August 31, 2021

Proceedings for
the G-2 TRADOC 2021

"Role of America's Army in National Defense, 2021-2030"

Campaign of Learning

Deputy Chief of Staff G-2, United States Army Training and Doctrine Command

Authors:

Dr. Russell W. Glenn

Dr. Mica J. Hall

Ian M. Sullivan

Thomas E. Switajewski, Jr.

Lee K. Grubbs

with Dr. Jacob E. Barton

TRADOC Deputy Chief of Staff, G-2: 1-757-501-6236 Email: usarmy.jble.tradoc.list.hq-tradoc-g-2-ops@mail.mil

TABLE OF CONTENTS

FOREWORD

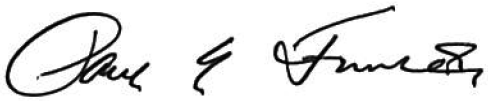
Commanding General, US Army Training and Doctrine Command, General Paul Funk II

"Is Ours a Nation at War" challenges our accepted way of thinking about war. A year ago, I directed TRADOC to look at how the operational environment was being affected by COVID-19 and recent adversary initiatives. The following builds on that work. It questions basic assumptions. It identifies national security vulnerabilities. And it provides new, innovative, and exciting recommendations by great Americans from throughout our society.

America's adversaries recognize and respect its impressive battlefield capabilities. They don't want to confront us, at least not yet. How does our Army meet the challenges posed by adversaries who seek to sidestep US battlefield advantages while pursuing their national security objectives during the period 2021-2030? The TRADOCG-2 developed a campaign of learning spanning five months, one drawing on expert opinion from the military, intelligence, rest of government, academic, and industry communities to find answers and provide counsel. These fresh thinkers—young and old, serving and retired—gave their valuable time to provide recommendations not only to the Army, not only to our military, but to all in government and beyond.

We are a threat-based Army. US Army TRADOC focuses on training that Army for war. We have traditionally considered our soldiers and leaders our asymmetric advantage. But what if adversaries are already competing with us in ways that seek to avoid our battlefield capabilities? What if foes look at war in ways we do not?

Our people will remain the key to meeting new challenges. For the Army, that means developing ethical leaders and training in realistic and innovative ways to ensure we stand ready to defend the United States no matter the nature of the threat: cyber, informational, technological, or otherwise, on the battlefield or off. We ready ourselves to be the best combat force in the world. That is a necessary condition. Insights from the campaign of learning tell us that America's Army also needs to look beyond the battlefield. While it must not lose its ability to fight and win, it must be able to compete and persevere in other ways as well. It must do so hand-in-hand with our joint, interagency, multinational, industry, and other partners. The pages below provide a look at new types of threats, what to do about them, and how to do it. We thank those who joined TRADOC in discussing these problems as they offered us their best thinking—thinking that reaches beyond this command and our Army. I encourage you to join us in continuing to ready our country to meet whatever faces us in the decades ahead.



Paul E. Funk II
General, US Army
Commanding

CHAPTER 1

The Campaign of Learning – Overview

If I were to fault the process [of planning the effort in Afghanistan], I would say that vastly more attention was focused on every aspect of the military effort than on the broad challenge of getting the political and civilian part of the equation right. Too little attention was paid to the shortage of civilian advisers and experts: to determining how many people with the right skills were needed, to finding such people, and to addressing the imbalance between the number of US civilians in Kabul and elsewhere in the country.[1]

Robert Gates, US Secretary of Defense, 2014

These proceedings summarize the insights and recommendations from a series of events that together comprise the G-2 US Army Training and Doctrine Command (TRADOC) 2021 Campaign of Learning. Individuals from across the US civilian and military communities were asked to consider the roles of the US Army during the period 2021-2030 in light of changes in the operational environment (OE), in particular the changing character of warfare and evolving threats. The overarching objective of the 2021 Campaign of Learning was to

> **capitalize on the expertise and experiences of a select group of individuals to better understand how the US Army—and by extension the nation's collective armed services and government—can meet the challenges posed by adversaries seeking to neutralize America's battlefield advantages via in part or completely avoiding those capabilities in pursuit of their national security objectives.**

Three primary questions drove pursuit of the above objective:

- How should the US Army's roles and capabilities change to meet challenges when key adversaries seek to "win without fighting" during periods of competition and crisis?
- How should US Army roles and competences be adapted for contingencies when key adversaries neutralize many of its armed conflict capabilities through their use of stand-off assets, cyberattack, information operations, human performance engineering, and other disruptive approaches that (1) separate the US from its allies, partners, and other elements of the joint force, and (2) otherwise neutralize Army ground combat proficiency?
- How must the Army adapt to an operational environment (OE) in which its adversaries will likely have rough parity in terms of materiel and can challenge the service across the DOTMLPF-P spectrum, particularly in terms of human capital (leader development, training, and education)?[2]

Many have long assumed that the US Army is the best equipped in the world, that its soldiers are the best trained and led, and that the service's ability to conduct maneuver warfare is unmatched. True or not, near-peer threat militaries continue to enhance their ground force proficiency via improved recruiting, training, leader development, and otherwise. There is no reason to assume they will not continue to do so during the period of consideration. We cannot assume continued US Army superiority in all critical areas. Competition with our great power rivals will expand and compel the US Army to work, innovate, and invest in maintaining its edge, particularly in people and our approaches to warfare.

[1] Alan Ryan, "Civil and humanitarian assistance," in *Niche Wars: Australia in Afghanistan and Iraq, 2001-2014,* ed. John Blaxland, et al., Acton, Australia: Australian National University Press, 2020, 187, as appears in Robert M. Gates, *Duty: Memoirs of a Secretary at War, NY: Knopf, 2014, 270-71.*

[2] Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy

CONTEXT

This document is not a "future nature of warfare," Multi-Domain Operations (MDO), or technology-oriented analysis (though its contents have application to all three). When one or more of this trio appears in the following pages, they do so as part of a broader analysis, one with a primary focus on other-than-technological solutions. The concern is not whether the Army should maintain its mission as currently stated ("to deploy, fight, and win our nation's wars by providing ready, prompt, and sustained land dominance by Army forces across the full spectrum of conflict as part of the joint force").[3] That the service must remain proficient in this regard is a given. The assumption underlying the Campaign of Learning was that battlefield dominance is a necessary but no longer sufficient condition given an environment in which threats recognize US Army dominance and seek to avoid combat while otherwise undermining the country's national security.

Writing in his *Deciding What Has to Be Done: General William E. DePuy and the 1976 Edition of FM 100-5, Operations,* Paul H. Herbert observed:

> **[An] important characteristic of the early 1970s that influenced the Army's doctrine was the condition of the US Army immediately after Vietnam. Neither defeated nor victorious in that war; misunderstood and unappreciated at home; rent by racial, drug, and disciplinary problems; short of experienced leaders; and in the throes of major personnel policy changes associated with the end of conscription, the Army, like its sister services, was not combat ready.[4]**

The progression of the Army from its post-WWII Cold War hunt for a *raison d'être* in light of nuclear weapons; through innovations during Vietnam and post-Vietnam soul searching; while fielding AirLand Battle doctrine; and nearly twenty years of conflict in Iraq and Afghanistan includes what might be considered two renaissances. The first successfully answered the question "What is the US Army's role in a nuclear world?" The second (post-Vietnam) demonstrated the feasibility of completing an effective transition in a dramatically short period of time, that from the difficult years following the conflict in Southeast Asia to stunning battlefield victory in the 1991 Persian Gulf War. Now, post-Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF), our country's primary ground force finds itself confronting an operational environment in some ways similar to—yet in others significantly different from—the two periods preceding these revitalizations. For the first time in history, the United States and its Army have to evolve from status as world hegemon to security guarantor under conditions of increasing multi-polarity and contestation in several realms—military, economic, informational, and ideological among them. Asymmetry in equipment, maneuver capability, and quality of leaders and led may still suffice against lesser adversaries.

In contrast, asymmetry more generally—in some or all of the realms of sub-threshold maneuver[5]—arguably favors America's foes and will do so to an increasing extent unless the US radically changes its approach to war and conflict in general. Regardless of whether one accepts the above presumptions regarding US Army superiorities, they are no longer sufficient to ensure the United States avoids defeat in contests with near-peer or peer competitors.

China, Russia, and select other threat entities are actively avoiding US and its partners' military capabilities. Theirs is an indirect approach, one that British interwar military theorist Basil Liddell Hart would have recognized. But while Liddell Hart conceived of avoiding an enemy's strength in terms of the physical location of an adversary's force, our foes today see it as incorporating maneuver in all relevant spheres: military when necessary, but primarily those diplomatic, informational, economic, social, and otherwise as niches, opportunities, and vulnerabilities present themselves. This should not surprise. It is a fair argument that America's Strategic Defense Initiative (popularly referred to as "Star Wars") was primarily an economic approach that helped in spending the Soviet Union into oblivion. Russia learned. Its economy cannot afford an armed forces capable of directly contesting battlefields against the United States. The country's current leaders therefore choose to invest in other means as combat multipliers or to support of operations below the threshold of armed conflict. China competes similarly, although due its more favorable economic condition, it also is transforming the People's Liberation Army into a force capable of waging what it terms "intelligentized" warfare.

---

[3] "Who We Are: The Army's Vision and Strategy," US Army webpage, https://www.army.mil/about/ (accessed June 29, 2021).

[4] Paul H. Herbert, *Deciding What Has to Be Done: General William E. DePuy and the 1976 Edition of Field Manual (FM) 100-5,* Operations, Leavenworth Paper number 16, Fort Leavenworth, KS: Combat Studies Institute, 1988, 101.

[5] "Sub-threshold maneuver" in the context of this paper refers to the employment of relevant resources to gain advantage with respect to select individuals or groups to achieve specified objectives while not triggering an unacceptable response by one or more adversaries. Such maneuver may include use of military capabilities. An example of successful sub-threshold maneuver is Russia's seizure of eastern Ukraine and Crimea while remaining below the North Atlantic Treaty Organization (NATO) threshold for an armed response. For more on this concept, see Russell W. Glenn, "The Indirect Approach Lives!...in China and Russia: Sub-threshold Maneuver and the Flanking of US National Security." The complete article is accessible via a link at the end of Mad Scientist blog #301, February 1, 2021, https://madsciblog.tradoc.army.mil/301-sub-threshold-maneuver-and-the-flanking-of-u-s-national-security/

Building a world-class military is expensive. It is also a long-term undertaking involving confrontation in terms of technology, manpower quality, leader development, training, education, logistics, and other components that only collectively and symbiotically constitute a successful warfighting force. Developing these components and molding them into an effective force requires years, often decades. For China, choosing to also compete in arenas other than the physical battlefield may therefore be a matter of buying time in addition to taking advantage of whatever economies an indirect approach provides. Time could prove that progress in non-military areas renders battlefield superiority unnecessary. Achieving national objectives without having to directly confront the United States in armed conflict would constitute the acme of skill.

CAMPAIGN OF LEARNING STRUCTURE

The 2021 Campaign of Learning included webinars and roundtables featuring subject matter experts, blog entries, an essay competition, a fireside chat with TRADOC's commanding general, the release of several articles by TRADOC G-2 authors, and a Young Minds on Competition and Conflict panel. The culminating event was a VIP expert panel in which the following individuals participated:

- General (US Army, retired) Keith B. Alexander, former Commanding General (CG), Cyber Command and Director, National Security Agency (NSA)
- Dr. James Canton, Chief Executive Officer and Chairman, Institute for Global Futures
- Lieutenant General (US Marine Corps) Dennis Crall, US Joint Staff J6
- The Honorable Michèle A. Flournoy, Founder of the Center for New American Security (CNAS) and former Under Secretary of Defense for Policy
- Lieutenant General (US Army, retired) Paul E. Funk, former CG, III Corps
- Vice Admiral (US Navy, retired) Robert S. Harward, former Deputy Commander, US Central Command
- General (US Air Force, retired) James M. Holmes, former CG, Air Combat Command
- John M. Pulju, Acting Chairman, National Intelligence Council, Office of the Director of National Intelligence
- Lieutenant General (US Marine Corps, retired) Paul Van Riper, former CG, USMC Combat Developments Command

The following chapter provides Campaign of Learning insights and recommendations offered by its participants. Participant lists and other additional details regarding 2021 Campaign of Learning components other than the VIP panel appear in Appendix 1. Appendix 2 is a compilation of participant and select previous G2 TRADOC intelligence/threat observations. It should be read as a precursor to chapter 2 by those wanting additional context for that chapter's material. Appendix 3 presents a concise summary of Campaign of Learning recommendations. VIP panelist biographical sketches and a glossary appear in Appendices 4 and 5 respectively.

CHAPTER 2

Is Ours a Nation at War? US National Security in an Evolved—and Evolving—Operational Environment

INTRODUCTION

We are in the interwar years – we need to take an integrated DOTMLPF-P approach to prepare for what's coming. We can no longer rely on having the best soldiers. China and Russia are changing from conscription-based armies to more professionalized armies and they are starting to copy us and train like we train. We have to think about how we stay ready below the threshold of armed conflict and stay ready to compete across the world.[6]

General Paul E. Funk II, Commanding General, US Army Training and Doctrine Command

The US Army and its partners confront an operational environment in which select state threats work to perfect ways of achieving national objectives without having to engage the United States in armed conflict. Yet at the same time, economic and other ties with these threats vary from virtually nonexistent to extensive. US leaders must incorporate these interdependencies into any strategies, recognizing both inherent opportunities and challenges. The operational environment is made the more complex as diplomatic, economic, and cultural tools find company in new, potentially existential threats as addressed in the opening chapter, heretofore unseen avenues for psychological manipulation of populations among them. This state of affairs has a complement in which nonstate actors and states with less robust economies can access capabilities previously reserved for heartier national budgets and development processes.

Countering this multitude of threat types is tougher for the US than for our adversaries who frequently have the advantage of being able to focus on a single, primary foe: us. Expert panel member John Pulju compared the current period to that in the aftermath of World War II (WWII) during which the emergence of a new strategic challenge—strategic nuclear weapons—did not obviate the requirement to be vigilant and capable in the conventional warfare arena. The struggle to find an effective yet affordable deterrence to those weapons was characterized by vigorous debate, trial and error, inter-service (and at time intra-service) tensions, and the building of some of history's strongest and longest-lasting alliances.

The United States found itself the world's hegemon when the Cold War ended. That status was of short duration yet one sufficiently long for many to conclude that ours is a force undefeatable on the battlefield. Several expert panel members and other participants in the Campaign of Learning find such a conclusion smacks of hubris. One likened the situation to that of once market leaders like Polaroid and US automobile manufacturers in the commercial world. But the challenge is tougher yet for the US. Unlike in those years immediately following WWII, the United States did not initially dominate in fields of emerging consequence. These are contested spaces, ones in which adversaries sometimes lead and are already refining their capabilities by testing them in locations such as Ukraine, India, and the Baltic states. China, Russia, and other parties constantly exercise information operations to undermine the appeal of democracy generally and that in the US in particular, portraying us as a nation whose social, political, and economic divisions are proof of democracy's inherent weakness as a form of government.

[6] GEN Paul Funk II remarks during US Army TRADOC virtual VIP panel, May 12, 2021.

Recent cyberattacks such as those perpetrated through SolarWinds and against the Colonial Pipeline demonstrate a willingness to employ these capabilities either directly, via surrogates, or through benign tolerance of criminal elements (who could be viewed as another form of surrogate). They represent a fundamental difference from the threats posed during the Cold War. Attacks with nuclear weapons were not a viable option. Complete defense should one side have decided to use these weapons was virtually impossible; even partial failure would have meant devastating results for all adversaries. Deterrence was the only viable option. Conditions are far different today. While complete defense against cyber and information attacks is impossible now as it was then, effective forms of deterrence remain elusive. The consequences of future assaults will sometimes be less obvious than those seen thus far. Affected computer algorithms may result in friendly forces receiving wrong or misguiding information or weapons striking incorrect targets for seemingly inexplicable reasons. The immediate battlefield effects might be significant; the longer-lasting undermining of trust in warfighting systems could be paralyzing. Unlike with nuclear weapons, such characteristics make their use attractive rather than unthinkable.

