity of effort. SDA supports these vital force multipliers. As Russia recently demonstrated with its destructive direct-ascent anti-satellite test on 15 November 2021, potential adversaries have the capability to directly affect our space capabilities. If adversaries contemplate use of these systems against US or allied space capabilities, protecting decision space for national leaders through advanced indications and warning would prove decisive for effective mitigation and counteraction. However, this is not the only benefit of bolstering our SDA capabilities.

US Space Command has a mandate to protect and defend our national orbital assets and the space commons in general. Given the size of our AOR, there are limits to our ability to continuously monitor wide swaths of the domain. Constantly tracking objects in orbit is hard. Accordingly, the Command is looking for new ways to expand sensor coverage by adding non-traditional SDA sensors currently used in other mission areas. Some examples include the Army AN-TPY 2 and the Navy Aegis radars designed and operated for ballistic missile defense. The additional coverage provided by these types of assets shortens the time needed for orbital analysis and enables decision-quality information to best position US assets in pursuit of national objectives, both terrestrial and space-based.

The pursuit of space superiority requires different approaches depending on where we need it within the domain. Most satellites operate in or below geo-synchronous orbit (GEO). From the GEO-belt and below, the flow of information from space to earth creates the 21st Century "space lines of communication." Ensuring near-real-time data to terrestrial users, especially in times of conflict, will be a deciding factor in an engagement or campaign. When considering the cislunar operating area beyond GEO, it is useful to position space systems in strategic "chokepoints." These include lunar orbit or orbit along one of the Earth-moon or Sun-Earth LaGrange points where gravitational forces balance. Since maneuvering in space relies heavily on gravitational forces, these points represent key terrain for maintaining the cislunar high ground and for eventual travel to other planets in the solar system. Within the last couple of years, China has successfully landed a lunar rover on the far side of the moon and placed a satellite in orbit at the L2 Sun-Earth LaGrange point 1.5 million kilometers from earth (Solar System Exploration Research Virtual Institute, n.d.). Any future US and allied cislunar missions using the efficiencies of the lunar gravity well will be in full physical and electromagnetic view of these Chinese assets. Without the United States and our allies placing similar capabilities in these critical LaGrange points, we will cede information superiority and likely space superiority in these locations.

Such capability is critical to US and allied space domain awareness, space superiority, and, by extension, a robust Integrated Deterrence capability. We must continue to build a range of options from which national leadership can choose to protect and defend space operations. However, as we continue the transition to distributed space architectures, we remain overly reliant on exquisite, legacy, and low-density systems for the short-term time horizon. We must

adopt distributed architectures now and decrease reliance on legacy systems. The strategic space environment is evolving too rapidly to wait any longer.

Space enables our warfighters and society-at-large through persistent connections to information-related capabilities. Due to emerging threats in space, the United States, its allies, and its partners must invest their efforts and resources into ensuring we can gain and maintain space superiority in a time, place, and manner of our choosing. This endeavor will require increasing organic and supporting SDA capabilities to decrease decision cycles. Focusing SDA and other relevant capabilities in position to protect key areas of the domain, such as space lines of communications inside the GEO-belt and at the LaGrange points in cislunar space, will create resiliency in our space architectures. Resiliency provides a deterrent effect against opportunistic targeting in conflict. Ultimately, robust space superiority places our coalition forces in a position of strength to deter adversaries from attacking our space assets and reduces the chances of in-domain escalation.

References

Solar System Exploration Research Virtual Institute. (n.d.). *Chang'e-2 moon orbiter reaches L2 point*. NASA. https://sservi.nasa.gov/articles/change-2-moon-orbiter-reaches-l2-point/

United States Strategic Command (USSTRATCOM)

Ms. Julie McNally
J57
Julie.a.mcnally2.civ@mail.mil

Among the many apex challenges in the operational environment, the most pertinent to US Strategic Command (USSTRATCOM) is the emergence of a multipolar world. As USSTRATCOM Commander Admiral Charles Richard stated in recent remarks, we currently are operating under crisis deterrence dynamics, and the nation has received thinly veiled nuclear threats by the leader of a nuclear power. We face the difficulty of deterring two peer adversaries at the same time, who must be deterred differently, both possessing the ability to unilaterally escalate a conflict to any level of violence, in any domain, worldwide, at any time, with any instrument of national power (Richards, 2022). This multipolar challenge manifests most acutely in the economic power and strategic breakout of the PRC and in the soon to be complete nuclear recapitalization and revisionist military activities (and energy supply manipulations) of Russia. There is persistent strategic competition across the diplomatic, information, military, and economic (DIME) levers of national power, presenting the quandary of deterring both states simultaneously.

Within the *2022 National Defense Strategy*, the prioritization is the PRC challenge in the Indo-Pacific region and then the Russia challenge in Europe. The Department states in this strategy that it "will act urgently to sustain and strengthen deterrence, with the PRC as our most consequential strategic competitor." Where this intersects with USSTRATCOM's responsibilities is in carrying out the mission of strategic deterrence in an environment that has changed into a three-party dynamic. The PRC's aggression is exemplified by transits of increasing numbers of warplanes over Taiwan's air defense identification zone and sending war ships close to its territorial waters and threats to use nuclear weapons against Japan in the event that it intervenes on behalf of Taiwan in a conflict with the PRC (Heinrichs, 2021). Russia's aggression goes without saying, as its invasion of Ukraine continues. Both the PRC and Russia have been increasing their nuclear capabilities in recent years while engaging in more aggressive activities in their near abroad.

