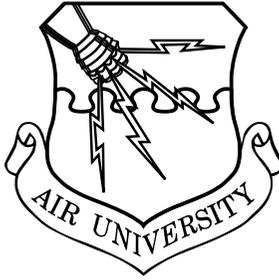


HUMAN, MACHINE, WAR

How the Mind-Tech Nexus Will
Win Future Wars



Edited by
Nicholas Wright, Michael Miklaucic, and Todd Veazie



Human, Machine, War

How the Mind-Tech Nexus Will Win Future Wars

EDITORS

NICHOLAS WRIGHT

MICHAEL MIKLAUCIC

TODD VEAZIE

Air University Press
Maxwell Air Force Base, Alabama

Air University Press

Director

Dr. Paul Hoffman

Acting Managing Editor

Donna Budjenska

Design and Production Managing Editor

Luetwinder T. Eaves

Project Editor

Jeanne K. Shamburger

Cover Art, Book Design, and Illustrations

Catherine Smith

Print Specialist

Jonathan Marks

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010

<https://www.airuniversity.af.edu/AUPress/>

Facebook: <https://www.facebook.com/AirUnivPress>

Instagram: https://www.instagram.com/air_university_press/

LinkedIn: <https://www.linkedin.com/air-university-press>

X: <https://x.com/aupress/>



Names: Wright, Nicholas, 1978-editor. | Miklaucic, Michael, 1954-editor. | Veazie, Todd, 1964-editor. | Air University (U.S.). Press, issuing body.

Title: Human, machine, war : how the mind-tech nexus will win future wars / editors: Nicholas Wright, Michael Miklaucic, Todd Veazie.

Other titles: How the mind-tech nexus will win future wars

Description: Maxwell Air Force Base, Alabama : Air University Press, 2025 | In scope of the U.S. Government Publishing Office Cataloging and Indexing Program (C&I); Federal Depository Library Program (FDLP) distribution status to be determined upon publication. | Includes bibliographical references.

Identifiers: LCCN 2025007577 (print) | LCCN 2025007578 (ebook) | ISBN 9781585663347 (paperback) | ISBN 9781585663347 (Adobe pdf)

Subjects: LCSH: Human-computer interaction. | Human-computer interaction—United States. | Military art and science—Technological innovations. | Military art and science—Technological innovations—United States. | Technology—United States—21st century. | Artificial intelligence—Forecasting. | War—Forecasting.

Classification: LCC QA76.9.H85 (print) | LCC QA76.9.H85 (ebook) | DDC 004.019—dc23/eng/20250224 | SUDOC D 301.26/6:H 88

LC record available at <https://lccn.loc.gov/2025007577>

LC ebook record available at <https://lccn.loc.gov/2025007578>

Published by Air University Press in April 2025

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the official policy or position of the organizations with which they are associated or the views of the Air University Press, Air University, United States Air Force, Department of Defense, or any other US government agency.

This publication is cleared for public release and unlimited distribution. Reproduction and printing are subject to the Copyright Act of 1976 and applicable treaties of the United States. This document and trademark(s) contained herein are protected by law. This publication is provided for noncommercial use only. The author has granted a nonexclusive, royalty-free license for distribution to Air University Press and retains all other rights granted under 17 U.S.C. §106. Any reproduction of this document requires the permission of the author.

This book and other Air University Press publications are available electronically at the AU Press website at <https://www.airuniversity.af.edu/AUPress>. The appearance of US Department of Defense (DOD) visual information does not imply or constitute DOD endorsement.

Contents

Foreword	<i>vii</i>
<i>GEN James E. Rainey, USA</i>	
Foreword	<i>xi</i>
<i>Sir Lawrence Freedman</i>	
Introduction	<i>1</i>
<i>Nicholas Wright</i>	
<i>Michael Miklaucic</i>	
<i>Todd Veazie</i>	

PART 1

THE MIND-TECH CRUCIBLE: INNOVATION AND ETHICS

1 The Mind and the Machine: Combating Automation Bias and Crafting Effective Human-AI Teams on the Battlefield	<i>29</i>
<i>Lauren Kahn</i>	
2 Accessing the Brain to Affect the Mind: Neuroethics of the Mind-Tech Nexus in Military Contexts	<i>39</i>
<i>James Giordano</i>	

PART 2

COMMAND, CONTROL, AND INTELLIGENCE IN THE NEW FOG OF WAR

3 Intelligence and the Mind-Tech Nexus: History and Futures	<i>61</i>
<i>Sir David Omand</i>	
4 Emergent Operational Complexity and the Need for Human-System Synergy	<i>77</i>
<i>Andrew D. Gainer, Karl F. Van Orden, Jamie R. Lukos</i>	
5 Breaking the OODA Loop: Human-Machine Symbiosis to Manage Complexity and Accelerate Decision-Making as a Decisive Warfighting Advantage	<i>91</i>
<i>Timothy Grayson</i>	

6 Mind-Tech Teaming in Defense: Integration and Imagination	117
<i>Michael Groen</i>	

7 Artificial Intelligence and Perception in Crisis and Conflict: Mating Twenty-First-Century Technologies with Eighteenth-Century Minds	127
<i>Jack Shanahan</i>	

PART 3

PERFORMANCE ENHANCEMENT

8 Enhancing the Humans in the Mind-Tech Nexus	151
<i>Nicholas Wright</i>	

9 Physiologic Intelligence (PHYSIOINT): A Framework for Assessing Warfighter Sustainment and Performance Improvement Using Physiological and Neurobiological Signals	181
<i>William D. Casebeer</i>	

10 Making Sense of Wearable Sensing: A Principled Approach to Quantifying Human Physiological, Cognitive, and Behavioral Attributes	193
<i>David Huberdeau</i>	

PART 4

CHINESE AND RUSSIAN MIND-TECH

11 The Case of Russia	211
<i>Samuel Bendett</i>	
12 The People's Liberation Army at the Nexus of Mind and Technology to Shape the Cognitive Battlefield	223
<i>Josh Baughman</i>	

PART 5

THE QUESTION OF WILL AND SUPPRESSION OF PERFORMANCE

- 13 First the Mind, Then the Tech: Focusing on the Human Aspect of the Mind-Tech Nexus for Improved Investments** 243
Ben Connable
- 14 The Will to Fight as a Complex System: A Research Agenda for the Employment of Neuroscience in Military Organizations** 261
Aaron B. Frank
- 15 Degrading the Performance of Humans in the Mind-Tech Nexus** 291
Nicholas Wright

PART 6

CONCLUSIONS FROM HUMANS—AND CONCLUSIONS FROM MACHINES

- 16 Conclusions Written by Three Humans** 323
Nicholas Wright, Michael Miklaucic, Todd Veazie
- 17 A New Beginning with Generative AI** 333
David Vernal
- 18 Conclusions Written by Generative AI** 339
Generative AI Prompted and Annotated by David Vernal
- Author Biographies** 359
- Acknowledgments** 371
- Index** 372

Foreword

No one can predict the future, but we can see the broad outlines. Changes in technology matter, but so do many other factors, like trends in politics, the climate, demographics, and the global economy. Plans for military transformation must account for the full range of variables.

Before we ask how warfare is changing, we should take stock of what is not changing. First, because war is a human endeavor, people matter most. Second, people live on land. Thus, while all domains are vital, armies must be able to seize and hold land. When they do, close combat is unavoidable. That means the ability to close with and destroy the enemy on land can be decisive. Finally, wars are unpredictable. No one can guarantee a war will be short or that it will not escalate. And, importantly, the United States abides by the Law of Armed Conflict. We will build our force accordingly.

At the same time, civilian and military technologies are changing at a pace not seen since before World War II. Information and communications technologies are revolutionizing how commanders get, manage, and use information. The proliferation of sensors and precision weapons means Soldiers are fighting on an increasingly transparent, lethal battlefield. We are approaching the time when AI-enabled robotic systems will face off at machine speed in battles where the software matters as much as the hardware. Meanwhile, military commanders at all echelons are learning to be attuned to the rapid interaction between battlefield events and the global information environment.

Because militaries are constantly adapting, new technology is rarely decisive in the ways people predict. But it is disruptive in that it changes how military forces operate, organize, and equip. The consequences of failure to adapt are severe. Technology will increase the punishment of unskilled commanders and untrained formations while creating opportunities for those skilled in its employment. Adaptation at intense velocity is leading to human-machine convergence, which this book calls the “Mind-Tech Nexus.”

To ensure the US military remains dominant, we must first sustain the asymmetric advantages we already have—our people and our competence in Joint and combined arms maneuver warfare. No military can compete with the US military on talent. We have a highly skilled, all-volunteer force. We produce high-quality leaders at scale—our noncommissioned officers are the envy of the world. Our culture of commander-centric planning and intent-based, decentralized execution

FOREWORD

makes us highly adaptable. Because of the way we train, the US military is without peer in Joint operations and maneuver warfare. The humans who execute command and control must effectively harness new technologies for managing information, such as artificial intelligence. By sustaining and building on those strengths, we will retain an advantage on an increasingly complex, fast-paced battlefield—regardless of how technology changes the mechanics of warfighting.

We must also develop the capability to fight with AI-enabled systems of systems, including human-machine integrated ground combat formations. The goal is not to replace humans with machines but to offload risk and work to machines. Doing so frees humans to do what they do best, including exercising judgement, deciding when to use lethal force, and practicing the art of command. We will develop this capability through formation-based transformation.

Formation-based transformation orients capability development on how people are organized, trained, *and* equipped—as a holistic solution. This approach is in sharp contrast to first orienting on equipment and later accounting for the human and other factors, such as organization and training. Thus, the best way to integrate technology is to put cutting-edge systems directly into our fighting formations. This strategy enables evolving technology to be useful today and mature in the laboratory of the real world.

In many cases, we are allowing the aspirational to stand in the way of the doable. There are technologies that would be helpful right now but are not yet fielded because we are waiting until they can do even more. New technologies with game-changing potential should be in operational units as soon as they are useful, even if only in small quantities of minimum-viable products. This paradigm accelerates development of the technology. But it also lets us learn how to best employ it, adapting organizations and training accordingly. Most importantly, it gives leaders experience using the technology as it evolves.

If a system is safe and, in the assessment of the leaders charged with its employment, useful enough to be worth the work of having, it is a candidate for fielding—at least to a few units. What we learn will then inform how formations are organized, trained, and equipped only a few years later. The result will be a continuously improving solution that integrates state-of-the-art technology quickly and discards bad ideas just as fast.

To dominate the ground, we must also dominate the air-ground littoral—the near-Earth space, up to thousands of feet. Formations

that can operate in the air-ground littoral can sense and strike further and faster. They can gain and maintain contact with large numbers of attritable systems, communicate over wider areas, and have new ways to achieve and sustain a vertical envelopment. The emergence of these formations may drive the biggest change in how we fight on land since armies learned to exploit the potential of mechanization.

We are not preparing for just a theoretical future fight. The competition among militaries to out-innovate one another is ongoing. With the onset of war, it only intensifies. Today, a military's ability to integrate new technology and transform during a war can matter as much as its form at the outset. Our commitment and sense of urgency come from our firm belief that a dominant US military makes a better and safer world.