These evolutions are changing the nature of warfare. With notable exceptions, most English definitions for "war" require opposing sides to engage in armed conflict. Even that seemingly sharp delineation permits considerable gray area both in terms of legal definitions (Was the 1950-1953 conflict in Korea a war or a police action?) and broader understanding. What of the operational environment today? Lieutenant General (LtGen) Dennis A. Crall proposed that our understanding of what constitutes warfare should be considerably broader than that traditionally accepted:

Fighting looks different today. It disarms people when they think that somehow it's not a fight. Many of the briefs that I've seen in the Pentagon start with this idea that we push our adversary into the competition space to avoid conflict. We don't need to push them there; that is exactly the space they want to be in.... They routinely rob our defense industrial base. They cut off years of research and development and save billions of dollars in technology development and fees. They have unprecedented access into our infrastructure. Why would they possibly want to change? I equate this to sending my kids to their room when they were younger. That's where they wanted to be! That's where all their stuff was. Our adversary seems to be operating in that space and we consider that not warfighting. We need to recognize that it is warfighting. It's not the fight that's coming; it's the fight we're already in.

Adversaries maneuvering in these other-than-combat realms means wars "will be sneakier," in the words of one speaker during the Campaign of Learning's first webinar. Deniability could be more valuable than firepower even as much of this maneuvering below the threshold of armed conflict is evident to all. China's aggressive promotion of its national interests via the Belt and Road Initiative (BRI) demonstrates adroitness in this regard—creative use of lending that sidesteps internationally accepted practices, imposing debt that hamstrings any successor government's efforts to undo unfavorable agreements put in place by its predecessor, employment information campaigns exaggerating benefits while ignoring obvious shortfalls of such commercial agreements—these comprise but a miniscule sample of past and ongoing practices.

Russia's seizure of Crimea and other portions of eastern Ukraine is a sterling exemplar of maneuver below a threshold that precipitates armed response. Use of surrogate militias, deception operations, and forms of attack for which NATO was largely unprepared (e.g., cyberattacks and economic coercion) left Russia threatened only with sanctions and diplomatic pressure deemed acceptable for the objectives achieved. There is good reason to believe that they will observe, learn, and adapt their approaches for using this broader understanding of warfare. Author David Kilcullen believes such could be the case with biological warfare. Having seen the effects of COVID-19 on US Navy ship crews, it is logical to conclude that the attractiveness of employing biological agents against such "captive" targets has been noted for possible future use.[7] The debates surrounding the source of COVID-19 demonstrate how difficult it could be to definitively identify a perpetrator much less cultivate the domestic and international support needed to employ armed force in response. That such attacks could cripple vital capabilities while remaining largely or entirely nonlethal would further promote a reaction remaining below the threshold of armed response.

[7] David Kilcullen, "The Convergence: Hybrid Threats and Liminal Warfare with Dr. David Kilcullen" podcast, January 21, 2021, https://episodes.castos.com/5e1729439f1d05-67192808/KilcullenFinal.mp3 (accessed February 16, 2021).

US VULNERABILITIES

Adversaries are using cyberattacks as an element of national power. Cyber is an existential economic and military threat. These attacks continue to grow in sophistication, size, and number and are emerging as the biggest crisis of our time.

General (Ret.) Keith B. Alexander

Every time we win, our adversaries are learning.

LTG (USA, ret.) Paul E. Funk

Military transformations for potential future conflicts simply do not occur during long periods of military conflict.[8]

Robert O. Work, "AI and Future Warfare: The Rise of Robotic Combat Operations"

[8] Robert O. Work, "AI and Future Warfare: The Rise of Robotic Combat Operations," presentation in support of Mad Scientist Disruption & the FOE-AI & Future Warfare conference, slide 7, April 24, 2019, https://community.apan.org/wg/tradoc-g2/mad-scientist/m/disruption-and-the-future-operational-environment/274690 (accessed May 27, 2021). FOE-AI is "Future Operational Environment-Artificial Intelligence."

INTRODUCTION

Discussion of US vulnerabilities arose throughout the 2021 Campaign of Learning. Largely focused on existing threats for much of the Global War on Terror—primarily those posed by improvised explosive devices (IEDs)—and committed financially to the conduct and recovery from wars in Afghanistan and Iraq, the United States found that by the middle of the 21st century's second decade adversaries exceeded US capabilities in several critical areas. This brief section does not attempt to exhaustively identify all such vulnerabilities, instead presenting only those mentioned by participants during the Campaign of Learning.

The cyberattack on the Colonial Pipeline took place just prior to the VIP panel's May 12, 2021 meeting. The immediacy of its impact and extent of potential crisis quickly faded from public view given the quick payment of ransom and "feel good" response on hearing that a portion of the money paid was recovered. A subsequent attack against the nation's food supply (in this case its meat industry) held attention for only a few days. General Alexander, Michèle Flournoy, and others expressed concern regarding both the scope of such attacks and apparent tactics backing them. Alexander cited the 18,000 companies impacted by the SolarWinds attack in addition to nine federal agencies that were affected and a subsequent incident affecting at least 30,000 companies via a hack of Microsoft exchange servers. "If those had been destructive attacks that had crippled those companies and government agencies," the former head of Cyber Command noted, "our nation would be in a depression, and everybody would be looking to the Defense Department and services for what they did or did not do."

These attacks' frequency and impact are both on the rise. Future targets (or past targets where the consequences may not have yet taken effect) will likely include American and partner weapons systems and other vital components of national defense. The extent of vulnerabilities increase with the proliferation of commercial and government systems taking advantage of the Internet of Things (IoT) that provides additional inroads for incursion. One example is the vulnerability of supply chains as unmanned aerial delivery systems and self-driven ground vehicles become ubiquitous. The effectiveness of these attacks comes relatively cheaply given China's theft of some $5 trillion in US intellectual property over the past decade.
General Alexander wrapped up his summary of concerns by noting, "We aren't even playing in the recon[naissance] battle in cyber." The difficulty of responding effectively to these challenges is greater given the lack of response options short of armed force. Adversaries' non-kinetic strikes fail to breach traditional thresholds for war even while possessing the previously suggested devastating potential for targeted economies, national security, government legitimacy, and the daily lives of citizens.

In addition to these concerns—ones the US has yet to fully recognize much less effectively respond to—maturing threats highlight other vulnerabilities. Fixation on the South China Sea, Taiwan, and North Korea detracts from understanding, analyzing, and funding responses to possibly greater dangers. Ms. Flournoy recognized the importance of the above trio but suggested the Army's relevance to both those and broader Pacific security challenges is under explored. Foes in that theater and elsewhere seek asymmetric advantages while avoiding our technological leads. Vast distances mean long lines of Pacific supply will be particularly vulnerable to interruption physically or via cyberattacks and diminished support for US actions thanks to adversaries' information campaigns. The consequences will be even more difficult to remedy given the likelihood that US forces will fight in command and control dusk if not dark thanks to threat-induced interruptions. Regional allies and partners will be fundamental to overcoming these obstacles, Ms. Flournoy noted, a situation requiring a broader strategic approach to security cooperation than has previously been the case. That this is particularly important in eastern Asia and the Indo-Pacific generally is consequent of many militaries in the region being land-force centric. Military-to-military ties based on army-to-army relationships and basing agreements are crucial; both should include existing relationships and others new.

Lack of a systematic approach to addressing specific logistics, command and control, and cyber issues compounds these vulnerabilities. LtGen Dennis Crall cited lack of joint training and general readiness in the information operations realm. The same is true of cyber. Author and analyst Dr. David Kilcullen observed that such challenges do not occur in isolation.[9] Readiness is a collective function. The National Intelligence Council's John Pulju provided the example of possible future cyberattacks that devastate the US economy, observing that such would themselves not mean the end of a war. How, he asked, would the US respond given that economic strikes represent only one of many threat types? LtGen Crall perceives the problem partly in terms of failing to consider all relevant perspectives. "I really haven't found many who understand [the potential for us to employ this broad spectrum of capabilities]," he observed, "but we recognize it when others do it to us." The implied question was clear: How can the US and its partners achieve their desired ends while experiencing asymmetric attacks as Ms. Flournoy predicts?

[9] David Kilcullen, "The Convergence: Hybrid Threats and Liminal Warfare with Dr. David Kilcullen" podcast, January 21, 2021, https://episodes.castos.com/5e1729439f1d05-67192808/KilcullenFinal.mp3 (accessed February 16, 2021)."

DOTMLPF-SPECIFIC VULNERABILITIES

I believe that by embracing a Future Ready posture, the US Army will successfully meet the challenges of countering threats to US global hegemony given the growing real-time and advancing hostility demonstrated by our near-peer adversaries. This is a whole-systems calculus. We need adversarial threats and existential peril to reinforce our pivot to becoming innovation warriors.

Dr. James Canton

The demarcation between an act of war and failing to breach that threshold is seldom a crisp one. The nature of an action itself is only part of the determination. Politics, perspectives, and previous frictions are among the factors that will lead some to believe a trespass has occurred even as others remain unconvinced. While several VIP panel members strongly supported a conclusion that the United States is already experiencing an evolved form of warfare, one in which armed conflict plays at most a supporting role, one panelist expressed concerns that broadening the understanding would allow what would otherwise be essential participants to avoid commitments with the excuse that "if it's war, it is the responsibility of the military." The determination becomes even more complicated when no act of armed aggression has taken place or, as in Crimea and Ukraine, use of force is sufficiently constrained or initially difficult to attribute.

Addressing one aspect of these threats, General Alexander observed, "The Digital Arms Race will be the greatest crisis of our time. Adversaries are going to come after our C2 [command and control]. They're going to use disinformation. We need to create a way for the public and private sectors to work together in cybersecurity." Yet when asked "What constitutes a digital/cyber act of war?" Acting Secretary of the Army John E. Whitley replied,

> **That's one of the hardest questions we are facing…. I do not know the answer…. We are under attack in ways that if they were kinetic, they'd be considered pretty significant. They are very significant in the cyber domain…. How do we characterize those? How do we describe those to the public? What types of reactions/counters are justified given the level of those attacks? We are trying to figure out what we can do…that's appropriate and consistent with our values, promotes long term peace, [and] doesn't end up doing more harm than good.[10]**

[10] John E. Whitley, "Advancing Army priorities for the future of warfare: A conversation with the Acting Secretary and the Chief of Staff of the Army" interview, Atlantic Council, May 10, 2021.

Neither current joint nor Army **doctrine** includes definitions of "war" or "warfare." The armed services and joint communities by default instead retain traditional and common-use understandings akin to war being "a state of armed conflict between countries or within a state."[11] This understanding denies cyberattacks, information incursions, economic manipulation, and other actions currently employed by multiple countries against the United States a status as acts of war despite their increasingly being directed against the US homeland and eroding US national security objectives domestically and abroad. Complicating the situation further: viewing these attacks individually rather than as part of a broader threat strategy blinds one to the true extent of the potential consequences. A logical response need not imply an armed one. It does suggest a sound and systematic counterstrategy that melds deterrence, defense, and offense, orchestrating the entirety of US and partner capabilities. Necessary responses include bringing more-than-military assets to bear in the service of national defense in ways previously unseen.

Unfortunately, current assaults on the country's national security take advantage of **organizational** factionalization while the threats conducting these attacks orchestrate their capabilities via more centralized regimes. Separation of government and private enterprises is a fundamental characteristic of the American economy. Yet cooperation between the two sectors has been no less fundamental to Americans persevering in during wars and preparation for war. Similar seams exist within the US government itself, ones that provided less risk to national security prior to cyber and other threats that have emerged in recent years. A recent Congressional Research Service report provides an example:

> **The Department of Energy (DOE) is the lead agency for the protection of electric power, oil, and natural gas infrastructure—cooperating with the Department of Homeland Security, the lead agency for pipelines…. The FERC [Federal Energy Regulatory Commission] and TSA [Transportation Security Administration] have statutory authority to regulate cybersecurity in the bulk power and pipeline systems, respectively. Although OE [Office of Electricity Delivery and Energy Reliability] participates in some of the same high-level groups as these two agencies…there is little discussion in published materials as to what extent OE collaborates directly with FERC or TSA on specific cybersecurity RD&D [Research, Development, and Demonstration] programs in the respective infrastructure sectors.[12]**

"Make the **training** harder than the fight" has proved good advice for the US Army. Leaders and led both relish and fear rotations at the service's combat training centers, knowing their training opportunities provide the acme of preparation for war where few mistakes go unpunished. Those training centers adapted when Cold War threats gave way to combat in Panama, Somalia, Afghanistan, and Iraq. Current rotations seek to replicate the requirement for joint operations. They are less effective in meeting the demands of multinational armed combat or honing skills when armed combat assumes a supporting role. Similarly, training at the highest echelons of government has yet to sufficiently incorporate current national security challenges as described herein. The same is true at the soldier level where better understanding of social media attacks, vulnerability of cellphones and other individual devices, and efforts of adversaries to undermine unit and family cohesion remain largely unaddressed. There has been some impressive progress in the training arena. The Army's Synthetic Training Environment One World Terrain (OWT) can replicate terrain anywhere in the world. Yet training capabilities thoroughly integrating this greater spectrum of threat types has yet to be developed.

[11] This is a simplified paraphrasing of definitions from several sources.

[12] Congressional Research Service, "Cybersecurity for Energy Delivery Systems: DOE Programs," R44939, August 28, 2017, ii and 15.

Campaign of Learning observations regarding **materiel** were limited (remembering that the focus of the campaign was other-than-technological concerns). Comments fell into two primary categories. The first, further addressed below, regards the lethargy and lack of responsiveness in acquisition-related matters. Put simply, US government acquisition processes remain overly complicated and ill-suited to today's dynamic security environment. The second category touches on the backward-looking nature of materiel efforts. In LtGen Crall's words, "of that emulation, of that money, of that contract work we do… about 95 percent of our effort is focused on legacy systems, much of it getting legacy systems to work together."

Leadership in the national security sphere demands much of its practitioners. The experiences and skills that allowed those to enter the senior-most ranks of today's army may be of limited use when dealing with current challenges much less those of years to come. Example Campaign of Learning comments included:

- "Yesterday's disrupters and innovators have become today's establishment. We have a distributed, decentralized threat matrix we never had before. We're missing the agility and adaptability we need. If you're not disrupting yourself, someone else will."
- "The sunken cost fallacy is killing future capabilities and readiness. It takes incredible courage and willpower to say something isn't working and we need to find another way."
- "The French with their Maginot Line 'solution' was military modernization for a force that lacked the imagination necessary to understand that the character of war was changing. It was leadership infected with backward-looking hubris that celebrated past laurels instead of critically looking forward to account for new realities."

Leaders in our evolving competition and armed conflict environments face both new challenges resultant of the vulnerabilities discussed here and more familiar ones. General Holmes noted the tendency for some to evade unfamiliar (and therefore uncomfortable) challenges. One Young Minds on Competition and Conflict panel member cited the equally well-entrenched break on readiness imposed by short-term thinking and the nature of armed service evaluation systems: "Current readiness fits in a rating period. Future readiness does not." LTG Paul Funk recognized the tension between the undebatable need to maintain combat proficiency and prepare for these new forms of waging war. The former is an essential not only for winning on future battlefields but also for demonstrating to allies and partners that we are serious about readiness and able to effectively assist any asking us to support their training.

There is no less call for innovation in readying for the future when it comes to **education.** Education of service members alone is essential but no longer sufficient. As noted, ours is an environment where soldiers, family members, and American society at large are targets of misinformation and disinformation skillfully honed to appear as fact. Use of messages falsely informing spouses and parents of their loved one's death, fabricated rumors of a leader's immoral behavior, invented reports of American atrocities, and realistic but concocted visual evidence portraying US forces in the worst of lights are already employed threat tactics. Even the prepared will find ignoring such "evidence" difficult. Failure to educate likely targets before these attacks virtually ensures adversary success.