Russia

Russia has expanded its strategic forces and is expected to finish recapitalization of its nuclear triad in the next few years. Worryingly, it has pursued the development and fielding of low yield nuclear weapons that are not accountable under existing treaties. Evident in the Ukraine invasion is their deterrence messaging regarding not only having that capability, but also the will to use them. Russia is clearly communicating this willingness in order to deter US direct involvement in Ukraine and to attempt to coerce the United States and NATO into ceasing its material support to Ukraine. Russia is reasserting that it is a major world power through such

references by Russian officials to its nuclear weapons capabilities (Congressional Research Service, 2022a). Russia is expanding its stockpile of non-accountable nuclear weapons, like theater- and tactical-range systems that Russia intends to use to deter or defeat adversaries in a conflict, and Russia's stockpile of non-accountable nuclear weapons "is being modernized with an eye towards greater accuracy, longer ranges, and lower yields to suit their potential warfighting role" (Congressional Research Service, 2022b). Russia also has developed an autonomous, nuclear-powered and nuclear-armed unmanned aerial vehicle (UAV) (called Kanyon) and a nuclear-powered, nuclear-armed cruise missile (called Skyfall). Such weapons can be used both coercively and punitively. The development of a spectrum of nuclear capabilities affords Russia the opportunity to threaten Europe with non-accountable nuclear weapons while holding the United States at risk with strategic nuclear weapons. US responses may have created, unintentionally, a perception by Russia that these weapons deter US or Western intervention.

Russia has used high-precision dual capable missile strikes on Ukraine, like the SS-21 and SS-26 missiles. Because they are dual capable and can carry low yields, this can create difficulty in distinguishing them during conflict. There is a lack of response options in US and NATO nuclear arsenals if Russia does use a low yield nuclear weapon. The options for nuclear retaliatory response would be high yield and likely not deemed a credible response by Russia due to its destructiveness being outsized in comparison to the low yield detonation. While there would be the option of using prompt conventional strike capabilities, those may not be sufficient to deter Russia from nuclear use at the low yields in its inventory.

PRC

Turning to the PRC's rapid capability development in the nuclear realm, this presents another serious challenge to strategic deterrence. The PRC's strategic breakout is evidenced by the rapid qualitative and quantitative expansion of its military capabilities, enabling them to shift their strategy. This subsequently requires a shift in Department of Defense (DoD) policy. Reports last year of commercial satellites discovering the existence of three ICBM silo fields under construction indicated the potential to triple its warheads over the next several years, assuming all silos were eventually to be equipped with a missile (Radzinsky, 2022). The PRC is also increasing its number of road mobile missiles and is making investments in land, sea, and air capabilities (Radzinsky, 2022) that has allowed it to establish a nuclear triad that it is further developing. As early as 2019 there were indications that the PRC intended to keep part of its forces on a launch on warning posture, though at the time it was noted that such a posture would require two things that were lacking: more silo-based nuclear missiles and more mobile launch platforms (Office of the Secretary of Defense, 2020). Now that these shortcomings are being addressed, evidence has been collected that the PRC is reassessing its military doctrine and nuclear policy in light of these expanded capabilities. There are comments found in training manuals, reports on military exercises, and in military newspapers related to issues such as how to respond to nuclear targets being attacked by conventional means, how a launch on warning posture might be designed, and how to use nuclear weapons to deter

conventional war (Twomey, 2021). Further, there are no crisis communications established between senior leaders of the United States and the PRC. In addition to this risk, there also is a lack of insight into what strategy and policy the regime is adopting for these new capabilities. The takeaway with their strategic breakout is that it allows the PRC to depart from minimum deterrence and to employ its nuclear capabilities for nuclear coercion and warfighting.

This combination of increasing nuclear capabilities and indications of the PLA reassessing their posture and doctrine have implications for US strategic deterrence. These capabilities are likely intended to increase nuclear force survivability and reduce vulnerability to a first strike. We must understand what strategies these new capabilities will allow the PRC to pursue, so we may develop strategies for countering them.

Tripolar Considerations

The challenge inherent in the multipolar environment is the different approaches that each competitor takes. While the PRC prefers to remain opaque and fluid, Russia is clear about its capabilities development and doctrine and is confrontational. In the 2020 release of the Basic Principles of the Russian Federation's State Policy in the Domain of Nuclear Deterrence, signed by President Vladimir Putin, their policy is clearly stated. Russia will use nuclear weapons in the event of the use of nuclear weapons and other weapons of mass destruction, if used against the state and/or its allies and, secondarily, if there were aggression against the Russian Federation with conventional weapons that would put the state under existential threat (Holloway, 2022). Moreover, they would use nuclear weapons if the existence of the state is threatened or if an irreversible balance of conventional force occurred in the enemy's favor. This language was referenced recently by President Putin during the Ukraine conflict as a reminder of Russian doctrine and as part of his messaging to attempt to deter further Western involvement in the conflict. The PRC's policy and doctrine for nuclear forces, on the other hand, tends toward ambiguity about what its capabilities are or will be and what their doctrine is. While there is some awareness of new capabilities developments, it is unclear what they intend for their force posture and what their strategy and policy will be. Complicating this is the consideration that part of their calculations for these will be oriented at strategic deterrence of India.