The impact of technology on conflict and war is complex and dates from time immemorial, constantly forcing transformations in the character of conflict and war and a constant process of human adaptation. However, the digital revolution of recent decades has increased the velocity and scale of transformation to such a degree that the human side of the equation has struggled to keep pace. Human attitudes and behavior, law, ethics, processes, and institutions evolve more slowly. Yet it is precisely the quality of the interface between the human and the technology that determines how effective their pairing will be in conflict. This book examines the many facets of how humans interface and converge with technology, providing an important mapping of the Mind-Tech Nexus.

JAMES E. RAINEY
General, US Army
Commander, US Army Futures Command

Foreword

When considering the future of war, we naturally concentrate on how exciting technological developments might produce new forms of warfare. One way to frame any new technology's impact is recognizing that innovation is unlikely to push aside older capabilities; instead, it adds another layer to previous developments. Since the old rarely goes away but is complemented by the new, these many layers interact with each other. For example, on any given day in the Russo-Ukraine war, you could see activities recognizable from the First World War—from digging trenches to throwing grenades—and the close air support and armored thrusts of the Second World War. In addition, smart weapons first introduced in the 1970s ensured that a properly identified target could be hit. They became more effective with sensors that could find, identify, and track targets and with communications enabling vital information to be passed quickly to the operators. Lastly come the modern drones in all shapes and sizes, providing constant surveillance and a cheap form of firepower.

The interactions between the layers of technology produce a complexity that poses considerable command and control problems—leading to many of the issues addressed in this book. And it is in the midst of these dilemmas where AI comes in, sorting out options for commanders and hopefully presenting them in a form they can understand. In a case of defense against incoming missiles, operations must occur so quickly that only a machine can handle the urgent computations required to establish the trajectory of an incoming missile, what it might hit, what interceptors are available, and what commanders must do to destroy the missiles. This scenario demonstrates the sort of problem that AI is excellent at solving: relatively narrow and with plenty of information to help in its resolution. Yet many military problems are not narrow but complex, involving questions of priorities when allocating scarce resources and depending on information and communications networks that are not always reliable. In such situations, an understanding of the Mind-Tech Nexus—how humans and machines interface and converge—can provide an edge. The challenge for an effective human-machine interface is not just one of presentation and timeliness but, as with human-human interactions, also requires trust.

Getting the best out of machines is a problem people face every day. Digital technologies have transformed our ability to do once demanding or even impossible tasks. With a few taps, we can access information; communicate with family, friends, and even strangers; watch events in

FOREWORD

distant places unfold in real time; and determine where we are and how to get to where we want to be. Many of these capabilities were initially developed for the military but were then redeveloped for civilians in ways that turned out to be transformational.

Yet even as we take advantage of these amazing capabilities, many of us realize that our performance is often suboptimal. For instance, our smartphones and cars have features we do not know or fail to use properly. While we may be frustrated about being suboptimal, the potential gains from more effort can seem too marginal to be worth the bother. We can still get by, waiting for the manufacturers to upgrade their products so that we can become ever more optimal without having to make more of an effort.

But the upgrades can disappoint. Engineers can improve devices in many ways, some immensely satisfying to the designers, offering neat solutions to complex problems. However, these innovations may leave consumers unimpressed if what they really want is more reliability and a longer battery life. If customers are going to pay for upgrades, they expect engineers to consider their needs versus showcasing their technological wizardry. Those accustomed to living a suboptimal life can cope without fancy options they don't fully understand if the core functions perform as required. Trusted, reliable systems can be more valued than those that can do amazing things only if the operator has an advanced degree.

As with consumers, so too with the military. For an example, consider maps. Improvements in cartography during the eighteenth century were vital to the development of modern strategy. The ability to identify the most appropriate locations for set-piece battles and determine possible lines of advance and supply routes encouraged the original definitions of *strategy* as being about “war on the map”—getting an army to the fight (at which point tactics would take over). Doing so required intelligence not just on the enemy order of battle but also on topography to identify natural barriers to movement and find paths forward. Executing these tasks has become much easier since satellite imagery has transformed mapmaking over the last sixty years. Operations planners also benefitted from GPS satellite capabilities that enabled locating oneself on a map even while moving and so navigate a way through unfamiliar terrain. The value of this capability became apparent in Operation Desert Storm in February 1991 when US and UK divisions set off into the desert to mount the “left hook” to envelop Iraqi forces with confidence that they would not get lost.

Journalists embedded with the troops in 1991 were soon keen to get their own satellite navigation. With the Cold War over, there was less pressure to preserve this and other high-quality capabilities, from detailed imagery to easy communications, for military use. Consumers did not need much persuading of the value of navigational aids. No longer was it necessary to spend hours before a journey staring at maps and trying to identify the quickest route. To be sure there were teething problems, as drivers were directed into rivers or down one-way streets. When offered a route, experienced drivers would shake their heads and stick to what they knew. But the quality of the systems steadily improved. Eventually, drivers were not only told the optimum route to follow but could be warned while the journey was underway of roadwork and accidents ahead. The more the system could be trusted, the less the need for backups. There was no longer a market for printed road maps. Unfortunately, sometimes the system goes down, and the screens go dark—leaving us more helpless than before, especially if we are in an unfamiliar place.

What may be an unfortunate accident or some system malfunction in civilian life can be result of deliberate interference in the military sphere. As we have seen in the Russo-Ukraine war, a considerable amount of effort now goes into electronic warfare seeking to disrupt enemy communications. So it is not always possible to rely on the machines. When they suddenly become unavailable, it may be necessary to find innovative workarounds or to go back to the older systems and skills previously dismissed as obsolete but that can still get the job done.

Another difficulty with discussions about the future of war is that they tend to present warfare in terms of a contest between armed forces without much regard for the context in which it is taking place. The more attention paid to nonmilitary factors, the less the potential role for AI. Machines can tell you how to fight wars but not why. They can identify enemy vulnerabilities but not explain why they are enemies. They can help allies work together without being able to negotiate an alliance. They can describe a route to victory, but they cannot decide what constitutes a victory or what concessions might be worth making to get a negotiated deal if a victory remains out of reach. They can help armies advance against the enemy but not inspire soldiers to move into harm's way or ease their fears. They can make it easier to topple a regime or occupy an enemy but lack the skills to replace the overthrown regime or deal with a suspicious population.

Humans largely shape this wider political context for war, reflecting clashes of values and interests and opposing world views. Any

FOREWORD

discussion of innovation in the design and uses of machines must never forget this context. Out of it comes the tasks for the armed forces and the factors that shape the ability of the armed forces to meet them. The advantages gained by a brilliant technological innovation might be lost through poor training or shoddy manufacturing, squandered by a sloppy peace negotiation, or neutralized by the enemy forging a new alliance. The political context introduces variables that can make any attempt to model future combat impossible. It is therefore understandable that the modeling must keep the focus narrow and manageable. But doing so can lead to scenarios framed too narrowly. When the aim is to understand how humans interact with the machinery of warfare, we need to keep this context firmly in mind.

As machines extend human power, those contemplating war must recognize the limits of the possible extension and how the enemy can respond. The essays in this book are largely about this process of extending power. They show how this extension is becoming less a matter of simply improving the range and lethality of weapons. Rather, it is more about the intelligent direction of fire made possible by a better appreciation of the battlespace and grasp of the available capabilities on both sides. It is therefore about how machines can speed up and sharpen human decision-making through their ability to get more and better information about the operational environment. In this, the humans and the machines will each be changed by the other as they converge over time. The essays also point to areas where machines can reshape the wider context if they can spread propaganda or engage in sabotage. Here, even more than with specific military functions, engineers must involve customers who provide input about their needs. The effectiveness of information campaigns and cyberattacks requires knowledge of the societies they are intended to influence. With the full potential of AI only starting to be realized, it is unsurprising that the ethical challenges posed dominate much of the debate. These challenges need addressing, but as the essays in this book make clear, reaching full potential is not straightforward, and the limitations of humans will also limit the impact of AI.

SIR LAWRENCE FREEDMAN
Emeritus Professor of War Studies
King's College London

Introduction

*Nicholas Wright, Georgetown University,
University College London, and Center for Strategic and
International Studies*

Michael Miklaucic, National Defense University

*Todd Veazie, Director, Strategic Multilayer Assessment,
Joint Staff*

In the 1920s and '30s, German military professionals like tank commander Heinz Guderian asked how the human factors of shock, creativity, guile, will, daring, and skill could be combined with the technology of their time to win wars. He was referring not just to machines but to minds plus machines in dynamic complementarity. For instance, how could they interface and converge, use armor en masse to surprise an enemy, or employ radio communications to think and decide faster than an enemy? In May 1940, Germany's blitzkrieg, or lightning war, catastrophically defeated the British and French armies. And while German effectiveness created the opening, Germany achieved a decisive overmatch against an enemy with more trained men, guns, tanks, and planes in large part because French will collapsed.

Throughout the post-World War II period, the United States relied heavily on superior technology to offset Soviet overmatch in conventional forces and geographic advantage. The first strategic offset depended on nuclear weapons to deter Soviet and Warsaw Pact aggression in Europe. The Soviet Union, then the People's Republic of China, and soon several others rapidly developed their own nuclear armories leading to the second strategic offset—precision strike capabilities displayed with great strategic impact during the 1991 Gulf War. The third offset strategy, initiated in 2015, prioritized concepts about cutting-edge technology—such as artificial intelligence (AI), cyber capabilities, and unmanned systems.¹ The US planned to use these technologies to counter Russian and Chinese military advances and buildup—particularly within the two countries' respective regional contexts—which directly threaten key allies and partners.

Early twenty-first-century America has the world's best technology—but it spent some two trillion dollars in Afghanistan and could not defeat the Taliban.² The Taliban lacked high-end technology but had

enough skill with their tools—and will—to emerge victorious. America now faces bigger challenges from great power competitors with groundbreaking technologies and relentless drive to supplant the liberal, rules-based global order. Prevailing in this competition cannot be taken for granted. The Western powers would be unwise to assume that our technological superiority alone will secure our strategic aims in conflict or achieve sustainable outcomes over the longer horizon. Russia is pioneering the use of drones, social media, and AI to exploit cognitive vulnerabilities. China’s vast air, maritime, and tech programs—including the “China Brain Project”³—focus on the dynamic interaction of human cognitive capabilities and state-of-the-art technology. Both have demonstrated technological initiative, innovation, and determination.

Success depends not on minds *or* technology but on the dyad of minds *plus* technology. We call this dyad the *Mind-Tech Nexus* and provide the following deliberately broad definition: how human factors (e.g., will to fight, skill, daring, perception) will interface and converge with the technologies of our time (e.g., digital, quantum computing, neuroscience) to help shape the character and the outcomes of competition (fig. I.1).