Vice Admiral Robert Harward got to the core of **personnel** considerations with his observation that "If our nation's war is a cyber war, what are we going to need [our] people on the ground to do?" Others raising personnel concerns questioned the effectiveness of current recruiting, retention, and retirement models. It was thought that current recruiting largely fails to recognize the motivations of today's American youth while at the same time overlooking a significant portion of those in the available pool of recruit candidates. LtGen Crall was among panel members observing that many youth motivated to support the country are unwilling to do so given the traditional model:

> **We don't know our target audience for recruitment very well. They don't want to join our teams in the conventional fashion…. They want to work where they want to live. They don't want to live on our bases. They want to live in Austin, Texas; Seattle, Washington; Los Angeles; or Portland, Oregon. Why can't they live there?… They claim they do their best work between 2300 and 0400. They are not interested in removing their body hardware. They don't like the idea of physical fitness tests. Frankly, I could care less about any of those things. We want their brains. We want their talents. They're ready to join us but they don't like the conditions that come with employment.**

Facilities concerns arose primarily in terms of exposure to enemy attack, a physical side to the informational assaults service members, their families, and Americans at large experience. John Pulju posited, "There won't be any safe havens. Even the homeland…will take more losses." Cyberattacks will accompany physical strikes. Command and control systems may be denied or compromised, confounding mobilization and deployment. That overseas bases will likewise be exposed to such assaults complicates basing agreements. Mission command—the process of decentralizing decision making after leaders provide clear mission statements and their intents—will have application during this initial period just as it will once organizations arrive in a theater.

Difficulties with existing **policies**, procedures, and processes was a theme interwoven throughout Campaign of Learning discussions. There were differing opinions on the sufficiency of existing Congressional authorities. Some believed most of those needed are already in place while others thought additions or adaptations were in order. In contrast, incentive structures were universally found wanting. Ms. Flournoy believes current incentives—formal or otherwise—favor the status quo and staying on-course rather than disrupting in-progress projects even when inefficiencies or shortfalls in ultimate effectiveness become clear. She cited the "insurgency" among those in the US Navy, that by individuals who took on battleship stalwarts in the interwar years to champion the naval aviation ultimately fundamental to victory in World War II. Flournoy believes the US military has the technological talent necessary for similar innovations today but that it is smothered by the absence of clear career paths for technologists as well as promotion standards that marginalize technologists or force them into general line positions where their talents are lost.

Longstanding acquisition processes likewise pose obstacles. General Alexander remarked that in his current position he can complete timely business-to-business contracts with civilian companies in a matter of weeks while it takes two or three years of convoluted process when the customer is the US military. He firmly believes that many in civilian industry want to assist those responsible for national security but find doing so to be unnecessarily complex. Dr. James Canton proposed that the Army (and by implication, other services and the joint community) develop a 25-year plan to unify efforts toward future readiness and provide a basis for identifying specific investments. The plan would be dynamic, agile, and assisted by ongoing scenario development to assist decision-making and responsive course changes.

How does the US continue as world leader in guaranteeing security against regimes set on imposing their will? It is to answering this question that the remainder of this chapter now turns. Readers familiar with Eliot Cohen and John Gooch's classic *Military Misfortunes* will find many of these Campaign of Learning recommendations fit among those authors' keys to success—learning, anticipating, and adapting—while inability to achieve one or more of the three courts failure. So too, readers will have the opportunity to consider innovative approaches rarely if ever previously offered. **Appendix 3 contains a concise summary of the recommendations below.**

RECOMMENDATIONS: DOCTRINE

CHINA'S TIME FRAME IS A SINGLE GENERATION…. AT THAT POINT CHINA WANTS TO HAVE INTERNATIONAL HEGEMONY IN THE NON-KINETIC SPACE. IT RECOGNIZES THE US AS A COMPETITOR BUT SEEKS TO AVOID KINETIC WARFARE. IT IS FOCUSING ON CREATING INTERDEPENDENCIES IN WHAT IT DESCRIBES AS "COOPERATIVE COMPETITIVENESS."[13]

DR. JAMES GIORDANO

THE ARMY IS IN A PERIOD ANALOGOUS TO POST-VIETNAM. NOW IS THE TIME FOR A THEORETICAL/CONCEPTUAL FOCUS TO UNDERSTAND HOW FUTURE WAR WILL BE FOUGHT. JUST LIKE COMING UP WITH AIRLAND BATTLE.

LTGEN PAUL K. VAN RIPER

[13] Dr. James Giordano remarks during Roundtable 1, February 16, 2021.

Redefine "warfare." The US Army and government as a whole need to reconceptualize their perceptions of war. The phrase "winning without fighting" is a misnomer. Ongoing competition in the economic, information, cyber, diplomatic, and other spheres poses existential threats in ways previously unthinkable. "This *is* fighting," LtGen Crall insisted, "This is just what fighting looks like these days." That adversaries have beneficial relationships with the US in some sectors (e.g., current US-China commercial ties) while simultaneously threatening national security complicates the challenge. Doctrine needs to acknowledge and provide guidance accordingly.

The Center for Strategic and International Studies' (CSIS) Todd Harrison posited that focusing doctrine on near-peer competitors will be insufficient; capabilities employed by those countries will proliferate to other threat entities. Future Army budgets are unlikely to support larger force structures, meaning increased tradeoffs between personnel and technological developments will be called for. Systems and supporting doctrine that provide for fewer personnel having greater positive effects may be one way to address this tension (one individual in a remote location conducting no-fly operations using swarming capabilities, for example). Harrison likewise recommended the Army (1) prepare for increasing its role as a force enabler and (2) shift priorities from power projection to denial capabilities. The latter could conceivably "flip the script" and prevent significant gains in Chinese power projection.[14]

Leaders at all levels, military and otherwise, need to recognize this evolved nature of conflict, one in which the conventionally understood line between war and peace continues to blur. President George W. Bush had expectations of Iraq, Afghanistan, Bahrain, Qatar, Oman, and the United Arab Emirates hosting US bases in the aftermath of OIF and OEF with purpose and manner being similar to basing in Europe and Japan after WWII.[15] Expectations based on historical precedence may bear fruit in some cases. Elsewhere they will not. As during the Cold War, the US has a competitor willing to compete economically when seeking international support. Unlike during those pre-1990 years, today's primary economic competitor is better able to do so on par with the United States and willing to use that power to influence nations friendly to the US as well as others neutral or hostile. Also unlike the Cold War: while Russia and others have recently employed surrogates and deceptive combat operations, major power competition of late less often relies on armed force. The Army must adapt accordingly. That adaptation should include how the US Army interfaces with current allies and partners in addition to expanding the number and type of its relationships.

Private organizations, US and otherwise, should be a part of this collective effort. US business and academic institutions need to be aware of the threats posed when adversaries operate in non-military arenas. Recognition that Army and other service roles may have to expand into other areas, adding domains other than those currently employed in service and joint doctrine—land, air, sea, space, and cyber—may be called for.

Adapt the current concept of maneuver. Reconceiving what armed forces mean by "maneuver" should be part of these adaptations. Maneuver is currently defined as the "employment of forces in the operational area, through movement in combination with fires and information, to achieve a position of advantage in respect to the enemy."[16] That is no longer sufficient when the means of competition have expanded in type and primacy. An enhanced understanding of maneuver better suited to Multi-Domain Operations and the challenges inherent in today's operational environment would include threat finance, supply chains, and other competition realms not previously considered in this context. A possible replacement for maneuver's current definition: "the employment of relevant resources to gain advantage with respect to select individuals or groups in the service of achieving specified objectives."[17]

---

[14] Mr. Todd Harrison, Center for Strategic and International Studies, comments during Roundtable 3, April 26, 2021.

[15] Vice Admiral (VADM) Robert Harward remarks during US Army TRADOC virtual VIP panel, May 12, 2021. VADM Harward had met with former President. Bush shortly before the panel meeting.

[16] *DOD Dictionary of Military and Associated Terms,* Washington, D.C.: Joint Chiefs of Staff, January 2021, 135.

[17] This definition does not cast fires, movement, and information aside as potential components of maneuver. It instead augments them with any other capabilities that are pertinent to achieving sought-after objectives. For further discussion of the reasoning behind a reconsideration of maneuver, see Russell W. Glenn, "Meeting Demand: Making Maneuver Relevant to the 21st Century," *Small Wars Journal* (July 5, 2017), http://smallwarsjournal.com/jrnl/art/meeting-demand-making-maneuver-relevant-to-the-21st-century (accessed August 9, 2017); and Russell W. Glenn, *Questioning a Deity: A Contemplation of Maneuver Motivated by the 2008 Israeli Armor Corps Association "Land Maneuver in the 21st Century" Conference,* Latrun, Israel: Israeli Armor Corps Association, 2008, ix, "Latrun 2008 Proceedings" at https://www.iamti.com/publications (accessed August 16, 2021).

Pursue ways of deterring in the cyber domain and information sphere. These represent a fundamentally different type of threat than that presented by nuclear weapons. Attacks with nuclear weapons proved to be unviable during the Cold War. Adversaries concluded defense would be only partially successful. Deterrence was the remaining option. Conditions are far different today. Recent attacks demonstrate that comprehensive defense is impossible while attacks reap few significant negative consequences.

Do not overestimate China's power and influence. Internal problems include issues of demographics, income, and political structure. These make it unclear whether the current version of the Chinese Communist Party is viable in the long run.

Recognize that total victory will rarely if ever be attainable. The nature of today's competition means that conflict is the constant state of affairs. Plans should include development of "off ramps" that ease tensions or deter foes at acceptable cost. Doctrine should also ensure better understanding of antagonists' versions of what is morally acceptable and the spectrum of capabilities they employ, including those non-kinetic.

Increase the strategic IQ of the US military across the force. Regional allies and partners will be fundamental to better planning, training, and operational execution, a situation requiring a more effective strategic approach to security cooperation than has existed in recent years. Additionally, relationships with active foes will often incorporate and require drawing on active commercial and other associations even as conflict is ongoing.

RECOMMENDATIONS: ORGANIZATION

When the Boeing 737 Maxes started crashing, there was a government agency whose entire job it was to gather up the facts of all those different crashes and then come up with a theory of what needed to be fixed and then oversaw the fixes that went into that.... We need the same kind of function in the US government [for cyber issues].... You have air, land and sea, and space and now cyber.... But in cyber, the private sector is front and center. Any conflict in cyberspace, whether motivated by a criminal element or motivated by geopolitical conditions, it's going to involve both the government and the private sectors. [You need] something similar to the NTSB [National Transportation Safety Board].[18]

Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds Hack"

Better orchestrate government and private sector capabilities. Better orchestrating government and private sector organizations will require new authorities, modification of those existing, and compromise by all parties involved if these relationships are to succeed. The Army must be a leader in establishing and maintaining closer ties just as when reinforcing and building new affiliations in the multinational arena. Failure means foes will exploit seams and gaps left unaddressed.

The Army should take the lead in establishing and maintaining closer ties with current and new military, government, and industry domestic and multinational partners. Leaders need to instill a sense of these expanded coalitions and partnerships' primacy and permanence in national security. General Holmes emphasized that other-than-combat requirements cannot be viewed as temporary. Soldiers cannot be allowed to consider such less traditional military elements of competition "a part-time job [after which] we get back to… what we like and are good at: fighting combined arms war in accordance with our current doctrinal constructs." He went on to commend the Army's Security Force Assistance Brigades (SFABs), suggesting this model should be applied more broadly and incorporate organizations other than the Army. He cited the cooperative cyber structures put together and deployed to locations like Romania and Ukraine in defense of the US 2020 elections against Russian interference and the importance of the Army in future efforts. "We're still organized around fighting during armed conflict, the violent part of it, and not organizing ourselves around competition…. It *is* war. It's a different way to fight it. We should be thinking about how we're going to organize to do that."

Structure organizations to support a culture of experimentation, learning, and innovation. Ideally these new organizations would be designed to support a culture of experimentation, learning, and innovation. They would encourage soldiers to take risks, learn, and share their experiences. Teams would operate with a "we" mentality—a "we" encompassing all participants, a comprehensive "we" rather than an intra-Army "we"—that supports innovation by connecting their members with other personnel and resources. Such organizations would encourage changing course when an approach or technique falls short of requirements.[19]

[18] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds Hack," National Public Radio transcript of "All Things Considered" broadcast, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (accessed June 7, 2021). The individuals quoted in the passage are respectively Alex Stamos, director of the Internet Observatory at Stanford University and former head of security at Facebook and Kevin Mandia, chief executive offer of the cybersecurity firm FireEye.

[19] Comment made by a member of the Young Minds on Competition and Conflict panel, May 6, 2021.

RECOMMENDATIONS: TRAINING

It's not just that the Chinese and others are developing AI and machine learning at a greater rate. They're perfecting another art that I think is more insidious, one that we don't seem to be paying much attention to: that's algorithmic warfare itself. It doesn't take a whole lot to reduce confidence in your machines' output if your data sources, your network, and your algorithms themselves are corrupt. If you don't trust the gauges you're looking at or if you hesitate when you look at them, that level of paralysis at the speed of the fight we're talking about [can be decisive. That is especially true when we are dealing with] intercept of hyper-sonics and other things that move relatively rapidly.... So in addition to increasing their prowess in this area, they're looking at ways to decrease ours. That's a two-fold approach we need to look at.

LtGen Dennis A. Crall

Make Army combat training center (CTC) events multi-domain, multinational, and whole of government. Current training rarely acknowledges the existential nature of other-than-combat threats. Such injects tend to be little more than superficial when they are incorporated into training. This should not surprise; training standards do not exist for these less traditional forms of competition. There is an immediate need for training that grants primacy to competitions in which armed conflict assumes a subordinate role. Rotations might include combat scenarios throughout. Combat might instead be a lesser part of other scenarios or play no part at all. Industry should be a participant, as should nongovernmental and inter-governmental organizations. The long-established special operations approach of "by, with, and through" when working with partners may have application in many of these cases. America's primary competitors today will not be changed by force. Deterrence and otherwise mitigating their aggression will be essential tools.

Eliminate performance grading during CTC rotations. General Holmes suggested that grading performance during combat training center rotations be eliminated.

We need to throw out the process of grading a unit's performance.... When you throw the grade in there, it means all the commander can think about is getting a passing mark, meeting his or her objectives, and moving on to the next test. [The result is commanders] don't really care about their teammates' training objectives or the multi-domain or multinational objectives because they've got that report card coming.

Prepare to employ cyberattack, defense, and deterrence regardless of the type of operating environment. General Alexander proposed that the US prepare to employ cyber regardless of the operating environment: in peace, during crisis, or in war.[20] His comment logically pertains to the application of capabilities in other domains and has obvious training implications. Bringing other services into Army training in the later 1970s was a major step forward in improving readiness. The discussions and recommendations above make it clear that the challenges of the 21st century here again require a comprehensive approach to training, meaning *all* relevant parties should participate and do so substantively.

RECOMMENDATIONS: MATERIEL

The rise of near-peer evolved competitors with advanced technology present a challenge to the US not seen since the Cold War.

John M. Pulju

You don't compete against weapon systems. You compete against institutions.[21]

Dr. David Finklestein

Maintain a systems perspective during materiel and other capabilities development, to include doing so when addressing deterrence, defense, and offense considerations. Like organizational considerations, those regarding materiel must be considered from a systems perspective. Members of the Young Minds on Competition and Conflict panel recommended a better offense-defense balance in the cyber and artificial intelligence areas given that US approaches arguably over-emphasize the offense, thereby limiting development of defensive capabilities. Deterrence merits similar consideration.

Ensure operational proficiency when working in degraded environments. Properly preparing for competition and armed conflict means ensuring proficiency when working in degraded environments, e.g., when attacks on algorithms corrupt or interrupt C2 capabilities or make reaction speeds unavoidably slow. Developing new and improving existing US capabilities should account for cyberattacks and other means of reducing operational effectiveness. Redundancy should be incorporated into materiel development, training, and organizations.