A secondary challenge is the convergence or alignment of interests between the PRC and Russia as described in a joint statement on their strategic partnership. Chinese officials recently described this partnership as having "no limits" and signaled clear support for the Russian position against an expansion of NATO while receiving Russian support for the view that the US involvement in the Indo-Pacific theater is illegitimate (Rajagopalan, 2022). The three components of this partnership are military cooperation, increased economic ties (notably in energy), and some coordination in their responses to international political issues or events (Gorenburg, 2020), though apparently only if it does not harm their national interests. The PRC seeks to evict US influence from the Asia Pacific to establish its sphere of influence there while uniting Southeast and Central Asia via its Belt and Road Initiative. Their end goal is to

leverage regional power into global power and to change the rules based international order such that its institutions favor PRC interests. Russia's aims, meanwhile, are to reestablish its power over the near aboard in Eastern Europe and Central Asia.

As the two nations have converged and their cooperation has increased, their stated strategic partnership has given them space to maneuver, as both recognize the problem this presents for US strategy—notably the two-front problem of revisionist and increasingly aggressive near-peer nuclear competitors in two very distant theaters (Brands, 2022). Though their primary aims are focused mostly on different territories and regions and on controlling their respective near abroads, their overall revisionist and anti-status quo goals are complementary. This poses significant challenges to strategic deterrence.

Addressing These Challenges

As the operational environment has shifted to multipolarity and the old ways of understanding strategic deterrence that were rooted in the bipolarity of the Cold War are losing some relevance, the Command must meet this emerging challenge in the cognitive realm. The Command has realized it needs new models for understanding the new problem sets that have emerged in this shift to multipolarity. As nuclear capabilities have expanded and revisionist competitors increased aggressive pursuit of their national interests, the need for understanding the underlying structures of these geopolitical challenges is acute.

Recognizing this need, and recognizing that unlike during the Cold War we no longer have as many collaborative ties with researchers in the deterrence field, Admiral Charles A. Richard established an Analytic Agenda for the Command. The purpose of this process is to identify the key research needs of the Command and to connect strategic deterrence researchers with the practitioners in USSTRATCOM. By rejuvenating the importance of this research by thinks tanks, academics, and government laboratories and creating space for planners, operators, and training and exercise action officers to learn from these experts in the field of deterrence, the Command can adjust its strategy and plans to meet this multipolar challenge.

The Command has hosted studies, led research projects, hosted conferences, and contracted with researchers over the past year as we cast a wide net to bring about a competition of ideas about how to understand strategic deterrence in this multipolar moment. The Analytic Agenda has already led to the development of some new models for understanding the structures of multipolar competition and conflict. Continuing this important work with researchers can lead us to strategies for competing in the multipolar environment.

Another aspect of meeting the multipolar challenge is the Command's commitment to developing an integrated deterrence framework (IDF) via the creation of an Annex to the future Joint Warfighting Concept 2.0. The integrated deterrence framework allows Commanders and Service Chiefs to fit their operations, activities, and investments into the national deterrence scheme and to contribute to achieving those objectives. The Command recognized the challenge of carrying out regional and strategic deterrence and the need for

integration of the instruments of national power to include military, economic, informational, and diplomatic. It has been actively engaged in collaboratively developing the integrated deterrence framework. As ADM Richard stated recently, the Command has put a lot of academic rigor into understanding potential adversary decision calculi and behaviors, and these are key elements to understanding how to implement integrated deterrence (Richards, 2022). The aims of this tailored and integrated approach are to impose costs, deny benefits, demonstrate stake, expose vulnerabilities, and respond in unanticipated ways. The Command's primary mission is to deter potential adversaries from a strategic attack. This will require an integrated deterrence framework that tailors deterrence to specific potential adversaries with a holistic, whole of government approach and toolset across the spectrum of conflict. We also must adapt the force to consider resources and authorities needed to maintain strategic deterrence in not only pre-crisis, but also during crisis and conflict.

An important aspect of integrated deterrence is our network of alliances and partnerships. Our competitors seek to exploit multipolarity to serve their national interests and military objectives. By strengthening NATO and our alliances in the Indo-Pacific and leveraging these relationships as part of our campaigning, we can undermine competitor coercion, complicate their military preparations, and develop warfighting capabilities together to strengthen strategic deterrence within the multipolar environment.

As we meet the challenge of facing multiple nuclear-armed actors in the dynamic operational environment, the importance of a cognitive approach, integrated deterrence framework, and the strengthening of our alliances and partnerships cannot be understated. We must understand the structures of the new problems we face and the drivers of action by competitors. This requires research and development of new models for understanding power dynamics at play in these problems sets, so that we can develop strategies for success. In gaining that understanding and developing new strategies, these research results can feed into an integrated deterrence process. These efforts combined with the inclusion of allies and partners work toward tempering the challenge of multipolarity in the environment. These Command efforts at understanding nuclear risks, new and emerging problem sets, and ultimately new strategies for deterring competitors, are strong approaches to maintaining relative advantage in this era of strategic competition.