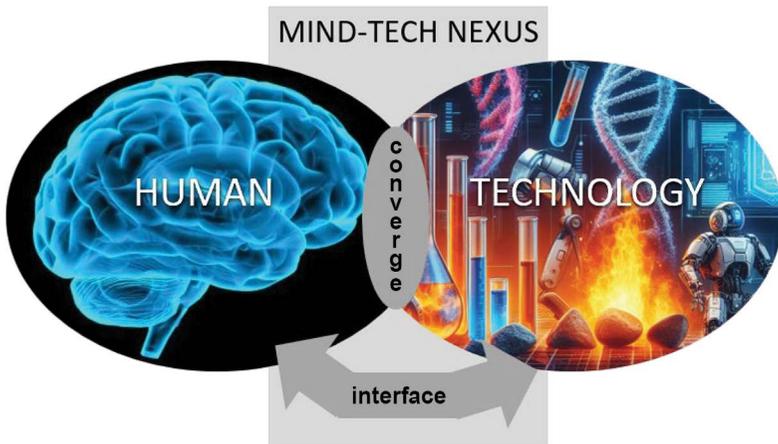


Figure I.1. Mind-Tech Nexus. This term refers to how human factors and technology will interface and converge to shape the character and outcomes of competition.

This book brings together world-leading experts to explore how the Mind-Tech Nexus is being—and can be—harnessed for military and geostrategic power. We aim to understand and describe:

- the latest thinking on minds and technology (e.g., neuroscience, AI, or quantum computing) and how they interface and converge;
- the implications of this Mind-Tech Nexus at every level of US national security, from the individual warfighter at the tactical level to leaders at the operational and strategic levels of war; and
- how the Mind-Tech Nexus matters not only for the US and its allies alone but also in the context of key competitors.

The synergy between human and technology or human and machine can be instrumental in shaping experiential outcomes through behavioral modification and performance enhancement (as well as performance suppression). For example, the development of corrective lenses has dramatically improved human performance in tasks requiring optical precision. Advances in material science have provided police and military personnel with protective equipment, significantly reducing their vulnerability and effectively altering their behavior under duress. The technologies emerging in our era will profoundly impact our human behavior and performance and hence how war is fought.

Having and harnessing the latest technologies to target human psychology can be equally crucial across the spectrum of human competition, from peace through the gray zone to high-intensity armed conflict. In the years of gray zone competition before 1939, Germany skillfully used deception, surprise, and propaganda internally and externally, taking it from the profound military weakness imposed by the 1919 Versailles Treaty to the military and strategic strength that smashed the Allied armies in war. Failure to anticipate the changed character of conflict was catastrophic for the Allies.

Britain better harnessed information for its vital defensive shields in 1940. The world's first integrated air defense system, Fighter Command, used pioneering technology and superior coordination of air assets to win the Battle of Britain—Hitler's first major defeat. Human creativity and technological excellence cracked the German Enigma codes to give a defensive and offensive edge. Prime Minister Winston Churchill engaged deeply with technologies and how they were used.

Of course, the nature of competition was not new in either World War II or its preceding gray zone competition. Panzer forces combined

arms and created surprise, but so did Napoleon, Hannibal, and Alexander the Great. Carl von Clausewitz described the “fog of war” in Napoleonic conflicts, but it applied just as well to every major contest before or after and will surely pervade future contests conducted via a panoply of AI-enabled systems. Failure to anticipate the changing character of competition can be disastrous. Anticipating what may change also requires grasping the unchanging nature of competition—for which human cognition provides a solid bedrock (box I.1). Technology changes, but the humans on the receiving—and giving—end of strategy remain human.

Box I.1. Changing character and unchanging nature of conflict between humans

A distinction is commonly drawn between the character and nature of war. Scholar Colin Gray, for instance, stated, “Many people confuse the nature of war with its character. The former is universal and eternal and does not alter, whereas the latter is always in flux.”

Strife, conflict, and war are essentially the permanent, inevitable struggle over the terms of coexistence—an interaction between humans and their psychologies. As Gray further notes, “The stage sets, the dress, the civilian and military equipment, and some of the language are always changing, but the human, political, and strategic plots, alas, remain all too familiar. . . . Interstate war and warfare continue to plague the human race. Even war between great powers is possible, given the political fuel lurking in the twenty-first century in the deadly and familiar classical Thucydidean categories of ‘fear, honor, and interest.’”⁴

US and allied success require both understanding the *nature* of competition, for which cognition is a solid bedrock, and anticipating its *character* in our coming epoch, which is aided by a grasp of technology. While neither cognition nor technology explain everything, they comprise much of what matters.

Some academics argue that AI changes the nature of war because it involves nonhuman systems in decision-making.⁵ But in many ways it is only the latest addition to the complicated mesh of systems within which human decision-making has long been embedded, such as the complex bureaucracies and other social systems that operate with their own nonhuman rules and processes. If the nature of war has changed, the most likely candidate remains the advent of mass-produced thermo-nuclear weapons with the capacity to annihilate civilization.

Interface and Converge

Humans and their technologies *converge*, coming together toward some point of unity and shaping each other on evolutionary and individual timescales.

Technology is the application of knowledge for practical purposes. Often, in the modern world, that knowledge comes from science, but technologies have been around for millennia. In fact, human evolution was shaped by our technologies. Humans had a remarkable ability to make tools like the hand ax about two million years ago and have controlled fire for around 400,000 years—before anatomically modern humans appeared around 300,000 years ago and cognitively modern humans around 30,000 years ago.

Our bodies were changed as our bigger and smarter brains helped us develop new technologies. Physically, adult humans are puny compared to even a juvenile chimpanzee. From the 1940s to the 1970s, a travelling circus went up and down the US eastern seaboard offering strong men the chance to earn money for every second they could pin a juvenile chimp to the floor—and in thirty years no one lasted more than five seconds.⁶ But humans have spears and axes. Humans have short bowels and weak jaws for tackling difficult foods, but they can cook, grind, and treat foodstuffs. It is not just being smart that is advantageous—nineteenth-century European explorers in the territories of hunter-gatherers would sometimes starve to death surrounded by foods that locals knew how to process.

During an individual's life, the use of technologies changes the structure and functioning of the brain. Brain imaging studies with groups including typists, jugglers, musicians, and golfers have demonstrated this effect.⁷ Tool use has been shown to change the brain in nonhuman primates, where more invasive neuroscience methods can be used: learning to use a rake to reach food changes a monkey's brain.⁸

Our remarkable human brains are the origin of these technologies—and so shape these technologies too. Humans are constantly imagining, adapting, and refining technologies. Tools are used and even made by some nonhuman animals, but nothing compares to the technologies wielded by a human hunter-gatherer. Humans originating in hot climates survived in the Arctic tens of thousands of years ago only through the adaptive use of effective technologies like clothes to keep warm and spears to kill huge animals like a woolly mammoth.

Humans and their technologies converge on these evolutionary and individual timescales. A sword feels like it is part of the body to a human expert, just like a monkey using a rake. When one of the authors of this introduction was a neurology doctor walking around the hospital wards, the stethoscope felt like a part of the body that naturally extended the body's capabilities. The design of that stethoscope had undergone decades of iterative development, converging to become ever more useful for the doctors who had to use it. During the service of another of this chapter's authors as a US Navy SEAL, one of the defining features contributing to the success of these small, elite units was the collective application of a suite of military technologies combined with highly realistic, effective training that enabled the performance of the collective to greatly exceed the sum of its individual operators. The resulting gestalt was further magnified by the SEAL operators' ability to think in three dimensions and rapidly integrate nearby human-machine teams from the sea, air, and land to achieve devastating effects.

Technologies and their humans also *interface*, which is where these separate systems interact—for example, pushing a pedal, turning a steering wheel, trimming the sail on a ship, flipping switches, or reading a computer screen. The B-17 Flying Fortress was a workhorse US bomber during World War II. However, many were lost just as they were landing back at base—but why? The problems were thought to be due perhaps to pilot error, poor maintenance, or runway quality. All were reasonable explanations, but all were wrong. After the war, research found the reason: on the B-17 cockpit instrument panel, the switch that engages the landing gear was next to the switch that operates the flaps. This design caused a plane returning from a long, dangerous mission over Germany to lurch to the ground, killing everyone on board.⁹ Many brave crew died because of a terribly dangerous interface.

As a doctor in the mid-2000s, one of the authors carried a Microsoft smartphone that connected to the internet, emailed, stored files and so on. However, he almost never used those features because the interface with a small stylus and keyboard was too clunky for practical use on the wards. To date, the single most commercially successful electronic gadget of this millennium is a smartphone that in theory could not do much more than the others. But what set the iPhone apart was its superior interface that made it user friendly (and ultimately generating a revenue of hundreds of billions of dollars).

Humans and technology interface and converge—and better interfaces and convergence always provide an edge in competition. Joint All Domain Command and Control (JADC2) is a set of vital new systems for US forces. These authors recently held an event with senior leaders from the US Air Force and Navy with deep knowledge of JADC2, and all agreed that while attention and resources were lavished on the technological aspects (which are key), insufficient attention was paid to how that technology would work with the humans who must use it.

Human-Machine Teams: Hammers, Horses, and Elephants

If you work with the Department of Defense, intelligence community, or industry, then your near future will increasingly involve collaborating with machines. If you have kids, they may already use generative artificial intelligence (GenAI, discussed further below) to “help” with homework. Human-machine teams are not options we are choosing to have or not have—the question is not to use or not use them but how effectively we will use them. AI will rarely replace humans but rather change the character of work.¹⁰

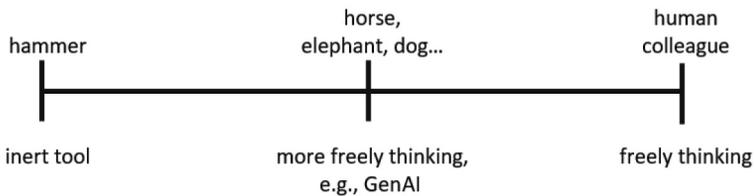


Figure I.2. How freely thinking is our “teammate”? The spectrum goes from an inert tool like a hammer to the freely thinking agent that is a human colleague.

We humans work with a spectrum of aids that can be distinguished by their capacity to process information (fig. I.2). At one end of the spectrum are inert tools like hammers. At the other end are fellow humans like colleagues or a partner in doubles tennis. In between lie things like the domesticated dog (e.g., to herd sheep, guide the blind, or pull a sled). Now, AI can enhance tools that lie in the middle of that spectrum, such as the widely used AI assistants that help computer programmers write code or students research and write essays.

Newer AI-enabled tools will keep moving further along this spectrum. A key question will be how to communicate to get the best from these enhanced tools. We have typically “communicated” with machines like cars, tanks, or aircraft using interfaces like steering wheels, levers, buttons, or switches like on the B-17 mentioned above. We communicate very differently with domesticated animals.

Communication is wide and deep in the middle of the spectrum, with dogs or horses becoming part of a relationship. We move toward the mix of verbal and subtle nonverbal communication that we have with other humans (discussed by Nicholas Wright in chapter 8). Increasingly, AI-enabled tools will interpret our facial expressions, tone of voice, and other cues to gauge and anticipate our confidence, emotions, and intentions. Cavalry and other mounted warriors—“human-horse teams”—played a central role in warfare from ancient times to the late nineteenth century due in part to the remarkably good communication between humans and their nonhuman teammates. Now, with GenAI, humans will increasingly be able to expand their communicative relationship with machines using complex language: humans *giving* prompts to machines, and humans *receiving* written or spoken responses back from the machines.