[20] Other obligations required GEN Alexander's departure from the VIP panel prior to its discussion regarding an expanded understanding of what constitutes war.

[21] Observation by Dr. David Finklestein during the Roundtable 1 discussion, February 16, 2021.

Improve anti-access/area denial (A2/AD) response capabilities. These may be technological or otherwise in character, the latter possibly including deception, improved and expanded partner intelligence agreements, quantitative advantages gained via alliances, and deterrence.

RECOMMENDATIONS: LEADERSHIP AND EDUCATION

MISSION COMMAND — THE CONDUCT OF MILITARY OPERATIONS THROUGH DECENTRALIZED EXECUTION BASED UPON MISSION-TYPE ORDERS.[22]

DEPARTMENT OF DEFENSE (DOD) DICTIONARY OF MILITARY AND ASSOCIATED TERMS

WE HAVE TO QUIT SAYING WE'RE THE BEST ARMY IN THE WORLD. IT GETS US IN TROUBLE.

LTG (US ARMY, RETIRED) PAUL E. FUNK

Avoid institutional hubris such as an unquestioning belief that US Army equipment, soldiers, and their leaders are the world's best, as is the force in terms of maneuver. The validity of such a belief is not the issue. The concern expressed was instead that such institutional hubris impedes recognition of evolutions in the OE and the learning and adaptation that recognition would logically bring. The old saw that "War doesn't change. Warfare does" bodes ill for an army that fails to grasp ongoing changes in the character of warfare. The first step is acknowledging the situation at hand. Only then can an institution meet Cohen and Gooch's requirement to learn, anticipate, and adapt effectively.

Enhance the theoretical and conceptual components of military education and expand its audiences. LTG Paul Van Riper suggested that today's military education should increase its focus on the theoretical and conceptual. The observation harkens back to what was arguably the Army's most revolutionary and successful post-WWII keystone doctrine, that underlying victory in the 1991 Persian Gulf War. Following on doctrine thought too prescriptive, AirLand Battle's 1982 introduction and update four years later blended its specific guidance with a theoretical foundation for how Army leaders should conceive of emerging ground combat challenges.

Employ effective mission command. It remains to be seen whether Multi-Domain Operations proves to be as successful as AirLand Battle. Mission command will be one of the foundation stones if it does. It is clear from previously cited observations made by the VIP panel and other Campaign of Learning participants that today's competition space requires a span of expertise exceeding any one individual's ability to grasp its entirety. Understanding much less systematically orchestrating the military, economic, information, cyber, diplomatic, political, technological, and other elements of that space requires clear mission and intent statements and decentralized decision-making by those most able and well-informed. Maintaining cross-domain and overarching situational awareness in support of decisions at every echelon will be a particular challenge. "How are you going to work out that conflict between having enough centralized [command and control] to integrate all these tools," Gen Holmes asked, "but enough flexibility forward for young, tough, smart warriors to figure out how to win their individual battles?" He answered his own question: mission command, a concept easily defined but difficult to establish and maintain in practice.

Maintain alliances even when not fighting. Related comments from VIP panel members included recognition of—in some cases re-recognition of—still relevant fundamentals:

- Alliances are essential throughout the conflict space.
- Forward basing of forces provides otherwise unattainable flexibility.
- Many of the Army's future challenges require other components of government and the private sector if they are to be met. The Army may need to take the lead the discussion of how to address these challenges in a whole-of-nation and broader manner.[23]

Develop plans and priorities identifying where the collective whole of US national and international security should be in ten years. These plans and priorities should take on difficult issues such as technology sharing policies.

Think like an insurgent. AI will provide decision-making advantages. Autonomous systems, resilient networks, cyber proficiency, and other technologies will enhance Army and broader US readiness…but these are also areas under active development by adversaries. Ms. Flournoy believes leaders must adopt more asymmetric mindsets, identifying adversary weaknesses and determining how we can undermine their strengths. In short, thinking like an insurgent should at once remove any complacency due to believing that we are the best military in the world while opening minds to approaches that would otherwise go unrecognized. She went on to advise that success will require checking rank and requirements for consensus at the door to encourage innovation and take advantage of subordinates' insights as well as those of partners from other communities.

[22] *DOD Dictionary of Military and Associated Terms,* Washington, D.C.: Joint Chiefs of Staff, January 2021, 144

[23] LtGen Paul K. Van Riper remarks during US Army TRADOC virtual VIP panel, May 12, 2021.

Ensure leaders and plans include a thorough understanding of antagonists' moral perspectives and spectrum of non-kinetic capabilities they employ, many being outside those traditional military. The introduction and continued maturation of disruptive strategies brings with it a multitude of ethical and moral dilemmas in addition to operational conundrums. These quandaries are outpacing existing laws, doctrine, regulations, and policy. The Army is not only challenged in identifying and preparing for its roles in this evolving OE. It will additionally be challenged with defining rules of engagement; ethical boundaries; and research, development, and operating policies that meet the demands of national security while not violating American standards of conduct.

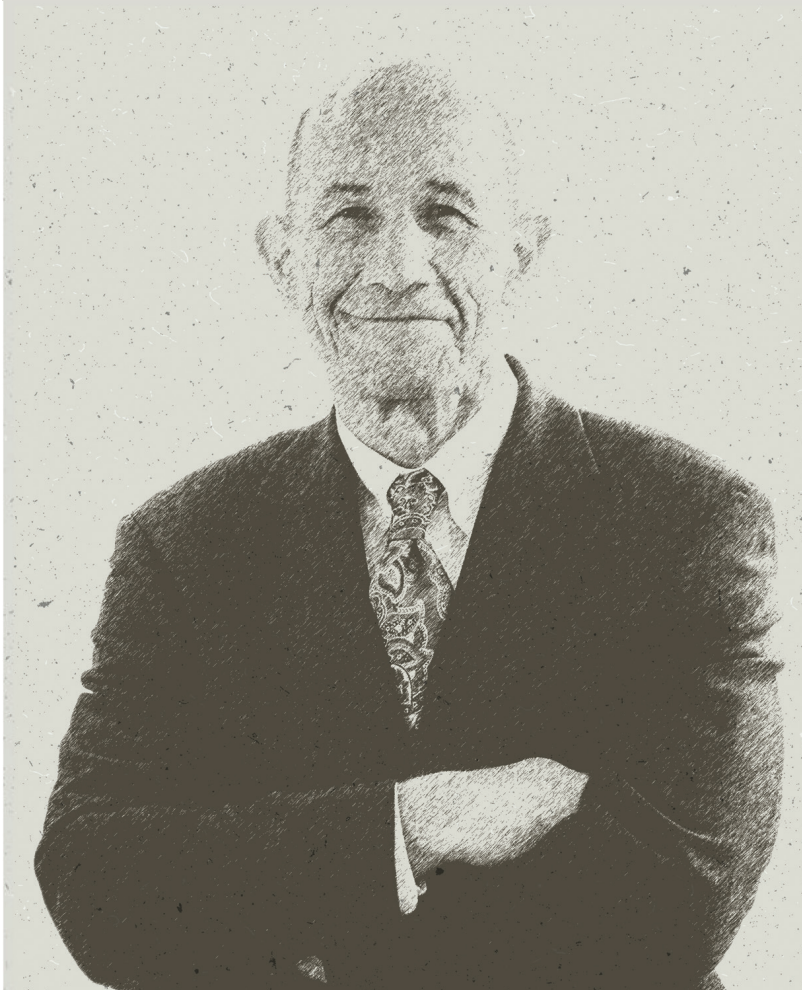
RECOMMENDATIONS: PERSONNEL

The long pole in the tent for you all is modernizing your talent management, your human capital approaches…. Number two, create a more competitive environment that welcomes ideas. Three, your training has to be much more realistic. [It needs to include] losing communications or situational awareness for a period of time, or suddenly not being able to trust incoming data because the enemy has messed with it. Technology investment and acquisition reform and all that are important too, but if you don't have those first three in place, the last piece isn't going to matter.

The Honorable Michèle A. Flournoy

Why not have a cyber auxiliary in the same way we have an air auxiliary in the Civil Air Patrol, one that's involved every day supporting homeland defense? Can we find a way that allows Americans to support and defend their country at a rate less than even the commitment of the reserve? To allow them to say "I want to do this; I'll do what it takes? I'll do it as I have time available, but I don't want to make that commitment of changing my lifestyle or having to move."

General (USAF, retired) James M. Holmes



Incorporate soldier talents developed pre-recruitment or during off-duty hours. There are several innovations ongoing in the US Army's personnel system. The Army is transitioning from the service's industrial age approach of gaging potential through rank and military occupational specialty (MOS) to a more information-rich focus on individuals' knowledge, skills, behaviors, and preferences (KSB-Ps).[24] Ideally these innovations will incorporate talents developed pre-recruitment or during off-duty hours, allowing leaders to identify those faculties when planning or operations require particular capabilities otherwise unavailable in sufficient numbers.

Find a way to allow Americans to support and defend their country in non-traditional ways; ways requiring less than current reserve commitments. This would dramatically expand the pool of those able and willing to lend their talents to national security by allowing remote work; waving physical conditioning, grooming, and work-hour standards; and providing for part-time service. General Holmes' remark in the above quotation spurred considerable enthusiasm among those on the VIP panel. One member thought it might address some of the inefficiencies inherent in the reserve force today. Dr. Canton saw it as a way to address Ms. Flournoy's previously noted call for asymmetric thinking. He recalled his time as an Apple executive during which the corporation had a unit tasked with developing its Macintosh computer. Canton described how the organization's management of which he was a part—what he described as "big army and corporate"—tolerated the group's "insurgency" as expressed in casual dress and other "out there" behaviors that included flying a pirate flag. Such innovation demands "leadership championing innovation at every level. Fail fast. Disrupt yourself. Relying on an innovation officer [alone] doesn't cut it." He went on to reinforce the need to include outside talent, expanding the Army's talent pool.

Better incorporate generational considerations in personnel management innovations. Comments from the Young Minds on Competition and Conflict panel reinforced the importance of including generational considerations in personnel management innovations. Developments in any successful personnel long game will require a holistic approach. Closing gaps between generations will be as important as reducing that between the public and private sectors. A US strength is its potential to leverage significant demographic and cultural diversity, one our competitors often actively impede in their own countries. The situation is by no means perfect in the United States, however. Microaggressions and non-inclusive attitudes can force valuable talent to leave the security industry or preclude entry by those potentially willing to serve. The panelists suggested the possibility of revisiting security clearance accessibility as part of fully leveraging these populations. Some from younger generations want to make an impact in the service of national security; incentives help bring them onboard. This in turn requires older generations to be open to the ideas of incoming generations.

RECOMMENDATIONS: FACILITIES

WE EXPECT ADVERSARY ACTIONS DIRECTED AGAINST THE HOMELAND. INSTALLATIONS ARE NO LONGER SANCTUARIES.[25]

"ARMY INSTALLATIONS STRATEGY: SUPPORTING THE ARMY IN MULTIPLE DOMAINS," DECEMBER 2020

Address expanded threats to installations and potential off-installation targets. The threats to domestic and international US Army facilities have expanded both qualitatively and quantitatively in recent years. Propaganda, misinformation, disinformation, and mal-information attempts to influence Americans or other populations; cyberattacks on facility infrastructure; drone use for reconnaissance and weapons strikes; vehicle-borne bombs; indirect fire: these and other threats become more treacherous when an adversary uses them collectively, e.g., using social media to recruit pliable individuals as surrogate attackers. That not all attractive targets are physically on military installations further complicates the challenges, as does the psychological effect of these "rear area" assaults on deployed soldiers morale and physical well-being.

[24] Michael J. Arnold (Deputy Director, Army Talent Management Task Force) comment during Association of the United States Army Thought Leaders on Talent Management panel event, June 3, 2021.

[25] "Army Installations Strategy: Supporting the Army in Multiple Domains," December 2020, 1, https://www.asaie.army.mil/Public/SI/doc/Army_Installations_Strategy%20DEC%202020.pdf (accessed June 29, 2021).

POLICY RECOMMENDATIONS

There was an institutional arrogance on the part of France's senior commanders who believed that their force and their approach to warfare would prevail. It took the French three terrible defeats to finally get the message that change might be needed. To win, France had to master competition, crisis, conflict, and change.[26]

Ian M. Sullivan, "Once More unto The Breach Dear Friends"

China is forging ahead. But it is not doing so alone or uncontested. Japan, India, Russia, and many others have their own designs. Far from being pawns, smaller countries are often the most pivotal players. Many of them have far more recent experiences dealing with outside powers than China has acting as one.[27]

Jonathan E. Hillman, The Emperor's New Road: China and the Project of the Century

Facilitate innovation, to include addressing acquisition shortfalls and taking steps to better allow companies less familiar with Department of Defense (DOD) procedures to present their ideas or products. Participants in the Campaign of Learning uniformly acknowledged the need to address (1) shortfalls in a dangerously lethargic US government acquisition process, (2) unresponsive Cold War-era policies and regulations, and (3) hyper-cautious contracting procedures. VIP members in particular encouraged finding additional ways to allow companies less familiar with DOD to present their ideas or products as a first step. Streamlining the progression from initial expression of interest through fielding of products and services is a second. Currently progress in these areas lags demand given a security environment with many more interlocking parts than was previously the case, one in which our foes are often innovating more quickly than us. Current client-provider relationships will continue to be appropriate for some military-industry dealings. Something akin to commercial partnerships otherwise promise greater effectiveness, particularly when seeking to redress antiquated government processes that fail to take advantage of those proven in the commercial arena. "We have not harnessed the private sector," Dr. Canton observed. "We don't have another generation to get this right. We've never faced an adversary like China."

Encourage project leaders to act when they recognize failing or suboptimal ongoing work. Innovation facilitation requires acknowledging what does not work while institutionalizing what does. Current formal and informal incentive (to include promotion) structures favor the status quo and staying-the-course rather than disrupting in-progress projects even when inefficiencies or shortfalls in effectiveness become apparent.

Avoid fixation on threats posed by China, Russia, and North Korea at the expense of broader readiness. This is notably the case in the Indo-Pacific region where distances and current national security concerns conspire to leave other threats and opportunities underappreciated. Army multinational partnerships, again those in the Indo-Pacific region in particular, would benefit from a shared focus on defeating A2/AD systems. Challenges regarding China, Russia, and North Korea cannot be ignored, but initiatives should avoid fixating on these threats to the detriment of broader readiness.

Establish a common cyber operating picture. General Alexander called for the establishment of a cooperative, common government-commercial operating picture that would provide all participants with a shared understanding of cyber threats in real time.

Review and, if necessary, revise policies regarding DOD and other US government agency restrictions regarding communications with Americans when those restrictions prevent citizen education on countering threat IO efforts. There is no reason General Alexander's recommendation should not extend to information operations. This means more effectively identifying and dealing with adversaries whose initiatives penetrate social media programs, as well as US and partner media companies, in order to target vulnerable segments of our populations or otherwise threaten national security.

DOD and other government restraints on engaging in information operations that might influence American citizens are for good reasons tightly circumscribed. Complicating the issue: Spillover from DOD and other government agencies' international information campaigns is practically impossible to prevent given the nature of the internet and social media platforms. Providing US citizens critical thinking skills and educating them regarding the potential negative effects of social media and ways to mitigate those effects is a challenge of particular significance, one with which the Army and DOD more broadly can help. Reevaluation of standing restraints merits consideration.

[26] Ian M. Sullivan, "Once More unto The Breach Dear Friends": From English Longbows to Azerbaijani Drones, Army Modernization STILL Means More than Materiel," Mad Scientist blog #300, January 28, 2021, https://madsciblog.tradoc.army.mil/300-once-more-unto-the-breach-dear-friends-from-english-longbows-to-azerbaijani-drones-army-modernization-still-means-more-than-materiel/

[27] Jonathan E. Hillman, *The Emperor's New Road: China and the Project of the Century,* New Haven: Yale University Press, 2020, viii.