References

Brands, H. (25 Feb 2022). The Eurasian nightmare: Chinese-Russian convergence and the future of American order. *Foreign Affairs.*

Congressional Research Service. (10 Mar 2022). Renewed great power competition: Implications for defense—Issues for Congress. Report R43838 https://crsreports.congress.gov/product/pdf/R/R43838/92

Congressional Research Service. (21 Mar 2022). Russia's nuclear weapons: Doctrine, forces, and modernization. https://crsreports.congress.gov/product/pdf/R/R45861

Gorenburg, D. (April 2020). An emerging strategic partnership: Trends in Russia-PRC military cooperation: Security insights. *George C. Marshall European Center for Security Studies*. https://www.marshallcenter.org/en/publications/security-insights/emerging-strategic-partnership-trends-russia-PRC-military-cooperation-0

Heinrichs, R. (8 Sep 2021). China's destabilizing nuclear weapons 'strategic breakout.' Hudson Institute. https://www.hudson.org/research/17254-china-s-destabilizing-nuclear-weapons-strategic-breakoutHolloway, D. (10 March 2022). Read the fine print: Russia's nuclear weapon use policy. *Bulletin of the Atomic Scientists*. https://thebulletin.org/2022/03/read-the-fine-print-russias-nuclear-weapon-use-policy/

Office of the Secretary of Defense. (2020). *Military and security developments involving the People's Republic of China* [Annual Report to Congress]. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-PRC-MILITARY-POWER-REPORT-FINAL.PDF

Radzinsky, B. (2 Feb 2022). The strategic implications of the evolving US-PRC nuclear balance." *The Washington Quarterly 44*(4).

Rajagopalan, R. (15 Feb 2022). Putin and Xi frame a new PRC-Russia partnership. *The Diplomat.* https://thediplomat.com/2022/02/putin-and-xi-frame-a-new-PRC-russia-partnership/

Richards, ADM C. (31 March 2022). Welcoming emarks and Introduction at the US Strategic Command Deterrence and Assurance Academic Alliance (DAAA) Conference, University of Nebraska at Lincoln. https://nationalsecurity.unl.edu/2022-us-strategic-command-academic-alliance-conference-and-workshop

Twomey, C. P. (2021). Assessing Chinese nuclear posture and doctrine in 2021. *Atlantic Council, Scowcroft Center for Strategy and Security*. http://hdl.handle.net/10945/68551

Conclusion

Lt Gen (Ret.) Tim Fay
timothygfay@gmail.com

All of the Commands represented in this volume did an excellent job communicating the perspective of their security environments and how they are working to deter, compete, and be prepared to win. When considered as a whole, the similarities and convergence are remarkable—and that is the biggest "so what" of the collection. This essay postulates that never before have the modern-era Commands been so aligned with respect to threats, priorities, and challenges. That said, there are some notable differences, and there is at least one major element that went largely unaddressed. This final essay will attempt to capture this convergence, divergence, and omission in the concluding pages of this volume. The intent is to leverage a final assessment to propose further deep thinking on what is essential to preserve effective deterrence outcomes in this security environment.

First is the convergence on the perception of the pacing threats and the implications for deterrence in this evolving security environment. Perhaps the USSTRATCOM Commander, Admiral Charles "Chaz" Richards, captured this convergence of perception most succinctly and precisely when he advised that "we face the difficulty in deterring two peer adversaries at the same time, who must be deterred differently, both possessing the ability to unilaterally escalate a conflict to any level of violence, in any domain, worldwide, at any time, with any instrument of national power." This may be the most succinct but thoroughly inclusive summary of our security environment, and it is worth unpacking each of these elements and how they all relate and converge with the priorities and challenges of all the Commands.

Note that the Admiral defined the challenge of deterrence with respect to two peer adversaries. Every Command identified China and Russia as their primary concerns. As noted, it is possible that this is the first time the modern-era Combatant Commands are unified in this priority perspective regardless of their geography or function. The common threads tying the Commands together was the way both adversaries have shown disdain for—and expressed various levels of desire and intent to remove and replace—the post-World War II rules-based international order, liberal democracy, and the non-negotiable imperative of basic human rights. Note that the Admiral categorized these adversaries as peers, and that is a significant common assessment from the Commands worthy of highlight.

Second, he noted that these two peer adversaries must be deterred differently and at the same time. This is a sea change compared to previous security challenges and a significant intellectual challenge for strategists. It is also a clear indication that deep knowledge and a cultural-level understanding of our adversaries is essential to our deterrence strategy. There has been some significant initial work on the implications for US deterrence strategy if one adversary views deterrence through the lens of the traditional deterrence model and the other

through the perfect deterrence model lens, but much work remains in this area. If it is demonstrated that our two adversaries are using different deterrence models, key implications for us within our military instrument of national power include our selected strategy and how the United States, our allies, and our partners train, equip, posture, and employ our forces. Should we fail to understand how each of our adversaries perceives the calculus of deterrence from their unique perspectives, it is all but assured that our strategy, policy, and posture will not be as credible or capable as desired to communicate and create effective deterrence outcomes. This emerging deterrence challenge requires significant and immediate intellectual investment.