We could go further, using a second set of new technologies that give us another route to communicate with our tools: brain-computer interfaces, which are machines that directly read from and/or write to the brain. Brains and machines that can read and write to each other promise enormous benefits to restore function after brain injuries, strokes, or disease to help restore the ability to speak, perceive, decide, act via machines, or interact with loved ones. Substantial resources are going into these medical advances in the private (e.g., Elon Musk’s Neuralink) and public sectors of the United States and China. China prioritizes brain-computer interfaces, achieving advantages in its primate research infrastructure, and McKinsey estimated its “medtech” market had revenues of some \$70 billion in 2021.¹¹ But while these powerful new technologies promise life-changing health benefits for millions of Americans, including veterans, they also carry implications for US defense and security for two reasons. First, many are dual use and could not just restore function but also augment human performance, for example by helping a pilot perceive, decide, and act faster than an enemy. Second, while the United States rightly restrains many research practices and applications for ethical reasons, such is not always the case for competitors. The US military will face adversaries,

potentially in battle, who are armed with these technologies—and thus it is crucial to understand the technologies, their defense and security implications, and how the United States can craft a response that is both effective and within our ethical parameters.

Nicholas Wright describes these technologies in chapter 8 and explores their implications for the national security practitioner. What are the new technologies we will work with in the near future? How can we best work with them to create military and strategic effectiveness? What are practical ways to build appropriate levels of trust with human-machine teams to avoid overreliance and enhance collaboration? What pitfalls should we avoid? How can we use science to get the best from the humans, machines, and teams?

Drones have already changed the battlefields in Ukraine, and drones will continue to develop along with the teams of which they are a part. First-person view (FPV) drones have been powerful in Ukraine.¹² An FPV drone operator dons goggles showing a real-time video feed from the drone as it flies and pilots it from a drone's view versus the pilot's perspective on the ground. A racing drone pilot notes that this perspective enables pilots to “become one with the drone” so that in the civilian world it can race around 3-D obstacle courses. The pilot adds, “You cannot tell that you're on the ground anymore. You forget where you are, and you just become that machine.”¹³

The design of FPV drones evolved through civilian racing and now to combat to be most effectively operated by their human pilots. FPV drones offer cheap, accurate firepower. A simple FPV drone costs only \$400 versus some \$100,000 for a GPS-guided munition and nearer \$200,000 for a Javelin anti-tank missile. Training in Ukraine takes a month. Skilled pilots can manipulate a drone to chase vehicles or soldiers, fly into buildings or trenches, or circle enemy tanks and strike a precise location just rear of the turret to detonate ammunition stored there. A typical Ukrainian assault group of twelve to sixteen soldiers may have a similar number of drone operators, including half a dozen FPV pilots, with the remaining drones conducting supporting tasks like reconnaissance—a human-machine unit.

Near-future US and Chinese forces will likely field not only single FPV drones but swarms of semiautonomous drones. Ukraine and Russia are already striving to add AI to their drones. Certainly, in future swarms of semiautonomous drones, some might stampede in the wrong direction—much like war elephants in ancient conflict. A war elephant was semiautonomous and had a degree of free thought

that opponents could exploit. Countermeasures will be continuously developed to make drones go or attack in the wrong direction, a bit like the Romans developed to drive enemy war elephants back to their enemy lines. However, unlike war elephants, these new, partially free-thinking aids—semiautonomous drones—can be constantly updated to meet those countermeasures.

Drones and unmanned vehicles on land, sea, air, space, cyberspace, and everywhere else will be vital as they already are on the battlefields of Ukraine. They will likely include a range of more and less sophisticated drones that are semiautonomous, autonomous, and directly flown. Such a mix was found in Germany's blitzkrieg that included sophisticated mechanized units and hundreds of thousands of horses to haul supplies and equipment. Not everything will be ultramodern, and the drones will take many forms. For example, Russia and Ukraine are now employing FPV dive bombers that can attack many times. This tactic again mirrors blitzkrieg as described by Erhard Milch, a German Air Force general, at a pre-war conference on blitzkrieg tactics: "The dive bombers will form a flying artillery, directed to work with ground forces through good radio communications. . . . Tanks and planes will be [at the commander's disposition]. The real secret is speed—speed of attack through speed of communication."¹⁴ How such different units are coordinated and integrated will be key.

Mind-Tech and the Twenty-First Century: Nimitz, Patton, or Eisenhower

New technologies aim to extend decision-makers' situational awareness through AI and digital networks that connect myriad sensors. JADC2 seeks to integrate sensors from across the military services. The Defense Advanced Research Project Agency's (DARPA) Mosaic Warfare aims "to fight as a system of systems . . . at mission speed."¹⁵ DOD programs even aim to harness ocean life as a network of billions of living, self-replicating sensors. Yet systems feeding ever more information to human decision-makers is just half the equation. Humans possess incredible perceptual and information processing capabilities, but they remain humans with cognitive limits to what they can process and how they decide. Technology can extend powerful human capabilities and exacerbate human fallibilities. How can these new sensor, networking, and AI technologies interface most effectively with human command-

ers and warfighters? Indeed, how can new technology support a twenty-first-century Patton, Nimitz, Marshall, their staffs, and warfighters?

One approach is to consider how humans receive new data from which they make decisions—and ask how technology will affect this process. Specifically, we can break the decision-making process down into a chain from *data* as a “raw material” processed into *information*, then *knowledge* (ordered sets of justified enough beliefs), and lastly, *wisdom* (broader context for more holistic judgments) (fig. I.3). The poet T. S. Eliot wrote of this chain, asking, “Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?”¹⁶ Carl von Clausewitz also described this chain in his chapter “Intelligence in War”:

By “intelligence” we mean every sort of information about the enemy and his country. . . . Many intelligence reports in war are contradictory; even more are false, and most are uncertain. What one can reasonably ask of an officer is that he should possess a standard of judgement, which he can gain only from knowledge of men and affairs and from common sense.¹⁷

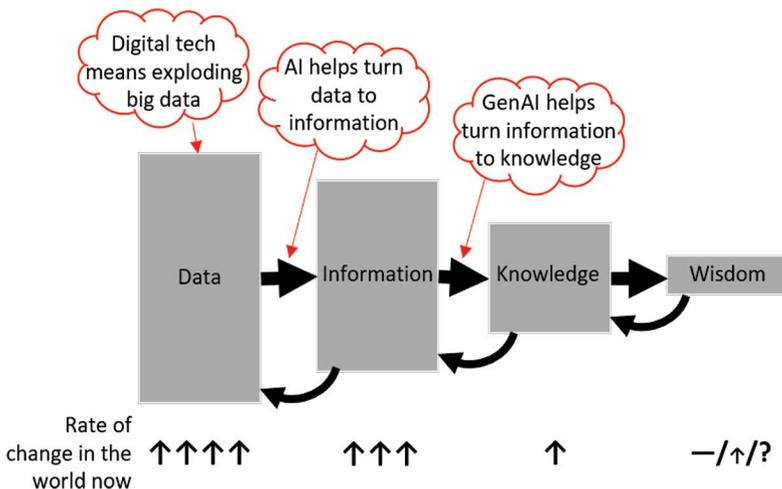


Figure I.3. Data, information, knowledge, and wisdom. The character of technology now means that data is expanding rapidly, which AI can now increasingly turn into information, but AI only more slowly increases knowledge or wisdom.

Box I.2 describes the four links in the chain and illustrates each with a military example. Not every link in this chain is equally affected by technology. Digital *data* is exploding, which AI like that used in Project Maven turns into *information*. Slightly more recently, advances in GenAI have enabled enhanced *knowledge*, and GenAI can already pass some exams at prestigious institutions like Wharton.¹⁸ *Wisdom* remains much more human—although that does not mean it cannot be operationalized via systematic approaches like jointness and net assessment that can be aided by technology.

Box I.2. Data, information, knowledge, and wisdom in military decisions

Data are facts and statistics collected for reference or analysis in which a single “datum” is a distinction that makes a difference (e.g., a thing is yellow or red).¹⁹ Data require processing to be meaningful (e.g., pixels from Earth observation satellites).

Information is meaningful data. It involves descriptions and is usually useful (e.g., vehicles counted and identified according to type, unit, and location).

Knowledge can be considered a more or less systematically ordered set of beliefs that are true and that we are justified in believing.²⁰ Knowledge is also often useful, and, furthermore, humans often require experience to master a body of knowledge (e.g., vehicles of this type taken together with other new capabilities, recent history, and changes in online discussions suggest a marked change in a competitor’s military posture. That actor may be about to strike another actor.).

Wisdom involves broader knowledge that provides context and a humility about what is unknown, enabling a more holistic assessment of the multiple key trade-offs required in complex judgments to act successfully.²¹ For example, what does this new knowledge mean within that actor’s broader sociopolitical context or wider regional and global contexts? As a senior US decision-maker once commented about the early days of the fight against the Islamic State of Iraq and the Levant (ISIL): the US can take many militarily powerful actions, but stepping back and looking at the bigger picture, if that means we lose Turkey as an ally, then we have lost far more than we gained.²² A stunning tactical or even operational advantage may be a strategic detriment.

US and allied success in our era requires attending to the changing Mind-Tech Nexus at every level—and the biggest drivers of change at every level are the new technologies we can expect over the next few years.

Which Tech Is Changing Things Now?

What are the key drivers for technological change looking ahead to 2031? This date is near enough for sensible predictions yet far enough for significant changes to emerge. What are the key drivers also relevant in the context of the warning by Adm. Philip Davidson, former Indo-Pacific commander, that “the threat [over Taiwan] is manifest during this decade, in fact in the next six years,” which would extend through 2027.²³

Here we draw on a recent synthesis of tech forecasts conducted for the Pentagon’s Strategic Multilayer Assessment Office.²⁴ The forecasts sought to identify key drivers of technological change at a large scale. Doing so therefore allows for time lags for cutting-edge research to go from the lab to the real world at a large scale. Forecasts included higher probability changes (e.g., incremental development and rollout of AI resulting from the leap around 2012) and lower probability changes (e.g., effective quantum computing that may have a larger impact).

Six areas emerged, as summarized in table I.1, that will likely drive change:

1. software (e.g., AI);
2. hardware (e.g., 6G);
3. biology (e.g., genomics);
4. outer space (e.g., low-cost commercial launch);
5. the question of who commands the tech (e.g., we have seen increasing exertion of government power over civilian tech companies across the globe—in the EU, China, India, and the United States—and this trend will almost certainly increase as new technologies become more critical to national security and infrastructure.); and
6. the inventors and builders of the tech (e.g., fig. I.4 shows that unlike the Cold War, they will be more civilian than military while China’s huge research and development [R&D] budget and innovative companies scaling inventions, for example, will likely continue).