CONCLUDING THOUGHT

Not everything will work in efforts to address the above recommendations. Continuously experimenting and divesting what does not work while institutionalizing what does will be key to the US maintaining its position as a global leader and successful guarantor of security objectives. Openness will apply to traditional Army missions such as defeating enemies in combat, deterring armed threats, and supporting allies and partners. Ideas and concepts may come from unexpected sources, both human and otherwise.

General Alexander recalled an artificial intelligence exercise that pitted a population of individual crabs against an alligator population. The alligators benefited in the game's not recognizing their having any known enemies while the crabs obviously suffered the fate of being ready reptile meals. Much to the monitors' surprise, after the simulation had been left to run overnight on one occasion, the artificial intelligence had provided a way for crabs to overcome their exclusive focus on individual survival to cooperate in the interest of common defense. In doing so, the crabs had joined forces to attack the alligators, killing one in the process. AI, younger minds, those unfamiliar with the military: there are few limits to sources of solutions to future security challenges.

APPENDIX 1

Campaign of Learning Components

Readers desiring to access websites appearing below may find it more effective to do so from non-government computer platforms. Government platform attempts to access the All Partners Access Network (APAN) used in support of Mad Scientist blogs often experience blocking issues. Entries below that are unaccompanied by a web address do not have an accompanying online reference.

• Webinars

◦ "The Operational Environment and Conflict over the Next Decade," January 19, 2021. Participants:

- Dr. TX Hammes (Distinguished Research Fellow, Center for Strategic Research, Institute for National Strategic Studies, National Defense University)
- Dr. David Kilcullen (Professor of Practice in the Center on the Future of War and the School of Politics and Global Studies, Arizona State University; Senior Fellow at New America)
- Dr. Sean McFate (Senior Fellow at the Atlantic Council)

◦ "Competition and Conflict in the Next Decade," February 23, 2021. Mad Scientist blog #308: **https://madsciblog.tradoc.army.mil/308-competition-and-conflict-in-the-next-decade/.** Participants:

- Dr. Zack Cooper (Research Fellow, American Enterprise Institute)
- John Edwards (Deputy Special Agent in Charge, Office of Strategic Planning and Policy, US Secret Service)
- Dr. George Friedman (Founder and Chairman of Geopolitical Futures)
- Dr. Eleonora Mattiacci (Assistant Professor for Political Science, Amherst College)
- Collin Meisel (Program Lead, Diplometrics, Frederick S. Pardee Center for International Futures, University of Denver)

• Roundtables

◦ "What is China doing to develop, train, and educate its military and, consequently, what should the US Army focus on to mitigate the threat?" February 16, 2021, summarized in Mad Scientist blog #307, **https://madsciblog.tradoc.army.mil/307-disrupting-the-chinese-dream-eight-insights-on-how-to-win-the-competition-with-china/.** Participants:

- Mr. Dennis Blasko (Independent analyst and former military attaché in Beijing and Hong Kong)
- Dr. David Finkelstein (Vice President, CNA and member of the National Committee for US-China Relations and International Institute for Strategic Studies)
- Dr. James Giordano (Georgetown University, Professor of Neurology and Biochemistry, Chief of the Neuroethics Studies Program and Director of the Program in Biotechnology, Biosecurity, and Ethics)

◦ "What is Russia doing to develop, train, and educate its military and, consequently, what should the US Army focus on to mitigate the threat?" March 16, 2021, summarized in Mad Scientist blog #315, **https://madsciblog.tradoc.army.mil/315-the-bear-is-still-there-four-insights-on-competition-with-russia/.** Participants:

- Sam Bendett (Analyst with CNA Advisory Analysis Group Russian Studies Program)
- Dara Massicot (Senior policy researcher at the Rand Corporation)
- Brigadier General (US Army, retired) Peter Zwack

◦ "Given what our adversaries are doing to develop, train, and educate their militaries, how should the US Army and TRADOC shape and manage its workforce to best posture the US to win across the continuum?" April 26, 2021. Participants:

- Mr. Christopher Dougherty, Center for New American Security
- Mr. Todd Harrison, Center for Strategic and International Studies
- Dr. Michael O'Hanlon, Brookings Institution

Additional events in the campaign of learning included:

- The Center for New American Security (CNAS) hosted a virtual fireside chat with General Paul E. Funk II, Commanding General, US Army Training and Doctrine Command, April 29, 2021. Dr. Stacie Pettyjohn, Director, Defense Program, CNAS, moderated the discussion regarding the topic "Why are threat-based leader development, training, education, and talent management important for the Army?" A recording of the event can be found at **https://www.cnas.org/events/special-event-virtual-fireside-chat-with-general-paul-e-funk-ii.**

- Army Mad Scientist Writing Contest on Competition, Crisis, Conflict, and Change. Launched December 10, 2020, the contest was open to the public with a March 15, 2021 deadline for entries. Essays were not to exceed 2,500 words. Participants were to address one or more of the following questions within the context of Multi-Domain Operations:

◦ How will our competitors deny the US joint force's tactical, operational, and strategic advantages to achieve their objectives (i.e., win without fighting) in the competition and crisis phases?

- What stand-off capabilities, cyberattack, information operations, human engineering, and other disruptive approaches will our adversaries use to achieve their objectives?

- How will our adversaries leverage non-traditional "kinetic" capabilities [e.g., proxy forces, private military and security companies (PMSCs)] in the competition and crisis phases?

◦ How will our adversaries create and exploit seams that separate us from our allies and partners?

- What capability gaps will our adversaries exploit to their advantage in competition and crisis?

- How will our adversaries seek to overmatch or counter US joint force strengths in future large scale combat operations?

- Imagine a future Kasserine Pass or Task Force Smith – how would our adversaries neutralize our ground combat capabilities?

- What convergences of emergent game-changing technologies will our adversaries employ to achieve overmatch?

◦ How could our adversaries deliver a "knock out" blow to win and return-to-competition without resorting to nuclear weapons?

The winning essay and a runner-up are available via the links below:

◦ Winner of the Mad Scientist writing contest: Anjanay Kumar (Captain, US Army), Mad Scientist blog #322, April 19, 2021, The Joint Forces Defeat Before Conflict," **https://madsciblog.tradoc.army.mil/322-the-u-s-joint-forces-defeat-before-conflict/**

◦ Runner-up in the Mad Scientist writing contest: Carlin Kelly (1st Lieutenant, US Army), "A House Divided: Microtargeting and the next Great American Threat," Mad Scientist blog #323, April 22, 2021, **https://madsciblog.tradoc.army.mil/323-a-house-divided-microtargeting-and-the-next-great-american-threat/**

• Campaign of Learning-related articles by G-2 TRADOC authors:

◦ Ian M. Sullivan, "The Operational Environment: Now through 2028," Mad Scientist blog #283, November 9, 2020, **https://madsciblog.tradoc.army.mil/283-the-operational-environment-now-through-2028/**

◦ Ian M. Sullivan, "Once More unto The Breach Dear Friends": From English Longbows to Azerbaijani Drones, Army Modernization STILL Means More than Materiel," Mad Scientist blog #300, January 28, 2021, **https://madsciblog.tradoc.army.mil/300-once-more-unto-the-breach-dear-friends-from-english-longbows-to-azerbaijani-drones-army-modernization-still-means-more-than-materiel/**

◦ Russell W. Glenn, "Sub-threshold Maneuver and the Flanking of US National Security," Mad Scientist blog #301, February 1, 2021, **https://madsciblog.tradoc.army.mil/301-sub-threshold-maneuver-and-the-flanking-of-u-s-national-security/ (article summary only at this website). Full article at https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/361310.**

◦ Ian M. Sullivan, "The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict," Mad Scientist blog #326, May 3, 2021, **https://madsciblog.tradoc.army.mil/326-the-operational-environment-2021-2030-great-power-competition-crisis-and-conflict/**

• Young Minds on Competition and Conflict panel, May 6, 2021. Mad Scientist blog #339, July 12, 2021, **https://madsciblog.tradoc.army.mil/339-young-minds-on-competition-and-conflict/.** Audiovisual recording available at **https://youtube/15U6l8QE9Gk**

- Primary topics addressed during the panel were:
  - The US Army's roles and capabilities while meeting challenges when key adversaries seek to "win without fighting" during periods of competition and crisis.
  - US Army roles and competencies that will be adapted for contingencies when key adversaries neutralize traditional conflict capabilities through their use of stand-off assets, cyberattack, information operations, human engineering, and other disruptive approaches.
  - How the Army can adapt to an operational environment in which our adversaries will likely have rough parity in terms of materiel and can challenge us across a wide spectrum, particularly in terms of human capital (leader development, training, and education)
  - Panel members:
    - Jessica Budlong – Founder and Executive Director of the Nuclear Fusion Project; Communications Assistant at University of Denver; former research intern at Lawrence Livermore National Laboratory and Center for Arms Control and Non-Proliferation.
    - Major Amos Fox – Executive Officer, 3rd Squadron, 4th Special Forces Assistance Brigade; US Army School of Advanced Military Studies (SAMS) graduate; COL Tom Felts award winner.
    - Captain Lauren Hansen-Armendariz – Deputy Chief of Innovation, 101st Airborne Division; intelligence officer
    - Evanna Hu – CEO, Partner at Omelas; technologist; information environment subject matter expert; Nonresident Senior Fellow at the Atlantic Council.
    - Major Michael Kanaan – US Air Force AI expert; author of "T-Minus AI;" Director of Operations, Department of the Air Force/MIT Artificial Intelligence; former Co-Chair of AI, US Air Force.
    - Jimmy Zhang – Policy Analyst, Emerging Threats at Department of Homeland Security; Director, National Security Programs at Embolden; former international affairs specialist at Department of Justice.

VIP panel: On May 12, 2021, the nine individuals listed in chapter 1 gathered virtually to capitalize on the expertise and experiences of a select group of senior individuals to better understand how the US Army—and by extension the nation's collective armed services and government—can meet the challenges posed by adversaries seeking to neutralize America's battlefield advantages via in part or completely avoiding those capabilities in pursuit of their national security objectives.

APPENDIX 2

Existing and Evolving Threats to US National Security

**THE FUTURE IS NOT COMING IN 13 YEARS.
IT IS COMING IN 13 MINUTES.**

DR. JAMES CANTON

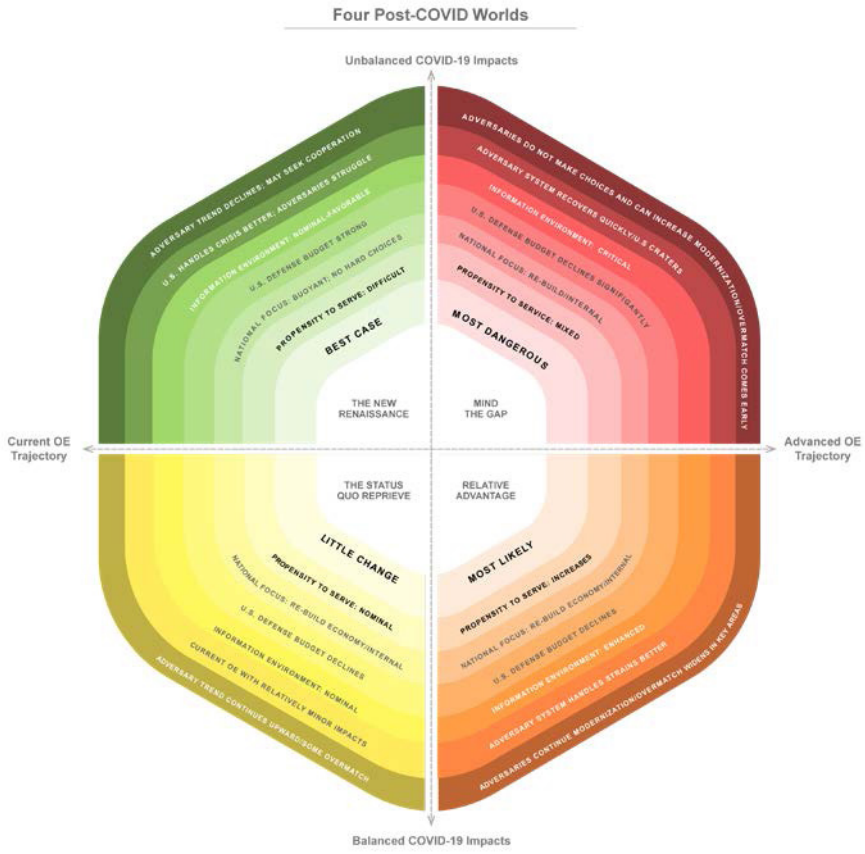


Figure 2.1: Four post-COVID-19 world models

In mid-May 2020, the Commanding General, US Army TRADOC, tasked the command's G-2 to conduct a reanalysis of the Operational Environment (OE) in light of COVID-19 and other recent evolutions in the security environment. The period of consideration was 2020-2028. This analysis spurred the campaign of learning for which this document is the proceedings.

G-2 devised four alternative futures, or "worlds" during the 2020 undertaking. These worlds represented the range of conditions found in the OE and the relationships between the United States and select threats to national security, the particular focus being on China and—to a somewhat lesser extent—Russia. Figure 2.1 concisely provides the key elements of each world.[28]

The first world, ***Status Quo Reprieve*** is essentially the OE as seen in November 2019 (pre-COVID) with limited changes incorporated due to the pandemic. ***Relative Advantage,*** the world deemed most likely to approximate conditions in the 2020-2028 period, is a future wherein the impacts of COVID and other factors are relatively balanced but where US adversaries' centralized systems allow them to recover more quickly from the pandemic's effects than does the United States. In ***Mind the Gap***, thought to be the most dangerous world, the US recovery bottoms out and its adversaries suffer comparatively limited consequences. In the fourth and best-case world for the United States, ***New Renaissance,*** US recovery outpaces its adversaries' and we have significant advantages.

[28] Expanded descriptions of these world's and their implications are available at Ian Sullivan, "The Future Operational Environment: The Worlds of 2035-2050," Mad Scientist blog #286, November 19, 2020, https://madsciblog.tradoc.army.mil/286-the-future-operational-environment-the-four-worlds-of-2035-2050/; and Ian M. Sullivan, "Once More unto The Breach Dear Friends": From English Longbows to Azerbaijani Drones, Army Modernization STILL Means More than Materiel," Mad Scientist blog #300, January 28, 2021, https://madsciblog.tradoc.army.mil/300-once-more-unto-the-breach-dear-friends-from-english-longbows-to-azerbaijani-drones-army-modernization-still-means-more-than-materiel/.

Four G-2 teams (accessions; leader development, training, and education; integration and force modernization; and resources and return on investment) analyzed the effects of each of these world models from a macro perspective and with a particular focus on the implications for US Army TRADOC. Among the more troubling insights was that regarding key US threats employing strategies and accompanying campaigns, operations, and tactical actions deliberately designed to avoid confronting American and partner nation military superiorities (with several of these advantages dwindling during the period to 2028).

Notable observations regarding the evolving nature of threats to US national security and America's vulnerabilities from the subsequent 2021 Campaign of Learning include the following.