The third element the Admiral discusses and where most of the Commands converge is how both adversaries can escalate across domains, time, and space employing any and all instruments of their national power. No longer do two oceans, two friendly neighbors and peaceful international commons provide the sanctuary of time and space for the security of the US homeland. Our adversaries have demonstrated capability and expressed various levels of intent to leverage space, cyberspace, information, economic, and other non-traditional means as they apply gray zone ways to achieve strategic ends. While the Clausewitzian truths of the nature of war continue to hold, the character of conflict and competition has rapidly evolved. All of the Commands acknowledge this evolution and the compression of time, space, range, and the impact it has on our previous geographic sanctuary. They also acknowledge the blurred lines of military and non-military means in gray zone competition and conflict. Finally, many of the Commands highlight the need to evolve and improve our strategy to account for this changing character of conflict and competition.

Last, although not explicit in the Admiral's excellent assessment of the security environment, the strategic advantage of our alliances and partnerships is a final common thread from all Commands. The Commands identify this as not only a strategic advantage for the United States, but some also consider it a potential weakness of our adversaries. Certainly the advantages of values-sharing allies and partners are on full display in the current war in Ukraine. The common theme of preserving, strengthening, and enabling our allies and partners is one of the strongest points of convergence in this collection. And while there is remarkable convergence across these diverse Commands, there are several areas where they potentially diverge, and two will be highlighted here.

First, there may be some divergence on the primacy of the "ways" to best deter. Specifically, there was varied discussion with respect to the primacy of a force designed for current daily competition versus a force designed to deter and win a high-end conflict. On one side, that discussion noted that effective deterrence must be anchored in the competition space, with our forces and capabilities engaged with and supporting allies and partners every day in this gray zone. The other side of this discussion anchored on the need to build a credible force and posture it to be prepared to win as the foundation of credible deterrence effects. That argument postulates that unless the force is sufficient to impose costs or deny benefits at the level of major conflict, then effective deterrence outcomes may be at risk.

The second and directly related divergence is on the preponderance of force types. Those that argue the primacy of competition sometimes emphasize the need for small units, SOF, and expeditionary forces capable of building long-term relationships as essential to effective deterrence effects in competition. Those that argue the primacy of forces postured for large-scale conflict sometimes emphasize mass, agile, and responsive over-the-horizon elements and technically superior conventional formations at scale.

While not to be addressed in this paper, previous work postulates that this is not a mutually exclusive choice. That work shows that both the strategies and force elements needed for competition and those needed for conflict are required to execute a holistic and effective deterrence posture with two peer adversaries in a global, all-domain security environment. This is another area where initial work has been done, but further work is needed to connect these perspectives and truly create the desired integrated deterrence. Choosing exclusively one or the other on the ends of this continuum without the ability to integrate and adjust creates a gap worthy adversaries will exploit. It is likely that the cause of these minor divergences is partially driven by the understandable tension between mission assigned and resources allocated. It is this last point—the allocation of resources—that was not directly addressed in this collection.

Some have postulated that the best way to assess priority and risk is to assess the allocation of resources. Nations and organizations expend resources—money, people, and time—where their priorities are or where they perceive the greatest risk. While the allocation of scarce resources relative to priority and risk was implicitly addressed by some in this discussion, there was not an explicit discussion. Discussing a strategy divorced from a consideration of understanding the resourcing necessary to execute that strategy creates the potential for a disconnect. While generally the Commands look to the services to resource their requirements, it is actually a larger national question. The dramatic change in the security environment may drive such a discussion, especially in light of the current war in Ukraine. Additionally, this question should be asked in the context of all the elements of national power, and how they must work together to synergistically create the conditions favorable to deterrence. While the defense budget as a percentage of GDP is a way to gauge priority and risk perceptions over time, it cannot be the sole measure. Additionally, trying to create absolute and subjective measures of relative national power—as some nations do, according to press reports—is certainly incomplete and imprecise and is also possibly strategically incorrect. Assessing the sufficiency of resources required and expended relative to the effectiveness of our deterrence strategy and posture is a final task this essay will highlight where deep thinking has been and is still required.

So to summarize, this collection of Command perspectives is absolutely remarkable. The level of convergence on threats, priorities, and challenges is impressive. While there are divergences and omissions, they are minor and not strategic in nature. This essay also built a roadmap of needed further study for our national security community. The Commands are signaling the need for additional work and deep thinking including: deep and wide understanding of our

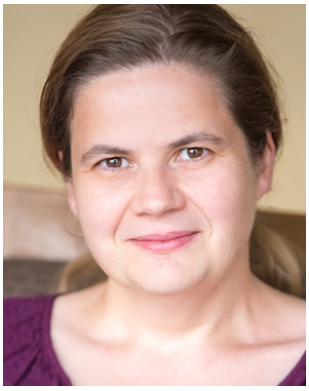
adversaries and their perspectives; a better understanding of deterrence theory and strategy effective against two distinct adversaries with two distinct perspectives; a deeper understanding of the evolving character of war as time, space, and range across all domains shrinks; work on the competition to conflict continuum and providing effective deterrence across that entire spectrum; and ways to better measure and understand the effectiveness of national resource allocation relative to creating successful deterrence outcomes. These are areas where there is great need and opportunity for intellectual commitment—all with high potential return for our nation. Hopefully, this collection added to both the discussion and understanding of the challenges and opportunities this security environment presents our Commands.