Table I.1. Future technology for 2031: six key areas that will drive change. (Adapted from Nicholas D. Wright, “The Future Character of Information in Strategy: Forged by Cognition and Technology,” *Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group*, ver. 1, August 2021, <https://nsiteam.com/>. Information is updated here to reflect GenAI emergence into useful applications.)

Key Aea	Impact of AI/Technology
Software	<ul style="list-style-type: none"> • AI analysis, often in the cloud, will continue to radically increase the amount of data transformed into information about individuals and organizations. GenAI will increasingly turn this information into knowledge. • AI will enable new actions by organizations—e.g., management of vastly complicated military logistics and supply chains—at a scale and pace far beyond current human or bureaucratic capabilities. • Low probability/high impact: AI learning can generalize from small amounts of data, e.g., vastly improving surveillance and enabling machines to operate in unfamiliar environments.
Hardware	<ul style="list-style-type: none"> • Smarter devices with sensors (e.g., smartphones, cars, in building materials) will enmesh individuals and organizations with greater density (e.g., in the West) and wider coverage (e.g., across Africa). • Global information infrastructure will be rebuilt with new technologies like 5G and, without forethought, by 2031 rollout of 6G will threaten “Five Eyes” information dominance. • Low probability/high impact: Quantum computing may enable (or threaten) decryption of secure traditional communications.
Biology	<ul style="list-style-type: none"> • Mass personalization of healthcare for aging populations (e.g., digitized health records enable new types of research and treatment) plus mass genomics (e.g., large fractions of populations are genotyped) will likely benefit health everywhere. This also affords powerful authoritarian tools. • Cheaper and easier dual-use biological weapons tech will lower barriers to entry for small states and non-state actors.
Outer space	<ul style="list-style-type: none"> • Huge rise in satellite numbers, e.g., after roughly doubling to 3,372 from 2017 to 2021, they are estimated to reach 15,000 by 2028. • Entanglements will increase, including those between “civilian” and “military” space assets (e.g., SpaceX) or between conventional and nuclear missions in space. • Low probability/high impact: Low-cost satellite internet access could enable global internet communications that are tricky to censor.
Who will command the tech?	<ul style="list-style-type: none"> • Every sovereign entity that can is increasing political control over big tech companies (e.g., the US, China, and the EU), although methods vary. • Digital sovereignty at the domestic/foreign border is rising everywhere, with a character varying from liberal to authoritarian.
Who will invent and build the tech?	<ul style="list-style-type: none"> • US R&D is now more civilian than military (fig. I.4). • China’s economic growth levels out toward 2031 are uncertain, but China will likely be either the world’s largest or second-largest R&D spender. • China will expand its lead in global manufacturing to include more high-tech sectors unless the US significantly changes its policy.

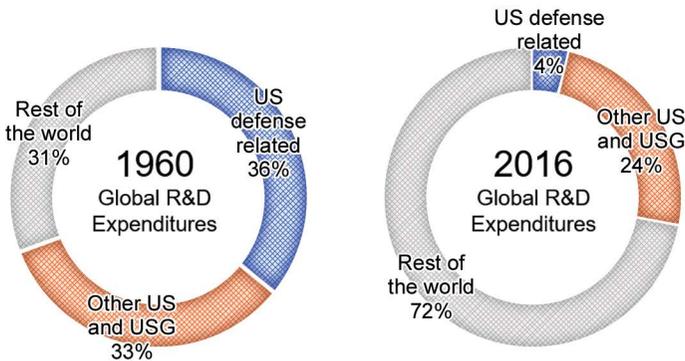


Figure I.4. Global R&D expenditures. (Source: Mike Brown, director, Defense Innovation Unit, presentation on Strategic Multilayer Assessment [SMA], February 2021.)

Beating Twenty-First-Century Maginot Lines

The French Maginot Line built in the interwar years to defend against Germany was a technological marvel of its time: carefully sited, with heavily armored gun turrets, elaborate underground quarters with kitchens, medical facilities, cinemas, and even air-conditioning. This technology did not commit France to a defensive strategy and could have freed troops for maneuver warfare. But, as the scholar Ernest May wrote on Germany’s victory over the confident French, it was “evidence of faith that technology could substitute for manpower. It was a forerunner of the strategic bomber, the guided missile, and the ‘smart bomb.’”²⁵

Who in our era is leaning too much on technology versus seeking to harness the mind plus technology that has so often led to success in conflict? Who now is best harnessing the Mind-Tech Nexus will only become evident following the audit of future war. Observers in the democracies were very confident in the strength of the mid-twentieth-century French army right up until its collapse. The “American way of war” famously leans heavily on technology—but too heavily?

In the course of the Mind-Tech Nexus project, including events with many senior current and former government officials and flag officers, a troubling trend has emerged. When asked to address the Mind-Tech Nexus—minds plus technology rather than just technology itself—most still tack intuitively toward the discussion of tech-

nology and not the human factors. Perhaps that is more comfortable. The human element of the Mind-Tech Nexus is more inscrutable; less easily measured and calibrated; difficult to monetize, let alone acquire; and inherently subjective. Yet it is no less important than the technology itself; indeed, this concept is precisely our central theme. It is the interface and convergence of the human and the machine—the Mind-Tech Nexus—that will determine the character and outcomes of future war. This paradigm may hold a lesson for the United States and its allies today: avoid the tendency to sail toward the more comfortable technological side of the equation. The rules of the emerging revolution in military affairs are being written now and will most certainly favor those who strike the correct balance between minds and tech.

Winston Churchill wrote that “a statesman in contact with the moving current of events and anxious to keep the ship on an even keel and steer a steady course may lean all his weight now on one side and now on the other.”²⁶ Moderation is not a course in and of itself—and in this case, aiming more toward the mind in the Mind-Tech Nexus could result in a more effective fusion of minds *plus* technology.

Failure to anticipate and respond proactively to the new character of conflict could be as catastrophic for the United States, in our era, as it was for the Allied armies facing panzer forces and blitzkrieg in May 1940. Fortunately, by July to October 1940, the Royal Air Force’s Fighter Command could harness minds plus technology just as decisively for defense to win the Battle of Britain. The world’s first integrated air defense system challenged ideas that had dominated interwar thinking on airpower—“the bomber will always get through”—and shot them down in flames.

Neither the German hammer nor the British shield was built in 1940. Years before, both had been forged by those like Germany’s Heinz Guderian (a principal architect of panzer forces) or Britain’s Hugh Dowding (the pioneering leader of Fighter Command), who looked ahead to exploit the future character of conflict.

Harnessing the Mind-Tech Nexus effectively will be even more critical in our time because, unlike World War Two, the “sleeping colossus” of world manufacturing is not the United States—which went from producing 5,856 aircraft in 1939 to 85,898 by 1943.²⁷ Estimates from the well-respected Organization of Economic Cooperation and Development showed that by 2023 China’s manufacturing production exceeded that of the next nine largest manufacturers

in the world put together.²⁸ Moreover, Western technological superiority can no longer be taken for granted. Our adversaries are keenly aware of the strategic potential of emerging technologies and are determined to achieve first-mover advantage. Russian president Putin has stated, “Whoever becomes the leader in this sphere [AI] will become the ruler of the world.”²⁹ China is already an acknowledged leader in 5G and 6G applications and is straining for leadership in quantum communications and computing with a substantial investment of monetary and human capital.

The United States and its allies and partners are not helpless. Indeed, due to their dynamic innovation ecosystems, highly educated populations, and deep capital resources, they are well-placed to compete and harness the Mind-Tech Nexus to their advantage over the next decade. However, they can only achieve this goal if they look ahead, motivate, mobilize, and synchronize their respective elements of national power and make the necessary course corrections.

Looking Ahead Through This Book

This book has six parts, described next. The scholarly and practical expertise of the authors presented in this work cannot hope to provide all the answers to the many questions raised by the Mind-Tech Nexus. Instead, we hope this book will open apertures and help frame better questions.

Part 1. The Mind-Tech Crucible: Innovation and Ethics

The book begins with foundational questions for building Mind-Tech capabilities. In chapter 1, Lauren Kahn considers the application of AI in organizations like the US military and how they can address the unique challenges arising at this juncture, such as automation bias—the tendency of human operators to offload responsibilities onto the automated tools they operate. In chapter 2, James Giordano raises vital ethical questions that every society—and most particularly democracies—must ask when building the Mind-Tech Nexus. He uses current and emerging developments in neuroscience and technology as a most literal exemplar of “Mind-Tech” fusion.

Part 2. Command, Control, and Intelligence in the New Fog of War

When seeking to apply deadly force to the correct area or to control escalating conflicts, no question matters more than *What do we perceive?* But perception is not so simple. Carl von Clausewitz described the “fog of war” in Napoleonic conflicts, but it applied just as well to every major contest before or after and will surely pervade future contests conducted via a panoply of systems using technologies like AI. The fog remains, but its character changes.

We have gone from the eye to the telescope, to the radar, through different layers of thinking in bureaucracies—and now ever more sensors will produce more data, and then more AI will help turn that data into more information. In a US-China escalation scenario, for example, both sides will perceive the world through more layers of technology. How should US analysts and decision-makers rely on each new source of information, weight various sources compared to each other, integrate them, or consider how their usefulness may change according to context? What if the new systems have been deceived? US success requires the humans and machines that can together manage this new kind of “fog” so that the United States has superiority not only in data and information but also in knowledge and wisdom.

In chapter 3, Sir David Omand, a former head of British Government Communications Headquarters (GCHQ), explores lessons from the history of intelligence that offer lessons for the Mind-Tech Nexus. Future scientific breakthroughs in the Mind-Tech Nexus (e.g., exploiting quantum computing at scale) must be expected to provide novel information advantage.

In chapter 4, Andrew Gainer, Karl Van Orden, and Jamie Lukos take the view from warfighters dealing with the fog of war—such as those aboard the ship *Vincennes* that tragically downed a civilian airliner in the 1980s. They illustrate past human-system synergy lessons learned, the enablers required today to make human-system synergy plausible, and a vision of future human-system synergy.

But perception is only an input to making and communicating better, faster, and wiser decisions. At its most fundamental, command and control (C2) represents how the Department of Defense makes operational decisions. As German forces showed in May 1940, the ability to decide and execute joint action more quickly than competitors can be devastating. What is the future of C2? Human commanders and staff will be central to success—and failure. Technologies will

be crucial, and the most significant changes in how we approach C2 are likely to come from the rapid development of information technologies, sensors, AI, and automation. How these humans and machines interface and converge will be key for successful decision support, operational management, logistics, and integration across multiple levers of power.

In chapter 5, Tim Grayson (former head of DARPA's Strategic Technologies Office and recent senior advisor to the secretary of the Air Force) takes apart Boyd's famous Observe-Orient-Decide-Act (OODA) loop to provide a template for distributing the cognitive burden of decision-making between humans and machines. As we move toward increasingly complex theater, strategic, and enterprise problems, we need to think like operators, develop similar AI-driven decision aids, and act with the same operational practicality and speed—avoiding the institutional traps of overcomplicating our already highly complex challenges.

In chapter 6, Lt. Gen. Michael Groen (USMC, retired, and former director, Joint Artificial Intelligence Center) provides a compelling vision of Mind-Tech teaming in defense, which must harness both integration and imagination.