Nature of Evolving Threats: Overview

Since 1885, the US has never faced a competitor or even group of competitors with an (aggregate) GDP greater than 40% of its own.[29]

Robert O. Work, "AI and Future Warfare: The Rise of Robotic Combat Operations"

- While the historical causes of future competition and armed conflict will remain, e.g., struggles for power and resources, the detailed character of these struggles will change. Megatrends such as demographic change, population migration, technology proliferation, climate change, and advances in productivity will create potential new points of conflict.
- America's foes will not entirely abandon conventional warfare, but it will less often be the first choice of US adversaries. By investing disproportionately in conventional warfare capabilities, the United States is preparing for the most dangerous but not the most likely form of future warfare. US adversaries are relying on the American perception of warfare as a duality between peace and war.
- US adversaries are increasingly borrowing techniques from non-state actors to create a hybrid style of warfare that operates below the US threshold of conflict.
- Adversaries are blurring the line between covert and overt action. While an action may be apparent, it may be difficult to firmly establish attribution and therefore target its sponsor. This incentivizes the use of mercenaries, making the approach available to wealthy state or non-state actors.
- Generally, future weapons will need to be small, smart, cheap, reliable, and easily maintained. These weapons will compete with the traditional "few and exquisite" weapons to which the US has become accustomed. Simplicity will be key, although smart systems will continue to proliferate.
- Though defense will dominate the air, sea, and land domains, offense will do so in the cyber and space domains. Competition in the latter two will escalate. The West is currently behind in the electromagnetic arena, which could become critical (unlike during the Cold War during which the US never lagged significantly). It is unclear to what extent deterrence will apply to these domains or what form it might take.
- Competition and armed conflict will increasingly be influenced by democratizing technology. This trend favors a move from conventional warfare to unconventional warfare during which "large numbers of small units," including non-state actors, will possess increasing survivability and lethality. Social media will enable weaker actors to exert disproportionate influence, allowing them to shape international opinion to their advantage. The proliferation and increased dependence on hyper-connective technologies will provide international actors with new threat vectors to target the US homeland, exposing new vulnerabilities within US society.
- Developments in artificial intelligence (AI) and quantum computing will expand the processing power and capabilities of both the United States and its adversaries. Advanced algorithms for microtargeting will provide foreign actors with advanced opportunities for the manipulation of information. AI could provide adversaries with new ways to manipulate information received and disseminated by decision makers during a conflict.
- Corporations will continue to influence societal consumption of information. It will be impossible for governments to control this influence completely. Instead, the United States must claim agency and explain its choices, thereby controlling the narrative regarding its actions. Exposing the power of corporations and explaining to US citizens the intent of activists on their platforms will enable a more information-literate population.

[29] Robert O. Work, "AI and Future Warfare: The Rise of Robotic Combat Operations," presentation in support of Mad Scientist Disruption & the FOE-AI & Future Warfare conference, slide 9, April 24, 2019, https://community.apan.org/wg/tradoc-g2/mad-scientist/m/disruption-and-the-future-operational-environment/274690 (accessed May 27, 2021).

- Victory in future wars will be fungible and favor the cunning. Controlling perceptions and identifying truth will be key components of victory.
- It is no longer possible nor beneficial to defend a US-led rules-based order.
    - The United States needs to learn from the amoral, hybrid techniques US adversaries have adopted. There will be methods of warfare employed by threats that will be unavailable to the United States due to American ethical standards and regulation.
    - "Unlike the United States, the enemy may well use armed robots programmed to fire without human oversight. [LtGen Crall] said at the Defense One Tech Summit: 'They may just simply put a machine-only solution to a firing solution, which may have errors and mistakes. And maybe they'll take that risk.'"[30]
- The future operational environment will be significantly different than that as envisioned only a decade or two ago:
    - Battlefields will be disrupted and chaotic as perhaps never before seen. These interruptions will be accompanied by targeting of headquarters with hypersonic and other weapons. Fragmentation and discontinuity will be a result.
        - Long-term interruption or complete denial of command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) capabilities is likely via cyberattack and other means, denying use of many systems now fundamental to combat effectiveness.
    - Individual leadership and mission command will play a significant role in continuing the fight.
    - Stocks of highly sophisticated systems will be depleted during any but very short conflicts.
    - Use of artificial intelligence will collapse time as decisions assisted by AI and made by automated systems become commonplace.

[30] Patrick Tucker, "It's Time to Wargame Against an AI-Enabled China," *Defense One*, June 23, 2021, https://www.defenseone.com/technology/2021/06/its-time-wargame-against-ai-enabled-china/174922/ (accessed June 24, 2021).

Nature of Evolving Threats: Specific Observations Regarding China[31]

If the PLA [People's Liberation Army] does go to war, it will mobilize and employ military, paramilitary, political, diplomatic, economic, financial, and civilian support in all domains.[32]

Dennis Blasko

- China is trying to modernize militarily on the cheap despite the growth of its economy. It spends one-third of what the US does on military modernization.
- China's ascendance in political and economic power is likely to continue, challenging US leadership in the international system. China will likely seek to avoid direct armed conflict with the United States, focusing instead on developing non-kinetic capabilities. The United States can mitigate its loss of international power by increasing its collaboration with regional allies, e.g., the Association of Southeastern Asian Nations (ASEAN) and developing new international partners.
- In addition to materiel advances, China's People's Liberation Army (PLA) is also modernizing its doctrine, organization, and training.
- It is important to pay attention to China's multi-generational military-civil fusion.
- China seeks to increase its influence at the cost of the United States. Although an Indian alliance with the US and NATO could offset this shifting balance of power, China's continued investment in denial capabilities challenges US power projection and global influence. The PLA's Anti-Access/Area Denial (A2/AD) capabilities are robust within the First Island Chain (the western line shown below in blue), and China seeks to strengthen its capabilities to reach farther east (the Second Island Chain line shown in red). These capabilities span the air, maritime, space, electromagnetic, and information domains. By mid-century, it is expected that China will attain one quarter of the global military power.

[31] Observations regarding China come primarily from comments made during the Campaign of Learning's

- Roundtable 1, "What is China doing to develop, train and educate its military and, consequently, what should the US Army focus on to mitigate the threat?" February 16, 2021. A summary appears as "Disrupting the 'Chinese Dream' – Eight Insights on how to win the Competition with China," Mad Scientist blog #307, https://madsciblog.tradoc.army.mil/307-disrupting-the-chinese-dream-eight-insights-on-how-to-win-the-competition-with-china/; and
- Webinar 2, "Are We Doing Enough, Fast Enough?" February 23, 2021. Mad Scientist blog #308: https://madsciblog.tradoc.army.mil/308-competition-and-conflict-in-the-next-decade/

[32] Observation by Dennis Blasko during the Roundtable 1 discussion, February 16, 2021.

- To avoid direct armed conflict with the United States, it is likely that China will turn to proxy warfare in regions of US interest. They may, however, engage in smaller, proxy conflicts around the globe in order to build power projection experience and further develop a level of international hegemony. This relatively low-risk behavior will allow China to divert US attention. It will mimic diversionary tactics used by the United Soviet Socialist Republic (USSR) during the Cold War. Potential areas of interest for this strategy include Cuba and the Philippines. The United States will need to be deliberate and intentional in addressing these conflicts.

- Taiwan is a focal point of US-China competition. While China does not currently have the ability to successfully execute an amphibious invasion of Taiwan, it will likely use proxy warfare, power projection, and denial capabilities to increase its influence and control of the island.

- The ability of PLA officers to conduct joint warfare remains a major challenge despite China's modernization efforts. However, the PLA is undergoing the greatest effort to improve its capabilities in history, to include officer and PME education with a new emphasis on joint operations. It is too early to gauge how effective these efforts will be.

  - The PLA seeks to become a joint force across all domains. Its leaders recognize that their current joint operations doctrine is inadequate and the size and force structure of the country's armed forces are imbalanced. Further, their officers and NCOs are insufficiently educated to deal with joint operations and technologies. Initiatives to address these issues began in 2015. This includes formation of a joint staff.

  - Only a portion of the two million-strong Chinese active military force is being modernized. Much of the force remains at 1990s mechanized warfare level.

  - This post-evolution PLA has a significantly different feel from that of only a few years ago.

- Chinese officers graduate from military academies where their educations are sub-par in comparison to those in the US. Their academies are the equivalent of vocational schools.

- Army primacy in the PLA has given way to Navy, Air Force, and strategic support force primacy.
    - Maritime capability is the initial focus of joint operations improvement. The army supports with aviation, SOF, and long-range missiles. The focus in training is the first island chain.
- China views bioscience much as it does AI in terms of developmental importance. It increased the GDP expenditure on bioscience more than 30-fold from 1991 to 2015. 76 percent of such expenditure is commercial but investors are primarily state-owned enterprises. Bioscience expenditure comprised 2.24 percent of GDP in 2020.
    - Current bioscience technology development tends to be experimental. China's Commission for Science, Technology and Industry for National Defense [rough equivalent of the Defense Advanced Research Projects Agency (DARPA)] uses the "triple helix" of academia, commercial sector, and government.
- China employs lawfare and ignores intellectual property laws in its efforts to gain advantage. ("What's ours is ours and what's yours is ours," a good example of conducting warfare in a sub-threshold manner.)
    - China takes "credit" for intellectual property and employs intellectual property "veiling" for dual-use technology, claiming proprietary rights to commercial products that may be used otherwise later. China claims to own the intellectual property rights if the intellectual property is made in mainland China, if Chinese nationals make it outside of mainland China, or if an entity with greater than 51 percent Chinese ownership produces it. These standards give China a broad set of claims over the growing body of research and intellectual property in biosciences.
- Moreover, China continues aggressive talent recruitment of foreign researchers, using the lure of attractive financial incentives and limited ethical controls. These efforts and broad state sponsorship of projects have China aspiring to create technological readiness in 40-48 months compared to approximately 60 months for the US.[33] Ultimately, China's lack of transparency and non-Western ethical practices in their research initiatives raise the risk of technological surprise.
    - Use of government money in taking on high risk, high payoff projects feeds not only PLA work but also that in Chinese academia and commercial enterprises. This pursuit can be done within the construct of their broad definition of what comprises ethical research.
- There is an inherent contradiction in Chinese capability development. They seek to empower initiative in a collectivist society in which citizens are constantly watched and leaders do not want to make mistakes. Political commissars are aware of these problems.
- China is aware of the US DOD and intelligence community's (IC's) focus on the military sphere. This is why they are developing other areas such as non-kinetic technologies and capabilities. They also employ the results of such development in the global marketplace.

[33] The example organization cited as employing these practices was China's Commission for Science, Technology and Industry for National Defense.

Nature of evolving threats: Specific Observations Regarding Russia[34]

Russia has demonstrated the intent and the most effective combinations of systems and concepts to challenge the US and its allies militarily in the near term. Russia's actions in Georgia, Ukraine, and Syria have demonstrated their intent to fracture the relationship between the US and its partners and their ability to pursue strategic objectives below the threshold of armed conflict. Russia uses unconventional and information warfare to propagate a narrative that breeds ambiguity and delays the reactions of their adversaries. Over the last decade, Russia has increased its investments in anti-access and area denial capabilities and systems intended to deny the Joint Force entry into a contested area and set the conditions for a fait accompli attack.[35]

TRADOC Pam 525-3-1, The US Army in Multi-Domain Operations 2028

- Russia is seeking to further develop artificial intelligence (AI) and unmanned systems (UxS) for combat, decision-making, de-mining, intelligence, surveillance, and reconnaissance. The country's military is starting to cooperate with domestic academic, industry, and private sector organizations to achieve this goal. Lessons learned from recent combat experience in Syria, Ukraine, and Nagorno-Karabakh have enhanced these efforts and improved platform development, testing, and evaluation. The military has surged to the top of those nations using unmanned aerial vehicles (UAVs) on a large scale for a variety of missions and tasks. This includes developing techniques for swarm employment. On a related note, they are also working counter-UAV capabilities and training. Other technological areas of focus include electronic warfare (EW). Capabilities include fielded systems with long ranges measured in hundreds of kilometers and others at very low-level tactical echelons. EW and UAV capabilities are sometimes combined to capitalize on the advantages of both system types.

- The defeat that the Azerbaijan military, equipped with Turkish and Israeli-manufactured armed unmanned aerial systems (UAS) and loitering munitions, inflicted on Russia's Armenian proxies in 2020 served as a wake-up call for many in the Russian defense establishment. Military journalist Victor Baranets bemoaned the fact that while "there are hundreds of light and medium-sized drones in the Russian military" they still do not possess "attack drones in the required quantity."

- Russia is working to modernize and professionalize its military forces. Results are mixed. There are more professional enlisted personnel than conscripts for the first time in the country's history. Russia continues to view the United States as the "gold standard" in the professionalization of its military and has sought to emulate aspects of US training to the extent allowed by its budget. In order to increase trust and retention in their military, Russia has improved many quality of life aspects for conscripts and contract servicemen, to include better living conditions (e.g., in terms of nutrition and housing), increasing communication and interaction between soldiers and their families, implementing changes to its training programs, and instituting other reforms to reduce hazing. These efforts have been successful in helping to diminish incidences of draft dodging and hazing, leading to the public's increased level of trust in the institution.

- However, military operations within the gray zone and continued connections with mercenary groups have hindered the Russian military's ability to build on this trust. The military's demonstrated relationship with mercenary groups combined with consistent denial of this connection by military officials threatens to undermine credibility building and trust both within the military and with the public. Signals of stalling professionalism and an erosion of public trust would include increased draft dodging, a return of hazing, and lower retention rates as soldiers leave to join private military companies and find other employment. Monitoring conscript mothers' social media groups could serve as a key barometer of the Russian military's health. Additionally, any consideration of deploying one-year conscript troops—about a third of Russian active duty land forces—would, given their connectivity with the mainstream Russian population, be challenging in a major long-term cross-border operation, especially if in proximity to controversial gray zone type actions.

- Russia and China currently collaborate on a transactional basis. Russia and China clearly have a growing partnership across multiple sectors. Their military cooperation, including exercises, is deepening. The key will be whether these activities move from colocation to real joint unit and systems interoperability. The United States must be mindful of not inadvertently pushing the two traditionally distrusting countries closer together.[36]

---

[34] Observations regarding Russia come primarily from comments made during the Campaign of Learning's Roundtable 2, "What is Russia doing to develop, train and educate its military and, consequently, what should the US Army focus on to mitigate the threat?" March 16, 2021. A summary appears as "How is Russia investing in their military human capital and promoting the military in the society, and how can the US Army maintain leadership overmatch in light of these investments?" Mad Scientist blog #315, https://madsciblog.tradoc.army.mil/315-the-bear-is-still-there-four-insights-on-competition-with-russia/

[35] TRADOC Pam 525-3-1 (TP 525-3-1), *The US Army in Multi-Domain Operations 2028,* United States Army Training and Doctrine Command, December 6, 2018, 7.

[36] For an additional consideration of Russia-China relations, see chapter 4 in Jonathan E. Hillman, *The Emperor's New Road: China and the Project of the Century,* New Haven, CT: Yale University Press, 2020, 60-77.

APPENDIX 3

Summary of Recommendations

Doctrine-related Recommendations

- **Redefine "warfare."** While the causes of future competition and armed conflict will remain similar to those historical—struggles for power and resources primary among them—the detailed character of how actors conduct these struggles will continue to change. America's foes will not entirely abandon conventional warfare; it will, however, even more so than in the past, be the ultimate extreme option. Leaders at all levels, military and otherwise, need to acknowledge this evolved character of conflict, one in which the conventionally understood line between war and peace continues to blur. Armed services and joint communities at present retain traditional and common-use understandings akin to war as "a state of armed conflict between countries or within a state."[37] This understanding denies cyberattacks, disinformation and misinformation, economic manipulation, and other actions currently employed by multiple countries against the United States status as acts of war despite their increasingly being directed against the US homeland and US national security objectives domestically and abroad. Ongoing competition in these other-than-armed force spheres pose existential threats in ways previously impossible. Complicating the situation further: viewing these attacks individually rather than as part of a threat strategy blinds one to the true extent of the potential or actual damage imposed. The US response need not be an armed one. Such would render the United States as the aggressor in many eyes. Effective responses do suggest a sound and systematic counter-strategy that melds deterrence, defense, and offense, and orchestrates the entirety of US and partner capabilities. This strategy would include other than military assets in the service of national defense in ways previously unseen. It will also require innovative approaches, for example, educating US and international private citizens and organizations regarding the threats posed when adversaries operate in spheres beyond those involving armed conflict.
- **Adapt the current concept of maneuver** to make it better suited to the demands of Multi-Domain Operations and the challenges inherent in today's operational environment. Use of surrogate militias, deception operations, and forms of attack for which NATO was unprepared during Russia's seizure of Crimea and eastern Ukraine (e.g., cyber, information, and economic) left Russia little threatened other than with sanctions and diplomatic pressure deemed acceptable in light of the objectives achieved. China's aggressive promotion of its national interests via the Belt and Road Initiative (BRI), use of lending procedures that sidestep international norms, and employment of information campaigns highlighting and magnifying the effects of social rifts in democracies provide another sample. A possible new definition for maneuver: "employment of relevant resources to gain advantage with respect to select individuals or groups in the service of achieving specified objectives."
- **Do not overestimate China's power and influence.** Internal problems—including issues of demographics, income, and political structure—make it unclear whether the Chinese Communist Party will be viable politically in the long run. It is possible that the United States is currently overestimating Chinese capability similar to its views on Soviet strength during the Cold War.
- **Pursue ways of deterring in the cyber domain and information sphere.** These represent a fundamentally different type of threat than that presented by nuclear weapons. Attacks employing those weapons proved unviable. Defense could not guarantee 100 percent interdiction. Deterrence was the only option. Conditions are far different with cyber, information, and select other capabilities. Recent attacks demonstrate that comprehensive defense is impossible while attacks reap few significant negative consequences.
- **Recognize that total victory will rarely if ever be attainable.** Plans should include "off ramps" that ease tensions or deter foes at acceptable cost.