Biographies

Major General Scott F. Benedict

Major General Benedict has served as a Marine Corps officer and Naval Aviator for more than thirty years. He currently serves as director of US Central Command's Strategy, Plans, and Policy Directorate (CCJ5). He is responsible for Middle East and Central and South Asia strategy, plans, and policy development, including joint military strategies, resource allocations, warfighting assessments, and theater security cooperation activities to support U.S. national security objectives in the US Central Command area of responsibility. He is a graduate of the US Naval Academy, US Naval War College, Marine Corps War College, and MIT Seminar XXI Fellowship Program.

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, US–China and US-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 project.

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.

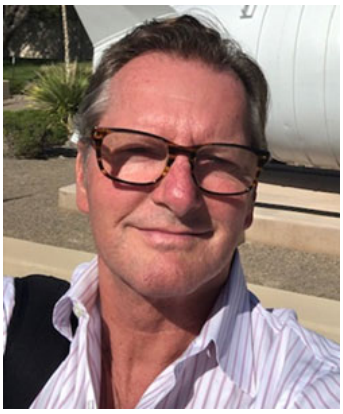
Mr. Michael A. Clark

Michael Clark, a member of the Senior Executive Service, serves as the US 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.

Dr. Zachary S. Davis

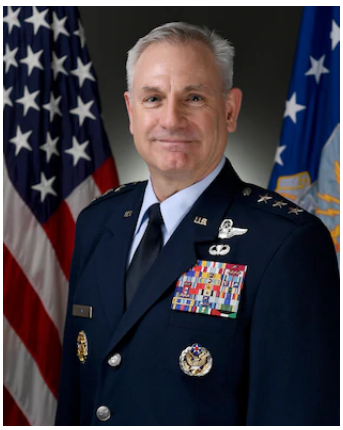


Dr. Zachary S. Davis is a Senior Fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory and a Research Professor at the Naval Postgraduate School in Monterey, California, where he teaches courses on counterproliferation. He has broad experience in intelligence and national security policy and has held senior positions in the executive and legislative branches of the US government. His regional focus is South Asia.

Davis began his career at the Congressional Research Service at the Library of Congress and has served with the State Department, Congressional committees, and the National Security Council. Davis was group leader for proliferation networks in LLNL's Z Program, and in 2007 he was Senior Advisor at the National Counter Proliferation Center in the Office of the Director of National Intelligence. He is the author of numerous government studies and reports on technical and regional proliferation issues. He currently leads a project on the national security implications of advanced technologies, focusing on special operations forces.

Davis's scholarly publications include articles in *Orbis*, *Asian Survey*, *Arms Control Today*, *Security Studies*, *The American Interest*, and chapters in numerous edited volumes. He was editor of the widely read 1993 book *The Proliferation Puzzle: Why States Proliferate and What Results*. His edited book on the 2002 South Asia crisis, *The India-Pakistan Military Standoff*, was published by Palgrave Macmillan. He is the editor of several recent books on emerging technology: *Strategic Latency and World Power: How Technology is Changing our Concepts of Security*, *Strategic Latency Red, White and Blue: Managing the National and International Security Consequences of Disruptive Technologies*; and *Strategic Latency Unleashed: Emerging Technology for Special Operations Forces*. Davis holds a doctorate and master's in international relations from the University of Virginia and an undergraduate degree in politics from the University of California at Santa Cruz.

Lieutenant General (Ret.) Timothy G. Fay

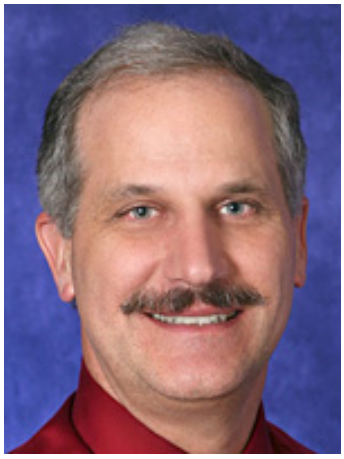


Lt. Gen. (Ret) Fay was commissioned following his graduation from the US Air Force Academy in 1987. His final assignment was as Director of Staff, Headquarters Air Force, the Pentagon, Arlington, Virginia. In this role, he synchronized and integrated policy, plans, positions, procedures, and cross functional issues for the headquarters staff.

His previous assignments include instructor pilot and weapons officer duties in the B-52 Stratofortress and B-2 Spirit, as well as staff service at Headquarters, US Strategic Command, US Forces

Iraq, Joint Staff and the Air Staff. He served in operations Desert Storm, Allied Force and Iraqi Freedom; commanded at the squadron, group and wing level; and is a command pilot with more than 3,900 flight hours. In his previous assignment, he served as the Deputy Chief of Staff for Strategy, Integration, and Requirements, Headquarters US Air Force, the Pentagon, Arlington, Virginia.