In chapter 7, Lt. Gen. John (Jack) N. T. Shanahan (USAF, retired, and founding director of the Joint Artificial Intelligence Center) argues that we are witnessing the early outlines of the third major revolution in our species' history—a digital revolution—that has fundamental differences in the effects generated by new versus previous technologies. Optimizing the integration of humans and AI-enabled machines depends on redesigning the interfaces between humans and machines as well as recalibrating and balancing human and machine roles and responsibilities—and that will be central for future military and intelligence operations in our age.

Part 3. Performance Enhancement

This section discusses how the changing aspects of the Mind-Tech Nexus will affect the individual warfighter. In chapter 8, Nicholas Wright surveys the new technological drivers, including new sensors, AI, GenAI, brain-computer interfaces, cognitive enhancing drugs, mass personalization, and technologies for monitoring the physiology of the human for war. How can the United States craft strategies to compete in a world where warfighter performance may be enhanced

in myriad ways across millisecond to multiyear timescales—and stay true to US values?

In chapter 9 William Casebeer, a former Air Force officer who led innovative work on neuroscience and physiology at DARPA before moving to the private sector, discusses the promise of *physiologic intelligence* (PHYSIOINT). Widespread collection using wearable sensors and a growing body of experimental data demonstrate the promise of assessing and forecasting warfighter performance on critical tasks. This capability can help improve performance among allied service members and better characterize the strengths and vulnerabilities of adversary forces.

In Chapter 10, David Huberdeau describes civilian technologies for physiological monitoring. He explores how these can be adapted for the military—demonstrating the crucial dual-use nature of the Mind-Tech Nexus in our time. He also explains how a principled application of these technologies can identify what can and cannot currently be quantified effectively.

Part 4. Chinese and Russian Mind-Tech

In 1939 the USSR invaded Finland. The mauling inflicted by outnumbered yet nimble Finnish forces led many to view Soviet forces as rotten and weak. Yet within three years, the Soviet Union had learned to counter the German blitzkrieg, combining human factors with brilliant equipment like the T-34. From the ashes of a world war that devastated much of Europe, the Soviet Union emerged in 1945 as a true superpower. In 1957 it launched Sputnik—the world's first satellite and proof that in some key strategic technologies the Soviet Union had surpassed the United States.

Discounting our adversaries' ability to learn or to innovate rarely turns out well. In 2022 many Western observers derided Russian adaptability during their invasion of Ukraine, but by the end of 2023, Russia had clearly shown its ability to learn and adapt—not least for operating FPV drones.³⁰ Russia has learned in the Syrian laboratory of war and is learning in Ukraine. It is linked with China and Iran. It remains a major arms supplier to India. Russia has also been thinking for years about how to combine new technologies with human factors. Unconstrained by many of the ethical scruples that bind Western powers, Russia's innovations pose a clear and significant threat. Its deeply felt historical grievances and aggressive doctrine of “new generation

warfare”³¹ are nurtured by a profound hostility toward the United States and the liberal, rules-based global order that has shaped international relations for the past nearly eight decades.

In chapter 11, Sam Bendett explores Russian military attempts at enhancing human combatant capabilities with modern technologies. While Russia’s invasion of Ukraine has revealed issues with military technology, concepts, and personnel utilization, Russian military institutions, academies, defense-industrial enterprises, and R&D centers charged with conceptualizing high-tech combat have maintained focus on the human-technology nexus.

And what about China? China is now good at technology from AI to quantum. Chinese soldiers pushed US-led forces to retreat hundreds of miles after their 1950 attack in Korea and then fought the massively technologically superior US to a standstill until 1953. China now has the technology and Chinese troops have proven they have the will and skill to fight—but what about the Mind-Tech Nexus that combines them? Recent research suggests the Mind-Tech Nexus is an increasingly critical area, particularly in Chinese thinking. In this vital area of warfare, can China outpace the US and its allies?

In chapter 12, Joshua Baughman describes how the People’s Liberation Army (PLA) underscores the paramount significance of the cognitive domain in achieving triumph in conflicts, particularly highlighting the integration of mental processes and technological interfaces. While technological platforms are pivotal to executing cognitive attacks for “system destruction,” the PLA equally emphasizes “system survival.” It involves bolstering the mental resilience of soldiers through a combination of traditional and technological approaches. Additionally, the PLA prioritizes equipping commanders with tools that facilitate the seamless integration of human capabilities and machine intelligence, thereby fostering informed decision-making on the dynamic battlefield.

Part 5. The Question of Will and Suppression of Performance

All the technology in the world—even the best technology—cannot guarantee success in warfare if the individual warfighter or entire military units lack the will to fight. What factors motivate soldiers to fight bravely? Or fail to do so? And how will the technologies in use today and those being developed for tomorrow’s battlefield affect the will to fight?

Part 5 examines resolve, courage, bravery, and will at the individual and small unit level and how we can harness these characteristics in our new technological era. It also explores how adversary information operations can target these factors—and how the United States and its allies might defend against such operations.

In chapter 13, Alfred (Ben) Connable describes the human as the most important element of the Mind-Tech Nexus. Present investments in human enhancement, monitoring, and human-robot teaming have the wrong order of priorities. Technical design and rapid fielding are favored over methodical research to anticipate cognitive and psychological impacts on the soldiers intended to wear and apply the new technology. He proposes ways to rectify this gap.

In chapter 14, Aaron Frank argues that understanding what neuroscience can and cannot do to affect “will to fight” depends on a broader understanding of military organizations as a complex system where the relations between soldiers are as important as the soldiers themselves. A complex systems perspective on will to fight creates space for discoveries in neuroscience to contribute to will to fight. Concurrently, it establishes a framework for setting realistic expectations, measures of effectiveness, and trade-offs between efforts to improve military effectiveness at the individual and group levels.

In chapter 15, Nicholas Wright asks how adversaries might use information operations to degrade the military performance of the joint force and allied militaries. How will GenAI affect such information operations? “Deepfakes” are already here, and what about the “metaverse”? Human cognition will always be the ultimate target of information operations, and human cognition always contains vulnerabilities. Mass personalization of influence operations is coming; countering it requires new human-AI teams and organization.

To conclude this volume, we aim to do something different that *could not* have been done even five years ago.

Part 6. Conclusions from Humans—and Conclusions from Machines

Chapter 16 includes the conclusions written by three humans—the three editors of this volume. With our human brains we aim to bring together the different strands of the book. We chart possible ways forward for the United States and its allies—as seen by these human

authors, drawing on the insights from the array of experts who contributed to this volume.

While this chapter would normally provide a natural end point in the narrative arc of this book, we also open the door for a new beginning. Many future books will not be static objects but through generative AI and other technologies will become more dynamic. We don't know precisely how that will happen. But to sketch out one beginning, we introduce David Vernal, a retired US Air Force colonel in the intelligence arena who has spent time at Stanford to learn about generative AI. In chapter 17, he launches us on the exploration of this remarkable new technology as it interfaces and converges with humans. After all, the big, new models learned from us humans.

In chapter 18, we present the conclusions written by generative AI—prompted and annotated by Dave Vernal. We will see what generative AI gets from this book and what products it can make for national security practitioners. This chapter includes several artifacts created by generative AI, including summaries, potential indicators and warnings, and insights in the style used by real-world practitioners.

Notes

(All references are fully cited the first time they appear in each section or chapter.)

1. Gian Gentile et al., *A History of the Third Offset, 2014–2018* (RAND Corporation, March 31, 2021), <https://www.rand.org/>.
2. Watson Institute for International and Public Affairs, “Human and Budgetary Costs to Date of the U.S. War in Afghanistan, 2001–2022, August 2021,” <https://watson.brown.edu/>.
3. Wm. C. Hannas and Huey-Meei Chang, “China’s ‘New Generation’ AI-Brain Project,” *PRISM* 9, no. 3 (2021): 18–33, <https://ndupress.ndu.edu/>; and Dennis Normile, “China Bets Big on Brain Research with Massive Cash Infusion and Openness to Monkey Studies,” *Science*, September 20, 2022, <https://www.science.org/>.
4. Colin S. Gray, “War—Continuity in Change, and Change in Continuity,” *Parameters* 40, no. 2 (2010): 6, 11, 12, <https://doi.org/10.5554/0031-1723.2521>.
5. Kenneth Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict* (Hurst, 2021).
6. Joseph Henrich, *The Secret of Our Success: How Culture Is Driving Human Evolution, Domesticating Our Species, and Making Us Smarter* (Princeton University Press, 2015), 69–70.
7. Cassandra Sampaio-Baptista et al., “Structural Plasticity in Adulthood with Motor Learning and Stroke Rehabilitation,” *Annual Review of Neuroscience* 41, no. 1 (2018): 25–40, <https://doi.org/10.1146/annurev-neuro-080317-062015>.
8. M. M. Quallo et al., “Gray and White Matter Changes Associated with Tool-Use Learning in Macaque Monkeys,” *Proceedings of the National Academy of Sciences* 106, no. 43 (October 27, 2009): 18379–84, <https://doi.org/10.1073/pnas.0909751106>.

9. Ian Levy, “So Long and Thanks for All the Bits,” blog post, National Cyber Security Centre, October 27, 2022, <https://www.ncsc.gov.uk/>.

10. Matthew Johnson and Alonso H. Vera, “No AI Is an Island: The Case for Teaming Intelligence,” *AI Magazine* 40, no. 1 (2019): 16–28, <https://doi.org/10.1609/>; and Carl Benedikt Frey, *The Technology Trap: Capital, Labor, and Power in the Age of Automation* (Princeton University Press, 2019), <https://press.princeton.edu/>.

11. Zoë Moore, “Brain-Computer Interfaces: Medical Miracles and Innovation Policy,” *China Brief* 24, no. 1 (January 5, 2024), <https://jamestown.org/>; William C. Hannas et al., “Bibliometric Analysis of China’s Non-Therapeutic Brain-Computer Interface Research,” issue brief, (Georgetown University, Center for Security and Emerging Technology, March 2024), <https://cset.georgetown.edu/>; Margaret Kosal and Joy Putney, “Neurotechnology and International Security: Predicting Commercial and Military Adoption of Brain-Computer Interfaces (BCIs) in the United States and China,” *Politics and the Life Sciences* 42, no. 1 (April 2023): 81–103, [https://doi.org/10.1017/pls.2022.2](https://doi.org/10.1017/pls.2022.2;); and Jody Tian et al., “Upgrading Medtech Commercial Operations in China,” McKinsey, March 13, 2023, <https://www.mckinsey.com/>.

12. Shashank Joshi, “How Cheap Drones Are Transforming Warfare in Ukraine,” *The Economist*, February 5, 2024, <https://www.economist.com/>.

13. “How ‘The Da Vinci of Drones’ Ryan Gury Designed the DRL Racer3,” Design Boom, <https://www.designboom.com/>; Grace Dean, “Drone Racing: Everything You Need to Know,” Space.com, December 7, 2021, <https://www.space.com/>; and Kathrin Maurer, *The Sensorium of the Drone and Communities* (MIT Press, 2023), <https://mitpress.mit.edu/>.