[37] This is a generalization that summarizes the key element contained in most current definitions of war.

Organization-Related Recommendations

- **Better orchestrate government and private sector capabilities** by creating new authorities, modifying those existing, and supporting compromise by all participants. Current assaults on US national security take advantage of government-commercial factionalization while adversaries conducting these attacks orchestrate their capabilities via their more centralized regimes. Separation of government and private enterprise is a fundamental tenet of the American economy. Yet cooperation between the two sectors has been no less fundamental to Americans persevering during wars and in preparation for war. Similar seams exist within the US government itself, ones that presented less national security risk prior to threat types that have emerged in recent years.
- **The Army should take the lead in establishing and maintaining closer ties with current and new military, government, and industry domestic and multinational partners.** Leaders need to instill a sense of these expanded coalitions and partnerships' primacy and permanence in national security. The Army's Security Force Assistance Brigade (SFAB) model should be applied more broadly to include incorporating organizations other than the Army as appropriate.
- **Structure organizations to support a culture of experimentation, learning, and innovation.** These structures should encourage soldiers and leaders to take risks, learn, and share their experiences. Such organizations would also encourage changing course when an approach or technique falls short of requirements.

Training-Related Recommendations

- **Make Army combat training center (CTC) events multi-domain, multinational, and whole of government.** Current training rarely acknowledges the existential nature of other-than-combat threats. There is an immediate need for training that grants primacy to competitions in which armed conflict assumes a subordinate role…if any at all. This training will more often than not include representatives from industry and nonprofit sectors.
- **Eliminate performance grading during CTC rotations.** This will encourage a "we" mentality in pinnacle training rather than a focus on individual performance. Barring this change, there is a risk that commanders will concentrate on their unit's performance to the detriment of that by the more inclusive organization.
- **Prepare to employ cyberattack, defense, and deterrence regardless of the type of operating environment** and in combination with other capabilities. Cyber is a key element of national power for China and other threats. It is one the US should expect to see employed if China finds American actions regarding Taiwan exceed those thought tolerable. Training at the highest echelons of the US government has yet to adequately incorporate cyber, information, intellectual property theft, and other national security challenges.

Materiel-Related Recommendations

- **Ensure operational proficiency when working in degraded environments,** e.g., when attacks on algorithms corrupt or interrupt C2 capabilities or reaction speeds unavoidably slow. The extent of vulnerabilities to such attacks increases with the proliferation of commercial and government systems integrating components of the Internet of Things (IoT) that provide potential additional inroads for incursion.
- **Maintain a systems perspective during materiel and other capabilities development** and do so while addressing deterrence, defense, and offense considerations. Readiness is a collective function. Addressing challenges discreetly ensures gaps that expose vulnerabilities just as does an undefended boundary between units on the battlefield. For example, deterring and defending against cyber attacks should include stopping future theft of US intellectual property, theft totaling some $5 trillion over the past decade alone. Adversaries pursue this theft in a variety of ways. For example, China continues aggressive talent recruitment of foreign researchers, using the lure of attractive financial incentives and limited ethical controls. It employs lawfare and ignores intellectual property laws in its efforts to gain advantage. Current US capabilities suffer given the lack of basic reconnaissance and awareness that would inform effective responses.
- **Improve anti-access/area denial (A2/AD) response capabilities. These may be technological or otherwise in character**, the latter possibly including deception, improved and expanded partner intelligence agreements, quantitative advantages gained via alliances, and deterrence.

Leadership and Education-related Recommendations

- **Avoid institutional hubris such as an unquestioning belief that US Army equipment, soldiers, and their leaders are the world's best, as is the force in terms of maneuver.** Cyber, artificial intelligence, information operations, human performance engineering, and other fields are already contested spaces. China is also actively seeking to improve its combat proficiency. Overconfidence and failures to adapt to evolving operational environments saw world leaders like Polaroid and US automobile manufacturers outmaneuvered and left behind by hungrier and more alert industry competitors. Reliance on the status quo and outdated assumptions exposes the Army to similar marginalization.
- **Enhance the theoretical and conceptual components of military education and expand its audiences.** Educating service members alone is not sufficient if we are to meet the demands of national security. Ours is an environment in which soldiers, their family members, and American society at large are targets of misinformation, disinformation, and mal-information. A sample of threats includes messages falsely informing spouses and parents of a service member's death, fabricated rumors of a leader's immoral behavior, invented reports of American atrocities, and realistic but fabricated visual evidence portraying US forces in the worst light (deep fakes). Even the aware will sometimes find it difficult to establish falsehood or ignore apparently legitimate "evidence." Failure to educate likely subjects before attacks virtually ensures adversary success.
- **Employ effective mission command.** Today's operational environment requires a breadth of expertise exceeding any one individual's ability to grasp its entirety. Understanding much less systematically orchestrating military, economic, information, cyber, diplomatic, political, technological, and other elements in that space requires clear mission and intent statements and decentralized decision-making by those most able and well-informed. Maintaining cross-domain and overarching context for decision-makers will prove a challenge at every echelon.
- **Maintain alliances even when not fighting.** The Army should play a primary role in alliance and coalition maintenance. That many regional countries' militaries are land force-heavy makes Army leadership particularly appropriate in this regard.
- In cooperation with allies and partners, **develop plans and priorities identifying where the collective whole of US national and international security should be in ten years.** Include difficult issues such as technology-sharing policies. Retain operational flexibility via forward basing, thereby taking advantage of partner nations' presence in and familiarity with contested regions. Such cooperation will be notably important when adversaries employ surrogate warfare.
- **Think like an insurgent.** Adopt more asymmetric mindsets when considering threats to national security. Identify adversary weaknesses and determine how we can undermine their strengths.
- **Ensure leaders and plans include a thorough understanding of antagonists' moral perspectives and spectrum of non-kinetic capabilities they employ.** The introduction and continued maturation of disruptive strategies brings with it a multitude of ethical and moral dilemmas in addition to operational conundrums. The Army will be challenged with defining rules of engagement; ethical boundaries; and research, development, and operating policies that meet the demands of national security while not violating American standards of conduct.
- **Increase the strategic IQ of the US military** across the force. Regional allies and partners, to include those in industry and the non-profit worlds, will be fundamental to better planning, training, and operational execution, a situation requiring a more effective strategic approach to security cooperation.

Personnel-Related Recommendations

- **Incorporate soldier talents developed pre-recruitment or during off-duty hours,** thereby allowing leaders to draw on needed skills when planning or during operations that require faculties otherwise unavailable in insufficient numbers.
- **Find a way to allow Americans to support and defend their country in non-traditional ways.** Allowing remote work; waving physical conditioning, grooming, and work-hour standards; and providing for part-time service without fixed commitments are among the adaptations that could dramatically expand the pool of individuals able and willing to lend their talents to national security.
- **Better incorporate generational considerations in personnel management innovations.** Closing gaps between generations will be as important as doing so between the public and private sectors. This will require older generations currently occupying most leadership positions to be open to the ideas and expectations of incoming generations.

Facilities-Related Recommendations

- **Address expanded threats to installations and potential off-installation targets.** Cyber and information attacks will accompany physical strikes. Command and control systems may be denied or compromised, confounding mobilization and deployment. Targets will include soldier loyalty and family and local citizens' support. Overseas bases will likewise be exposed to such assaults, complicating basing agreements.

Policy Recommendations

- **Facilitate innovation, to include addressing acquisition shortfalls and taking steps to better allow companies less familiar with Department of Defense (DOD) procedures to present their ideas or products.** Participants in the 2021 Campaign of Learning uniformly acknowledged the need to address (1) shortfalls in a dangerously lethargic US government acquisition process, (2) unresponsive Cold War-era policies and regulations, and (3) hyper-cautious contracting procedures. Current client-provider relationships will continue to be appropriate for some military-industry dealings. Something akin to commercial partnerships otherwise promise greater effectiveness, particularly when seeking to redress antiquated government processes that fail to take advantage of those proven in the commercial arena.
- **Encourage project leaders to act when they recognize failing or suboptimal ongoing work.** Current formal and informal incentive (to include promotion) structures favor the status quo and staying-the-course rather than disrupting in-progress projects even when inefficiencies or shortfalls in effectiveness become apparent.
- **Avoid fixation on threats posed by China, Russia, and North Korea at the expense of broader readiness.** This is notably the case in the Indo-Pacific region where distances and current national security concerns conspire to leave other threats and opportunities underappreciated. Army multinational partnerships, again those in the Indo-Pacific region in particular, would benefit from a shared focus on defeating A2/AD systems.
- **Establish a common cyber operating picture.** General Alexander called for the establishment of a cooperative, common government-commercial operating picture that would provide all participants with a shared understanding of cyber threats in real time. A similar approach would assist in confronting IO threats.
- **Review and, if necessary, revise policies regarding DOD and other US government agency restrictions regarding communications with Americans when those restrictions prevent citizen education on countering threat IO efforts.** Providing US citizens critical thinking skills and educating them regarding the potential negative effects of social media and ways to mitigate those effects is a challenge of particular significance, one with which the Army and DOD more broadly can help. Reevaluation of standing restraints merits consideration.

APPENDIX 4

VIP Panel Member Biographical Sketches

General (United States Army, retired) Keith B. Alexander, founder and CEO of IronNet Cybersecurity, one of the foremost authorities on cybersecurity in the world. A four-star Army general, GEN Alexander was previously the highest-ranked military official of USCYBERCOM, NSA/CSS, where he led these DOD agencies during the conflicts in Afghanistan and Iraq when attempted cyberattacks against the US were on the rise. In recognition of cyber's increasing importance, President Barack Obama and Defense Secretary Robert Gates appointed GEN Alexander as the first commander of USCYBERCOM, a newly created military institution charged with defending the nation's security in cyberspace against sophisticated cyber threats to businesses and government operations in an increasingly interconnected world. A leader with vision and a pragmatic approach to tackling the ever-changing cyber threat landscape, GEN Alexander built IronNet to bring this knowledge and experience to the private sector and fill in a critical gap between cyber threats and available security technology. IronNet provides best-in-class cyber defense based on complex behavioral modeling, big-data analytics, and advanced computing capability. GEN Alexander holds a B.S. from the US Military Academy, an M.S. in business administration from Boston University, and M.S. degrees in systems technology, physics, and national security strategy.

Dr. James Canton is a global futurist, social scientist, and advisor to business and governments. He is chairman and CEO of the Institute for Global Futures, a leading San Francisco-based think tank and global advisory firm he founded in 1990. He has worked with three White House administrations in advancing investments in future science and technologies. His firm has advised over 100 governments and organizations around the world on global trends, operations, global risks, and tech innovations. He directs the Global Risk Analytics and Innovation Strategy practice, which focuses on advanced science and technology innovations that impact markets, society, and global security. He advises Fortune 100 corporations and governments worldwide on trends and global strategy in innovation, health care, work, climate, energy, security, and demographics. The company analyzes advanced and emerging sciences and their impact on security, markets, and society. Specific technologies include nanoscience, neuroscience, bioscience, geo-intelligence, convergent technologies, data science, information, and network science.

Dr. Canton has conducted forecasting projects, collaborations, and advisory work for leading global companies including HP, Google, Cisco, IBM, Apple, UPS, GE, Siemens, General Mills, Philips, and McKinsey. He has conducted advisory work, forecasting briefings, and projects for a wide range of defense, intelligence, and state department clients including USSOCOM, CYBERCOM, SPACECOM, ODNI, Proteus, the US Army War College, US Air Force, Pentagon Futures Group, Lawrence Livermore Labs, Sandia Labs, US State Department, US Navy War College SSG, and USSOCOM University. Areas he has specialized in working with his government clients: The future of artificial intelligence, big data, analytics, cyber war, autonomous systems, dark networks, bio-nano-IT convergence, global threat rogue scenarios, threat finance, emerging science and technology uses for innovations in security, energy, communications, commerce, and digital finance.

Dr. Canton was the first private sector advisor for the US government on nanoscience and nanoengineering when he was appointed to the National Science and Technology Council (NSTC) in 1999. These efforts led to the National Nanotechnology Initiative. He has been involved in additional security and technology projects across US administrations for the President's Council of Advisors on Science and Technology (PCAST) and the White House Office of Science and Technology (OSTP). Prior to this he had worked in high tech startups (AI, computing, Internet), investment banking, and policy development for the US government between 1978-1980. He was an executive at Apple Computer from 1981-1984 where he worked on the development and introduction of the Macintosh computer, conducted strategic forecasting and business development, and forecasted the emergence of artificial intelligence working with government and private sector companies. From 1985-1990 he was engaged in high tech and investment startups in the Bay Area. He co-founded and was CEO at UmeCorp, one of the first artificial intelligence companies working in industrial controls and virtual reality platforms for NASA, Ford, and both Asian and European clients. He went on to be a serial entrepreneur working with Internet, mobile, and AI companies engaged in Silicon Valley. He was a partner at Swiss Occidental, an investment-banking group, where he worked on global investments, cross border transactions, and trade finance for multinational clients.

Dr. Canton has been an advisor to the National Science Foundation, Research Visionary Board, Motorola Research, MIT's Media Lab, EU, International Advisory Council, Economic Development Board, and state of Singapore. He was a fellow at the Neurotechnology Center at the Potomac Institute and Founding Advisory Board member and Co-Chairman, Futures Forecasting Track, Singularity University at NASA. Dr. Canton was also Senior Fellow at the Center for Research in Technology & Innovation at Kellogg School of Management. He is the author of the books *Future Smart* (2015), *The Extreme Future* (2007), and *Technofutures* (1998). He is a frequent guest of the media and is a commentator on Fox, CNBC, PBS, and CNN as well as for *Forbes, Fortune,* and *The New York Times.*

Lieutenant General (United States Marine Corps) Dennis A. Crall currently serves as the director for Command, Control, Communications, and Computers/ Cyber and chief information officer, Joint Staff J6. Recent assignments include deputy principal cyber advisor/senior military advisor for Cyber Policy; and director – Command, Control, Communications, Computers (C4), Headquarters Marine Corps/chief information officer (CIO) of the Marine Corps.

Lieutenant General Crall is a native of South Carolina where he graduated from the University of South Carolina. He is a career aviation command and control officer who has commanded at the squadron and group levels. He deployed as the Direct Air Support Center – Airborne, officer-in-charge in support of OIF conducting 34 combat missions spanning over 350 flight hours.

Joint assignments include: Deputy principal cyber advisor/ senior military advisor for Cyber Policy; Chief, Joint Cyberspace Center, US Central Command (CENTCOM); executive officer to the Deputy Commander, CENTCOM; division chief, Information Operations, CENTCOM; division chief, Developments and Concepts, CENTCOM; branch chief, Strategic Plans, Information Operations, US Special Operations Command (SOCOM); and joint liaison officer to the 7th Air Force, 607th Air Support Operations Group in Osan, Korea.