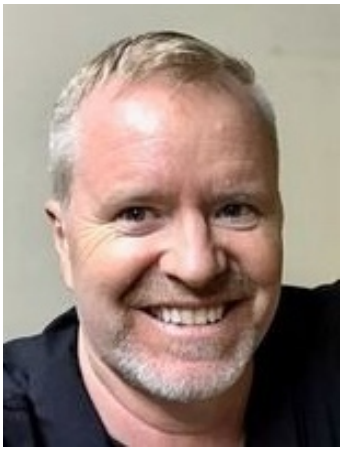
Mr. James M. Jenista



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 plankowner 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 US Army Special Forces Colonel, a former Deputy District Attorney, and the senior strategist at US 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. Jimmy Krakar

Jimmy Krakar is the United States European Command Academic Coordinator, in which role he coordinates with military and civilian academia to support the command. Previously, he worked at the TRADOC G-27 Models and Simulations Branch (M&SB) at Fort Leavenworth, where for over seven years he participated in numerous Operational Environment analytical efforts in support of Department of Defense clients, serving as the Team leader and lead analyst for the M&SB efforts which provided on-site support to SOCCENT and CJTF-OIR. Before that he worked as a Counterinsurgency Advisor for the COMISAF Advisory Assistance Team (CAAT) in Afghanistan.

Militarily, Jimmy retired from USSOCOM J-8, which he supported as an Army Reservist. He had over 25 years of active and reserve military experience in Infantry, Civil Affairs, and Human Terrain operations, with deployments to Somalia, Iraq, and Afghanistan. Prior to this job, his most recent European experience was at NATO Special Operations Headquarters (NSHQ), where he served as a Plans Officer.

Jimmy received his BS in Military History from the United States Military Academy and an MS in Intelligence from American Military University, and he graduated the Defense Language Institute as a basic Arabic Linguist. His most recent periodical publication was "The Civil Engagement Spectrum: A tool for the Human Domain," published in the Sep/Oct 15 issue of *Military Review*.

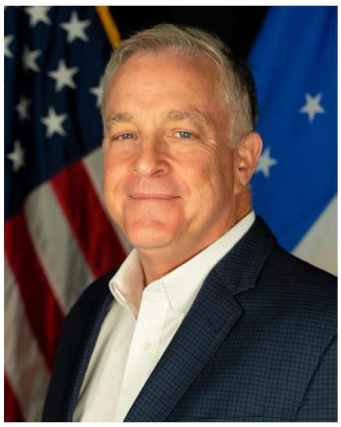
Ms. Lesley Kucharski

Lesley Kucharski is an analyst at Lawrence Livermore National Laboratory, where her research focuses on the role of information confrontation [*informatsionnoe protivoborstvo*] in Russia's approach to multi-domain deterrence and strategic competition, with an emphasis on the nexus between the information and nuclear domains. She is a Russian linguist and has worked on nuclear policy issues at NATO and the United Nations. Kucharski holds master's degrees in nonproliferation and terrorism studies from the Middlebury Institute of International Studies at Monterey and in Russian language from Middlebury College, and a bachelor's degree in Russian studies and economics from the University of Michigan.

Ms. Julie McNally

Julie McNally is a Senior Deterrence Analyst at USSTRATCOM and oversees research for the command's Analytic Agenda. She holds an MS in International Security and an MS in Project Management from Bellevue University and a BA in English from University of Iowa.

Mr. William J.A. (Joe) Miller



Joe Miller is Director of Joint Training, Exercises, andWargaming for North American Aerospace Defense Command and United States Northern Command, Peterson Space Force Base, Colorado Springs, CO. He is responsible for all Joint Training, Education, Exercises, and Wargames for both Commands and their respective Regions, Components, and Subordinate Commands. He leads approximately 170 personnel in seven Divisions covering: Campaigns, Integration, Assessments, and Futures; Joint Exercises; Joint Training and Education; Qualification Training; Joint Resources and Readiness; Assessor Authority Training; Joint Wargaming; and Innovation.

A Business Administration graduate of the University of Florida, Joe served on active duty in the Army for 26 years, leading and commanding soldiers from platoon to Brigade Task Force in Germany, Texas, Kosovo, Colorado, Afghanistan, and Iraq, with intermediate stops at Ft Knox, Ft Benning, the Air Force Institute of Technology (AFIT), Ft Leavenworth, the Pentagon, USCENTCOM, and as Chief Operating Officer at MSCubed in Tampa, FL prior to his assignment as J5 Director of Plans at USSOCOM. He has Master's Degrees in Operations Research from AFIT and from the School of Advanced Military Studies (SAMS) at Ft Leavenworth, KS, and he has completed postgraduate coursework in Executive Education at the JFK School at Harvard University, MA. He is a Life Member of the Council on Foreign Relations and is an Adjunct Research Fellow at Columbia University, NY.

Ms. Christina L. Peters

Ms. Christina Peters is a former Marine Corps Public Affairs officer. She is currently a communication strategist assigned to US Central Command's Strategy, Plans, and Policy Directorate (CCJ5). She develops strategic-level communication products for USCENTCOM leadership. Ms. Peters is a graduate of the US Naval Academy and holds a Master's Degree in Forensic Psychology with a focus on violent criminal/terrorist behavior.

Lt. Col. Jean Purgason

Lt. Col. Jean Purgason is the Speechwriter and Special Assistant to the Deputy Commander, United States Space Command, Peterson Space Force Base, Colorado. As a member of the Commander's Action Group, he develops speeches, publications, and talking points for use by the Deputy Commander during key leader engagements. He executes special projects at the direction of the Commander, Deputy Commander, and Command Senior Enlisted Leader.

A career space officer with 15 years of Air Force and Space Force experience, Lt Col Purgason's operational assignments include Intercontinental Ballistic Missiles, Spacelift, and Space-based Missile Warning units. Prior to his current assignment, Lt. Col. Purgason was assigned to United

States Space Command as a Joint Planning Group lead in the J3 Future Operations Division, responsible for command-wide campaign and contingency operations planning.