14. Quoted in John Keegan, *A History of Warfare* (Pimlico, 1993), 370.

15. “Panel 4: Mind-Tech Nexus: How Can New Tech Support a 21st Century Patton, Nimitz, Marshall, Their Staffs, and Their Human Warfighters?” (The Decisive Decade: Building Enduring Advantage, conference, February 8–9, 2023, Joint Base Andrews, Maryland), <https://nsiteam.com/>.

16. T. S. Eliot, *The Rock* (Harcourt, Brace and Company, 1934), pt. 1, Internet Archive, <https://archive.org/>.

17. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Oxford University Press, 2008), 64.

18. Christian Terwiesch, “Would Chat GPT3 Get a Wharton MBA? A Prediction Based on Its Performance in the Operations Management Course,” Mack Institute for Innovation Management at the Wharton School, University of Pennsylvania, 2023, <https://mackinstitute.wharton.upenn.edu/>.

19. Luciano Floridi, *Information: A Very Short Introduction*, illus. ed. (Oxford University Press, 2010), 23.

20. Knowledge and information are members of the same conceptual family, but knowledge enjoys a web of mutual relations that allows one part of it to account for another—once some information is available, knowledge can be built in terms of explanations or accounts that make sense of the available information (Floridi, 51). *Knowledge* as “justified true belief” has been a powerful definition since Plato, although the problems raised in Edmund Gettier’s 1963 paper as to whether this descriptor is sufficient have compromised that definition for many contemporary philosophers of knowledge. Jonathan Jenkins Ichikawa and Matthias Steup, “The Analysis of Knowledge,” published February 6, 2001; last revised March 7, 2017, in *Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta (Metaphysics Research Lab, Stanford University, Summer 2018), <https://plato.stanford.edu/>.

21. Wisdom is discussed across diverse disciplines. For accessible discussions of wisdom in philosophy, see, for example, Sharon Ryan, “Wisdom,” published January 8,

2007; revised February 4, 2013, in *Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Spring 2020 (Metaphysics Research Lab, Stanford University, 2020), <https://plato.stanford.edu/>; in psychology, see, for example, Igor Grossmann, “Wisdom in Context,” *Perspectives on Psychological Science* 12, no. 2 (March 27, 2017): 233–57, <https://doi.org/10.1177/1745691616672066>; in management, see, for example, Jennifer Rowley, “The Wisdom Hierarchy: Representations of the DIKW [data-information-knowledge-wisdom] Hierarchy,” *Journal of Information Science* 33, no. 2 (2007): 163–80, <https://doi.org/10.1177/0165551506070706>; and in functional genomics, see, for example, Chris P. Ponting, “Big Knowledge from Big Data in Functional Genomics,” *Emerging Topics in Life Sciences* 1, no. 3 (November 14, 2017): 245–48, <https://doi.org/10.1042/ETLS20170129>

22. Comment by a senior US decision-maker to one of the authors and paraphrased here.

23. Mallory Shelbourne, “Davidson: China Could Try to Take Control of Taiwan In ‘Next Six Years,’” *USNI News*, March 9, 2021, <https://news.usni.org/>.

24. Nicholas D. Wright, *The Future Character of Information in Strategy: Forged by Cognition and Technology*, Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group, v. 1, Intelligent Biology, August 2021, <https://nsiteam.com/>.

25. Ernest R. May, *Strange Victory: Hitler’s Conquest of France* (Farrar, Straus and Giroux, 2000), 9, 119–20.

26. Quoted in Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen and Leadership in Wartime* (The Free Press, 2002).

27. Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500–2000* (Unwin Hyman, 1988), 455.

28. Richard Baldwin, “China Is the World’s Sole Manufacturing Superpower: A Line Sketch of the Rise,” *VoxEU/CEPR*, January 17, 2024, <https://cepr.org/>.

29. Radina Gigova, “Who Vladimir Putin Thinks Will Rule the World,” *CNN*, September 1, 2017, <https://edition.cnn.com/>.

30. Mick Ryan, “Russia’s Adaptation Advantage: Early in the War, Moscow Struggled to Shift Gears—but Now It’s Outlearning Kyiv,” *Foreign Affairs*, February 5, 2024, <https://www.foreignaffairs.com/>.

31. James Derleth, “Russian New Generation Warfare Detering and Winning at the Tactical Level,” *Military Review*, September–October 2020, <https://www.armyupress.army.mil/>.

Part 1

**THE MIND-TECH CRUCIBLE:
INNOVATION AND ETHICS**

Chapter 1

The Mind and the Machine

Combating Automation Bias and Crafting Effective Human-AI Teams on the Battlefield

*Lauren Kahn, Senior Research Analyst, Center for Security and
Emerging Technology*

Abstract

This chapter examines the role of artificial intelligence (AI) in enhancing military operations, positioning AI as a strategic augmenter of human capabilities in many cases, not as a replacement. For centuries, militaries have been investing, developing, adopting, and deploying new technologies to make them more effective and faster and provide them with more information. AI represents the latest iteration in this long tradition. The extent to which nation-states and their militaries successfully leverage AI will largely depend on how effectively they manage human-machine teams and address the unique challenges arising at this juncture, such as automation bias—the tendency of human operators to offload responsibilities onto the automated tools they operate.

AI Promises

For centuries, as states have sought to employ their militaries to advance their interests and demonstrate, exercise, and wield power on the international stage, they have had to grapple with the profound uncertainty inherent in warfare—a concept succinctly articulated by Clausewitz as the “fog of war.” While it is not possible to eliminate the fog of war or the friction that emerges from managing it, militaries work to reduce the uncertainty they have to contend with on the battlefields and in conflict—since having even marginally more clarity than one’s adversaries could prove decisive in victory or defeat.

Militaries understand that relatively faster and more reliable communications can increase their capabilities. The pursuit of enhanced information has evolved throughout history, with innovations like the

telegraph allowing greater command and control in the US Civil War and radio communications in World War II that facilitated quicker, decentralized decision-making, enabling the blitzkrieg. This trend continued with the development of command-and-control systems and intelligence, surveillance, and reconnaissance (ISR) capabilities, which matured during the era of the Second Offset Strategy and were first demonstrated for the broader public via precision strike capabilities in the 1991 Persian Gulf War.

From strategic war rooms to the frontlines of battle, militaries worldwide are developing and deploying artificial intelligence technologies for the potential advantages they promise to deliver. AI is already proving its mettle in this capacity in situ. From using AI to synchronize artillery fire and integrate sensor and targeting data with satellite imagery to employing neural networks to “combine ground-level photos, video footage from numerous drones and UAVs, and satellite imagery to provide faster intelligence analysis and assessment,” AI is seemingly being used to make the Ukrainian military a more agile, adept, and lethal force.¹

However, developing technologies and tools to continuously acquire and leverage more information and make better, quicker decisions effectively places a growing burden on the primary actor in this context—the warfighter. The warfighter oversees all operational components, makes instantaneous decisions, and maintains awareness amid many dynamic elements. As the sources of information proliferate and diversify, synthesizing this wealth of data becomes increasingly formidable. As a Congressional Research Service report states, “Currently, information available to decision-makers comes in diverse formats from multiple platforms, often with redundancies or unresolved discrepancies.”² Uses of AI represent a means to alleviate some of this cognitive load on the warfighter. The United States views AI as a force multiplier. As a result, AI is assuming an expanding role in the collection, identification, and synthesis of multiple data streams to enhance real-time battlefield and situational awareness, fostering stronger connections between sensors, operators, and decision-makers. The military will increasingly use AI to generate a common operating picture or “glass battlefield”—a real-time, three-dimensional view of the operational area combined with sensor data.

The promise of AI is not just to make munitions, warfighters, and a hierarchical chain of command more effective but to become a force multiplier and, potentially, a factor of combat power itself.

The Overlooked Aspect: Human-AI Interaction

In its recently released Data, Analytics, and Artificial Intelligence Adoption Strategy, the Department of Defense (DOD) explicitly outlines its overarching goal: “As a result of implementing this Strategy, DOD leaders and warfighters will be able to make rapid, well-informed decisions by expertly leveraging high-quality data, advanced analytics, and AI as part of a continuous, outcome-driven, and user-focused development, deployment, and feedback cycle.”³ The crux of the new DOD AI strategy revolves around the human element, with AI playing a supportive, augmentative role.

Nevertheless, current discussions surrounding AI often divorce the technology from its real-world applications and implications, primarily fixating on the systems and technology themselves while overlooking the pivotal juncture where humans and systems intersect. AI is often, misleadingly, characterized as a potential human replacement—a notion appropriately termed the “substitution myth” in robotics circles—thanks to its ability to enable increasingly autonomous operation and functionality, from driverless cars to customer service chatbots.⁴ This assumption constitutes a distorted portrayal of automation’s impact. AI might necessitate adjustments in skills and routines, but such adaptation comprises a reshaping and not a replacement of human work. Despite its potential to automate specific tasks, AI at its core fundamentally remains a tool to be wielded by human operators.

The successful transition of an AI application from experiment to deployable capability thus hinges on its seamless integration into existing systems and processes and its ability to interoperate effectively with human users. In military contexts, AI has the potential to become an incredibly potent tool, but how humans employ and interact with it will define its utility and impact. Even in its most autonomous forms and applications, AI’s effectiveness (and ultimately, its success and impact) relies on human involvement, both in task delegation and in reliance on its outcomes and outputs.

While there is a wealth of literature on human-machine interaction, little has extended to the specific dynamics of human interactions with AI and autonomous systems.⁵ Such a gap becomes particularly worrisome as militaries worldwide forge ahead with the development, adoption, and eventual deployment of these advanced technologies and capabilities without concurrent guidelines. Comprehensive policies

must govern the evolving dynamics between humans, AI, and increasingly autonomous systems.

This oversight could prove detrimental given that the successful use of AI hinges on effective human-machine teams. Without understanding and optimizing this relationship, the full potential of AI for enhancing command and control will remain unrealized. Further, failing to establish limits and guardrails also elevates the likelihood of adverse outcomes such as the precipitation of failure cascades, accidents, inadvertent escalation, or even unintentional conflict.⁶

Prioritizing Human-Machine Teaming in International Security Contexts

As states continue to incorporate AI into military environments, particularly within decision-making contexts, ensuring human operators are relying on and using these systems appropriately is paramount for ensuring the safety and effectiveness of the systems. Consequently, there has been a growing emphasis on these concerns throughout every phase of the technology lifecycle, from the initial design to testing, evaluation, validation, and verification (TEVV) to adoption and deployment. The human element emerges as an indispensable component in developing effective policies, particularly personnel policies. Therefore, it is imperative for states to define what constitutes effective human-machine interaction and to design and implement policies that ensure the success of human-machine teams.