Supporting assignments include director – Command, Control, Communications, Computers (C4), Headquarters Marine Corps/chief information officer (CIO) of the Marine Corps; Marine Corps Recruiting Command, operations officer, Recruiting Station Albuquerque, NM; and contact team officer, 6th Marine Corps District, Parris Island, SC.

Lieutenant General Crall is a graduate of the Marine Corps Command and Control Systems Course; a distinguished graduate of the US Air Force Air Command and Staff College where he earned an M.S. in military operational art and science; and a distinguished graduate of the National War College where he earned an M.S. in national security strategy. He has also completed the Harvard Kennedy School Cybersecurity Executive Program.

The Honorable Michèle A. Flournoy is co-founder and managing partner of WestExec Advisors, and former co-founder and chief executive officer of the Center for a New American Security (CNAS), where she currently serves on the board.

Michèle served as the Under Secretary of Defense for Policy from February 2009 to February 2012. She was the principal advisor to the Secretary of Defense in the formulation of national security and defense policy, oversight of military plans and operations, and in National Security Council deliberations. She led the development of the Department of Defense's 2012 Strategic Guidance and represented the department in dozens of foreign engagements, in the media, and before Congress.

Prior to confirmation, Michèle co-led President Obama's transition team at the Defense Department.

In January 2007, Michèle co-founded CNAS, a bipartisan think tank dedicated to developing strong, pragmatic, and principled national security policies. She served as CNAS's president until 2009 and returned as CEO in 2014. In 2017, she co-founded WestExec Advisors, a strategic advisory firm.

Previously, she was senior advisor at the Center for Strategic and International Studies for several years and, prior to that, a distinguished research professor at the Institute for National Strategic Studies at the National Defense University (NDU).

In the mid-1990s, she served as principal deputy assistant secretary of defense for strategy and threat reduction and deputy assistant secretary of defense for strategy.

Michèle is the recipient of numerous honors and awards, including the American Red Cross Exceptional Service Award in 2016; the Department of Defense Medal for Distinguished Public Service in 1998, 2011, and 2012; the Chairman of the Joint Chiefs of Staff's Joint Distinguished Civilian Service Award in 2000 and 2012; the Secretary of Defense Medal for Outstanding Public Service in 1996; and CARE's Global Peace, Development, and Security Award in 2019. She has edited several books and authored dozens of reports and articles on a broad range of defense and national security issues. Michèle appears frequently in national and international media, including CNN's *State of the Union,* ABC's *This Week*, NBC's *Meet the Press*, BBC News, NPR's *Morning Edition* and *All Things Considered,* and PBS's *News Hour*, and is frequently quoted in top tier newspapers.

Michèle serves on the boards of CNAS, Booz Allen Hamilton, Amida Technology Solutions, The Mission Continues, Spirit of America, and CARE. She serves on the advisory boards PIMCO and Opentrons, and on the honorary advisory committee of The Leadership Council for Women in National Security. Michèle is also a former member of the President's Intelligence Advisory Board, the CIA Director's External Advisory Board, and the Defense Policy Board, and is currently a member of the Council on Foreign Relations and the Aspen Strategy Group, and is a senior fellow at Harvard's Belfer Center for Science and International Affairs.

Michèle earned a bachelor's degree in social studies from Harvard University and a master's degree in international relations from Balliol College, Oxford University where she was a Newton-Tatum scholar.

Lieutenant General (US Army, retired) Paul E. (Butch) Funk: Lieutenant General (Retired) Paul E. Funk is presently employed by the National Mounted Warfare Foundation as the president and chief executive officer. He is also a member of the National Mounted Warfare Foundation Board of Directors.

General Funk was born in Roundup, MT. He holds a Doctorate of Education and Masters in psychological counseling from Montana State University. He earned Distinguished Military Graduate honors from Montana State University where he was commissioned a second lieutenant. His basic military education includes Armor Officer Basic and Armor Officer Advanced Course, Helicopter Flight School, the Armed Forces Staff College, and the Army War College.

General Funk has held a variety of command positions from platoon through division, leading to his assignment as the Commanding General, III Corps and Fort Hood, TX. He served as the commanding general of the US Army Armor Center and Fort Knox, KY from June 1992 to October 1993. He commanded the 3rd Armored Division, United States Army, Europe from December 1990 to April 1991 when the division distinguished itself as part of the VII Corps during Operations Desert Shield and Desert Storm in Saudi Arabia, Kuwait, and Iraq. He was the commanding general of the National Training Center and Fort Irwin, CA; assistant division commander, 9th Infantry Division (Motorized), Fort Lewis, WA; Commander of the 194th Separate Armored Brigade; and 5th Battalion, 33rd Armor, Fort Knox, KY.

Prior assignments at Fort Hood include Deputy G3 for Training; III Corps; chief of staff, 1st Cavalry Division; and several platoon leader assignments with the 2nd Battalion, 13th Armor and 1st Armored Division.

Other key assignments include vice director, J3, the Joint Staff, Washington, D.C. and assistant commandant, US Army Armor School, Fort Knox, KY. General Funk served a combat tour in Vietnam as executive officer and then commander of Troop A, 1st Squadron, 9th Cavalry, 1st Cavalry Division. He commanded four companies/troops and led three platoons. General Funk has also served in the Republic of Korea.

His awards and decorations include the Distinguished Service Medal (with two Oak Leaf Clusters), Defense Superior Service Medal, Legion of Merit (with two Oak Leaf Clusters), Distinguished Flying Cross, Bronze Star Medal (with two Oak Leaf Clusters), Meritorious Service Medal (with three Oak Leaf Clusters), Air Medal with "V" device and (twenty-five Oak Leaf Clusters), Army Commendation Medal with "V" device and (three Oak Leaf Clusters), Vietnam Service Medal (with three Oak Leaf Clusters), Kuwait Liberation Medal, Saudi Service Medal (with three bronze stars), the Army Aviator Badge, and the Joint Chief of Staff Identification Badge. He was selected as one of the top 100 graduates in the first 100 years from Montana State University. In 1998, he was awarded an Honorary Doctorate of Engineering from Montana State University.

Previously, General Funk worked as the vice president of Middle Eastern Operations for General Dynamics in Riyadh, KSA and later as the vice president for Services for General Dynamics Land Systems in Sterling Heights, MI. Recently, General Funk worked as director for the Education and Technology Applications Division at the University of Texas at Austin Institute for Advanced Technology where he was also a member of the Army Science Board.

Lieutenant General (Retired) Funk and his wife Danny have three children: GEN Paul E. Funk II (the current Commanding General of US Army Training and Doctrine Command), James Funk, and Becky Clonts. The Funks are proud grandparents to eight grandchildren and are great-grandparents to one great-grandchild, Jack.

- Member of the National Board of the American Hereford Association for four years.
- In 1992, selected as a "Significant Sig" by the National Fraternity of Sigma Chi.

Vice Admiral (United States Navy, retired) Robert Harward is the chief executive (CE) for Lockheed Martin Middle East and has lived in Abu Dhabi for seven years. In his role as CE, he is responsible for all aspects of the company's business in UAE, Bahrain, Kuwait, Oman, Jordan, Lebanon, Qatar, Pakistan, Iraq, and Afghanistan, including strategy, operations, and profitable growth of Lockheed Martin business. He was recognized by Forbes (October 2019) as one of the fifty (#10) most influential CEO's in the Middle East.

A national security expert in both theory and application, he served on the National Security Council for the Bush administration, commissioned the National Counter Terrorism Center, and has extensive combat experience as a US Navy SEAL in Afghanistan and Iraq. (He led invasions in both countries in October 2001 and March 2003.) His combat experiences also include Syria, Somalia, Yemen, and Bosnia as well as the rest of the Middle East. He was asked by President Trump to serve as his national security advisor. A US Naval Academy alumni, he holds a master's degree in international security affairs and is a graduate of the Naval War College and the MIT Foreign Policy Program. He also served as an executive fellow at RAND. Prior to joining Lockheed Martin, he was a Vice Admiral (SEAL) in the United States Navy with his last assignment as deputy commander, US Central Command (USCENTCOM). Mr. Harward grew up in Iran, graduated from the Tehran American School, and speaks Farsi.

Mr. Harward's significant recognitions include the Donovan Award from the CIA, the Distinguished Service Award from the Department of State, the German Silver Star, and the Polish Silver Star. He was designated a Commander of the Polish GROM (Special Operation Forces). The Department of Defense awarded him the Defense Distinguished Service Medal (three), the Navy Distinguished Service Medal, the Bronze Star with V device (four), and the Presidential Unit Citation (two) for combat operations in Afghanistan and Iraq. He was also recognized with the US Naval War College Distinguished Graduate Leadership Award.

Aside from his responsibilities with Lockheed Martin, Bob served on the Secretary of Defense Threat Reduction Advisory Committee (TRAC) where he chaired the Counter Weapons of Mass Destruction Task Force. He is an advisor to Draper Labs, adjunct to RAND, and sits on several commercial boards to include Channel, USAA REALCO, and Shield AI. On the personal side, Bob is a professional parachutist, performing around the world, and enjoys all forms of physical and intellectual competition, particularly chess, racquetball, golf, and squash. He set the world record for the highest parachute landing on the West Col Base Camp of Mount Everest at over 23,000 feet on October 27, 2019.

General (United States Air Force, retired) James M. Holmes retired from the US Air Force in October 2020 after nearly 40 years of service. He is a member of the Council on Foreign Relations, an adjunct fellow at the Center for a New American Security, a senior advisor at The Roosevelt Group, Chairman of the Board at Red 6, and advises several defense and tech companies.

He completed his Air Force service leading the transformation of Air Combat Command (ACC), a global organization operating and sustaining over 1000 aircraft and eleven Air Force bases with an annual operating budget of $7.4 billion. As the Air Force's deputy chief of staff for Strategic Plans and Programs, he led a team that shifted Air Force strategy to respond to a new national security environment and built and defended the USAF's input to three $600 billion Five Year Defense Plans with the Department of Defense and US Congress. As the Deputy Commander of Air Education and Training Command, he directed all aspects of USAF education and training, from basic and technical training to advanced degree programs. As the Air Force's assistant deputy chief of staff for Operations and Requirements, he coordinated global Air Force operations and requirements with the Joint Chiefs of Staff and regional military commanders. As principal director for Mid-East Policy in the Office of the Secretary of Defense, he formulated regional defense policy with the National Security Council and Department of State and coordinated US defense relationships and activities with international partners. Before assuming his strategic roles, he commanded Air Force teams in positions of increasing complexity, responsibility, and accountability at the squadron, group, and wing level, including a year in command of Air Force forces in Afghanistan.

Mike graduated from the US Naval War College National Security Strategy program with highest honors and completed both the US Air Force's School for Advanced Air and Space Power Studies program and the Fighter Weapons Instructor Course. He was the Graduate of the Year in the University of Alabama's MA in history program at Maxwell AFB and received a BS in electrical engineering from the University of Tennessee. He is a fighter pilot with over 4,000 hours in the F-15 and T-38, including over 500 combat hours, and continues to fly general aviation aircraft.

Mr. John M. Pulju has served as acting chair of the National Intelligence Council since May 2020. He served as deputy assistant director of CIA for Counterterrorism from January 2017 until joining the NIC in early 2020. Previous management assignments of note include chief of analysis for CTC, director of the DNI's PDB staff, and director of the Office of Iraq Analysis. He joined the CIA in 1984 as arms transfer analyst, focusing on Soviet exports and the gray arms market. He has supervised units covering these topics as well as a range of terrorist, illicit finance, sanctions, and related issues.

Lieutenant General United States Marine Corps (Retired) Paul K. Van Riper considers himself a close friend of the US Army. He is a graduate of the Ranger and Airborne schools as well as the Army War College. He additionally served as an instructor in the former JFK Institute for Military Assistance, Fort Bragg, NC; has consulted for TRADOC on a number of projects since retirement; and participated in Army Title X wargames for ten years. He retired from the United States Marine Corps in October 1997 after more than 41 years of commissioned and enlisted service. During those years, he was assigned to a variety of command and staff billets at posts and stations around the world.

In seven tours in the Fleet Marine Force, he served in each of the three active divisions. Lieutenant General Van Riper participated in or observed combat operations during five tours.

Lieutenant General Van Riper commanded the Marine Barracks in Cecil Field Florida; 2nd Battalion, 7th Marines; 4th Marine Regiment; and 2nd Marine Division. He was director of Marine Corps Command and Staff College, served as the first president of Marine Corps University, was assistant chief of staff for Command and Control, and director of intelligence at Headquarters Marine Corps. In his last tour, he was commanding general, Marine Corps Combat Development Command.

Lieutenant General Van Riper is a graduate of the Marine Corps Amphibious Warfare School and Navy's College of Command and Staff.

His personal decorations include the Distinguished Service Medal, Silver Star Medal with gold star in lieu of a second award, Legion of Merit, Bronze Star Medal with Combat "V," Purple Heart, Meritorious Service Medal, Joint Service Commendation Medal, Army Commendation Medal, Navy Achievement Medal, and the Combat Action Ribbon with gold star.

Since retiring, Lieutenant General Van Riper has remained active within the national security community. He held teaching chairs at Marine Corps University for eleven years.

APPENDIX 5 Glossary

A2/AD	anti-access/area denial
ACC	Air Combat Command
AI	artificial intelligence
APAN	All Partners Access Network
ASEAN	Association of Southeast Asian Nations
B.S. or BS	Bachelor of Science
BRI	Belt & Road Initiative
C2	command and control
C4	command, control, communications, and computers
CE	chief executive
CEO	chief executive officer
CG	commanding general
CIA	Central Intelligence Agency
CIO	chief information officer
CNAS	Center for New American Security
COVID-19	coronavirus of 2019
CSS	Central Security Service
CTC	Counterterrorism Center
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNI	Director of Naval Intelligence
DoD or DOD	US Department of Defense
DOE	Department of Energy
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities-policy
EU	European Union
EW	electronic warfare
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FM	field manual
FOE-AI	Future Operational Environment-Artificial Intelligence
G-2	intelligence section in a single service headquarters commanded by a general officer
GDP	gross domestic product
GEN or Gen	general
HP	Hewlett Packard
IC	intelligence community
IED	improvised explosive device
IoT	Internet of Things
IQ	intelligence quotient
IT	information technology
J6	command, control, communications, and computers/cyber staff section of a joint headquarters
JADC2	Joint All-Domain Command and Control
KSA	Kingdom of Saudi Arabia

KSB-P	knowledge, skills, behaviors and preferences
LTG	lieutenant general
LtGen	lieutenant general
M.S. or MS	Master of Science
MDO	Multi-Domain Operations
MIT	Massachusetts Institute of Technology
MOS	military occupational specialty
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCO	non-commissioned officer
NDU	National Defense University
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSTC	National Science and Technology Council
NTSB	National Transportation Safety Board
ODNI	Office of the Director of National Intelligence
OE	operational environment
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OSTP	Office of Science and Technology
PCAST	President's Council of Advisors on Science and Technology
PDB	President's daily brief
PLA	People's Liberation Army
PMSC	private military and security companies
RD&D	research, development, and demonstration
SAMS	School of Advanced Military Studies
SEAL	sea, air, land: a US Navy special operations capability
SFAB	Security Force Assistance Brigade
SPACECOM	US Space Command
SSG	strategic studies group
TP	TRADOC pamphlet
TRAC	Threat Reduction Advisory Committee
TRADOC	US Army Training and Doctrine Command
TSA	Transportation Security Administration
UAE	United Arab Emirates
UAS	unmanned aerial system
UAV	unmanned aerial vehicle
U.S. or US	United States
USCENTCOM	United States Central Command
USCYBERCOM	US Cyber Command
USSOCOM	US Special Operations Command
USSR	Union of Soviet Socialist Republics
UxS	unmanned systems
VADM	vice admiral
VIP	very important person
WWII	World War II

NO. 21-665
October 2021