Lt. Col. Purgason is a graduate of the School of Advanced Air & Space Studies, with additional degrees from Air University, Central Michigan University, and the University of North Texas.

Col. (Ret.) André Shappell

Col. (Ret.) André Shappell is the Chief Strategist and Senior Advisor, Commander's Action Group, Headquarters United States Space Command, Peterson Space Force Base, Colorado. He develops the Commanders' strategic intent documents and narratives; researches and crafts strategic messaging to include speeches, briefings, messages to the force, and articles for publication; and executes special projects at the direction of the Commander, Deputy Commander, and Command Senior Enlisted Leader.

A career Intercontinental Ballistic Missile launch officer, André commanded an ICBM Squadron, an ICBM Operations Group, and held various staff positions on the Joint Staff and at the Major Command level. A master ICBM launch officer, and master space operator, André served as Air Force Space Command's Chief, Launch, Range and Networks Division, and as the Deputy Director, Air, Space and Cyber Operations Directorate. He retired from active duty in 2011.

André is a graduate of Harvard University's National Security Fellows program, with additional degrees from Air University, the University of Colorado, and the University of Washington. Prior to joining the Commander's Action Group at Headquarters United States Space Command, André was a Program Manager and Director, Business Development in the LinQuest, Exelis, and Vectrus corporations.

Dr. Robert M. Toguchi

Dr. Robert M. Toguchi is currently serving as the Chief, Concepts Division, Force Modernization Directorate (FMD), in the US Army Special Operations Command at Fort Bragg, North Carolina since 2013. He has spent over 30 years on active military duty while serving as a Functional Area 59 strategist for the US Army. His past assignments included a tour as the Director, Strategic Plans and Chief, ARCIC Initiatives Group, TRADOC. In the Pacific region, he spent a tour with the US Pacific Command while serving as the Deputy Director, J8 and the Chief, Strategic Plans, J5 Directorate. Dr. Toguchi was also assigned to Africa in 2005 while serving as the senior US military observer to the U.N. Mission in Liberia. Previously, he served on the faculty and taught military strategy at the US National War College, National Defense University. Additionally, in the Washington D.C. area, Dr. Toguchi gained valuable experiences within the halls of the Pentagon while serving as a strategist in the DAMO-SSP, Strategy and Policy Division, Army G3/5/7 and as a war planner in DAMO-SSW, War Plans Division, Army G3/5/7, 1996-1999. Dr. Toguchi received a B.S. degree from the US Military Academy in 1980 and received a PhD in History from Duke University in 1994.

Dr. Robert Toguchi's book publications include: *The Competitive Advantage: Special Operations Forces in Large Scale Combat Operations*, Army University Press, and *Land Warfare in the Information Age*, Institute of Land Warfare. His previous co-authored article publications include: "The Battle of Convergence" in *Military Review*; "Unveiling the Army's Capstone Concept" in *Small Wars Journal*; "Achieving Excellence in Small Unit Performance" in *Military Review*; "The Future of Army Ground Forces" in *Small Wars Journal* and "Predicting Futures Military Threats*:* Implications of the Black Swan" in *The National Interest*.

Major Trisha E. Wyman

Maj. Trisha E. Wyman is a professional psychological operations (PSYOP) officer in the US Army at Fort Bragg, North Carolina. Throughout her career, Maj. Wyman has deployed to Paraguay, Afghanistan, Qatar, and other locations to conduct PSYOP and special operations with interagency and host nations. She has been assigned to the 1st PSYOP Battalion, 82nd Airborne Division, 8th PSYOP Battalion, 4th PSYOP Group (4th POG), US Special Operations Central Command (SOCCENT), Defense Intelligence Agency (DIA), and the US Army John F. Kennedy Special Warfare Center and School (SWCS). Maj. Wyman holds master's degrees in science in information strategy and political warfare from the Naval Postgraduate School and professional studies in security and safety leadership from the George Washington University, and a bachelor's degree in global studies with a concentration in political science from Methodist University.

Strategic Multilayer Assessment

Joint Staff, Deputy Director of Global Operations (DDGO)

Established in 2000, Strategic Multilayer Assessment (SMA) provides planning and decision support to combatant commands and other US government (USG) departments and agencies.

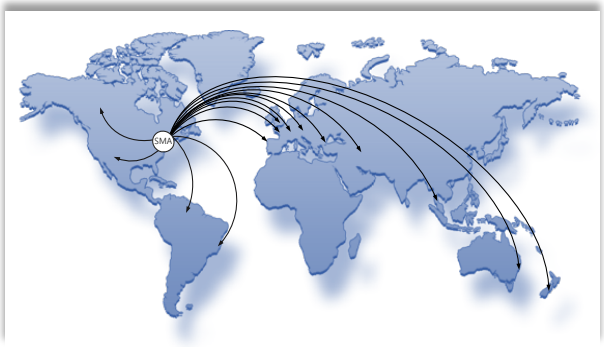
SMA's mission is to enable decision makers to develop more cogent and effective strategy and doctrine, bridging the gap between the academic research community and operators and planners.

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 US 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, US 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, J39, SMA (mariah.c.yager.ctr@mail.mil).