States worldwide recognize the crucial role of human interaction in AI systems as evidenced in international political declarations and debates, domestic policies, and even the very systems and capabilities they are pursuing. Over forty countries have signed the Political Declaration on Responsible Military Use of AI and Autonomy, which highlights the need to ensure operators “sufficiently understand the capabilities and limitations of those capabilities to make appropriate context-informed judgments” and warns against the risk of automation bias.⁷ China has noted how the “command brain” concept—for AI to reduce the cognitive load on military commanders and decision-making on the battlefield—will be essential in achieving “intelligentized” warfare.⁸ However, it, too, has emphasized that the focus is on assisting human decision-making and, ultimately, human-machine collaboration.⁹

States are not merely making rhetorical nods to the significance of human-machine teams in their policies or viewing humans solely as controllers or checks on automated systems. Instead, they are directly investing in these concepts from a capabilities perspective. For example, the Department of Defense has consistently underscored this approach, implicitly evident in its AI strategy, how it handles AI implementation, and even the capabilities it actively pursues. AI now occupies a central role in the Joint All-Domain Command and Control (JADC2) framework, which seeks to leverage automation, AI, predictive analytics, and machine learning to centralize the planning and execution of operations spanning air, space, cyberspace, sea, and land domains, striving to create a fully integrated and synchronized force.¹⁰ Similarly, the US Air Force is actively pursuing the Combat Collaborative Aircraft (CCA) project; the name indicates its focus on autonomous systems, but the project emphasis is on how these systems can enhance, support, and empower human pilots. Instead of merely replacing human pilots, CCA aims to serve as a true force multiplier. The concept is that the “proposed CCAs will comprise a new breed of significantly less expensive and highly autonomous, mission-focused, unmanned collaborative combat aircraft to fly along with fifth-generation and newer human-crewed fighter jets,” thereby distinguishing them in terms of “form and function” from other capabilities and even other uncrewed aerial vehicles and autonomous systems.¹¹

The Challenges of Human-Machine Teaming

Appropriately combining human and artificial intelligence yields a greater collective strength than their individual capabilities. However, human-machine teaming also presents distinctive challenges. When working in tandem, humans and AI might not only amplify their respective strengths but occasionally also their weaknesses, manifesting in challenges and risks such as automation bias, the potential for failure cascades, and communication breakdowns.

In commercial aviation, a prime example of human-machine interaction is found in flight management systems. These systems rely on a high degree of automation and the expertise of well-trained pilots. The synergy between pilots and aircraft is deeply ingrained in FAA regulation, established protocols, operational methods, and the overarching institutional policies and standards governing the collaboration,

integration, and teamwork between pilot and autopilot. This intricate equilibrium hinges on the premise that pilots are extensively trained and the systems are rigorously tested. It is not surprising that most aviation accidents and incidents today stem not from isolated mechanical failures or pilot error—the systems are more robust than that—but from cascading failures that originate at the juncture of human-machine interactions.

For example, in the two 2019 incidents involving the 737 Max Boeing aircraft, independent investigations agreed that the human element had not been adequately addressed in integrating the new automated system. It was introduced without sufficient advance notice, training, and guidance for pilots regarding their roles and procedures for overriding and managing the updated system.¹² Postaccident reporting of two separate accidents in 2003 involving Patriot missile systems revealed that while the accidents were initially triggered by an error in an automated decision aid, they were ultimately compounded by established organizational practices.¹³

More than merely regulating the algorithms or AI systems themselves is required. The solution to this complex dynamic lies in a tandem strategy that concurrently trains human operators (informed by the system's design) and carefully designs and regulates the AI systems and algorithms (informed by the human operational procedures). Governance efforts should include operator training; assurances of interoperability; clear delineation of authority, responsibility, and task distribution between humans and machines; established personnel and operational protocols; and further research into human-machine teaming more broadly.

Automation Bias in Human-Machine Teaming

One of the specific challenges encountered in human-machine teams is the phenomenon known as “automation bias.”¹⁴ Automation bias refers to the tendency of humans to place excessive reliance on automated systems or decision aids, which can result in errors in omission and commission. Automation bias manifests and can be exacerbated and mitigated at various levels:

1. Individual level: At the individual level, personal preferences, knowledge, and familiarity with systems play a substantial role in shaping individual biases and determining how a human operator

interacts with a system. Factors such as an individual's level of experience, trust, and confidence in the system as well as their self-confidence in task completion can impact the circumstances under which an individual is more inclined to delegate cognitive tasks to the AI, or conversely, more hesitant to rely on it.

2. System level: The design of the system, encompassing elements like user interfaces and human-factors engineering, is of paramount importance. System design can profoundly affect how users interact with it. For instance, in the commercial aviation sector, the interaction between pilots and aircraft (or in the context of autonomous vehicles, the interaction between drivers and cars) is deeply ingrained within the systems and their inherent functionalities, from how warnings are displayed to the shape and location of toggles, switches, and buttons.
3. Organizational level: At the organizational level, policies, procedures, and cultural philosophies shape and institutionalize how AI systems are approached, employed, and trusted (or not) within an organization.

While far from being a novel concept—applicable to any capability featuring a degree of automation—automation bias is potentially exacerbated in human-AI interactions. At its current pace of development, AI is simultaneously becoming more powerful and often more opaque and “black boxed,” with outputs, behaviors, and even malfunctions that are challenging to decipher, trace, and understand.

Thus, navigating the AI landscape in military contexts demands a comprehensive approach to addressing automation bias at all levels, and recognizing and mitigating this bias is not just a matter of technology design or policy formulation.

Conclusion

This chapter has explored AI's current and future role in modern military operations, emphasizing the importance of effective human-machine teaming in leveraging the full potential of these technologies. The key points discussed highlight the need for a comprehensive understanding of human-AI dynamics, the challenges of automation bias, and the criticality of centering the interaction point between humans and AI in technology design and policy formulation.

Looking forward, the potential of AI in military contexts is vast, yet its application requires a balanced approach that considers the force-multiplying capabilities of AI systems and the irreplaceable value of human judgment and decision-making. As military organizations worldwide continue integrating AI into their operations, the need for ongoing research, policy development, and training in human-machine teaming will remain paramount. The successful leveraging of AI on the battlefields and a significant determinant of whether AI will enable effective military innovations will be the interaction between technological advancements and our ability to adapt and evolve in our understanding and management of these complex systems.

Notes

(All references are fully cited the first time they appear in each chapter.)

1. Tom Cooper, “Kropyva: Ukrainian Artillery Application,” *Medium* (blog), June 10, 2022, <https://medium.com/>; and Sam Bendett, “Roles and Implications of AI in the Russian-Ukrainian Conflict,” *Russia Matters* (blog), July 20, 2023, <https://www.russiamatters.org/>.
2. Kelley M. Saylor, “Artificial Intelligence and National Security” (Congressional Research Service, August 26, 2020), <https://crsreports.congress.gov/>.
3. Chief Digital and AI Office, Department of Defense, “2023 Data, Analytics, and Artificial Intelligence Adoption Strategy,” fact sheet, November 2023, <https://media.defense.gov/>.
4. S. W. A. Dekker and D. D. Woods, “MABA-MABA or Abracadabra? Progress on Human–Automation Co-ordination,” *Cognition, Technology & Work* 4, no. 4 (2002): 240–44, <https://doi.org/10.1007/s101110200022>.
5. Margarita Konaev et al., “Trusted Partners: Human-Machine Learning and the Future of Military AI” (Center for Security and Emerging Technology, February 2021), <https://cset.georgetown.edu/>.
6. Wyatt Hoffman and Heeu Millie Kim, “Reducing the Risks of Artificial Intelligence for Military Decision Advantage” (Center for Security and Emerging Technology, March 2023), <https://cset.georgetown.edu/>; and Michael C. Horowitz and Lauren Kahn, “Leading in Artificial Intelligence Through Confidence Building Measures,” *The Washington Quarterly* 44, no. 4 (2021): 91–106, <https://doi.org/10.1080/0163660X.2021.2018794>.
7. Department of State, “Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy,” November 9, 2023, <https://www.state.gov/>.
8. Chinese Society of Artificial Intelligence (CSAI), 演讲实录 | 林建超 从‘围棋脑’到‘指挥脑’的跃升 [Speech record, Lin Jianchao, The leap from “go brain” to “command brain”], Sohu (see English translation), November 8, 2016, <https://www.sohu.com/>; and Elsa B. Kania, “China’s Rise in Artificial Intelligence and Future Military Capabilities,” in *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power* (Center for a New American Security, 2017), 8–32, <https://www.jstor.org/stable/resrep16985.6>.
9. CSAI, 演讲实录 | 林建超 从‘围棋脑’到‘指挥脑’的跃升 [Speech record, Lin Jianchao].

10. “DoD Announces Release of JADC2 Implementation Plan,” United States Department of Defense, news release, March 17, 2022, <https://www.defense.gov/>.
11. “Collaborative Combat Aircraft (CCA), USA,” *Airforce Technology* (blog), July 17, 2023, <https://www.airforce-technology.com/>.
12. Niniek Karmini and Margie Mason, “Inadequate Training Contributed to Boeing Crash in Indonesia, Report Finds,” PBS NewsHour, October 25, 2019, <https://www.pbs.org/>.
13. John K. Hawley, “Patriot Wars: Automation and the Patriot Air and Missile Defense System” (Center for a New American Security, January 2017), <https://s3.us-east-1.amazonaws.com/>.
14. Michael C. Horowitz and Lauren Kahn, “Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts” (arXiv, June 28, 2023), <https://doi.org/10.48550/arXiv.2306.16507>.

Chapter 2

Accessing the Brain to Affect the Mind

Neuroethics of the Mind-Tech Nexus in Military Contexts

James Giordano, Center for Disruptive Technology and Future Warfare, Institute for National Strategic Studies, National Defense University, Washington, DC

and

Departments of Neurology and Biochemistry, Georgetown University Medical Center, Washington, DC

Abstract

This chapter focuses upon current and emerging developments in neuroscience and technology (neuroS/T) as a most literal exemplar of “Mind-Tech” fusion. As introduction, a short definition of relevant terms (i.e., brain, mind) and their meaning(s) is provided to afford insight into the intended utility of neuroS/T as an applied toolkit. From this, a brief description of the assessment and interventional Mind-Tech capabilities is offered to illustrate the current state of the field and its capabilities, limitations, possibilities, and potential, both in ways promising and problematic for individual and public health, as well as national and global safety, security, and balances of multidimensional power. In light of the viability and considered value of Mind-Tech capabilities to be used in national security and defense initiatives, a discussion of the ethical and policy issues focal to these applications follows. I conclude with a proposal for ways that such issues can, and perhaps should, be addressed.

Neuroscience and Engineering as “Mind-Tech”

In addressing “Mind-Tech,” I use a most literal example, namely, the techniques and technologies that are developed to assess, access, and affect the brain and its functions (herein to be considered, somewhat colloquially as “mind”). To begin such a discussion, let us hold fast to

an adage that states that individuals have a brain, but they *are* a mind. So, the idea of the embodied mind—the connectivity between body and brain—which establishes dimensions of consciousness, cognition, emotion, and behavior, is critical. The embodied brain~mind is embedded in environment(s), and this bio-psychosocio-environmental reality reflects the lifelong interactions of one's internal ecology and their external surroundings, in and across scales, place, and time. This is not mere musing; it could rightly be stated that those techniques and technologies that are aimed at the brain to affect the mind (and body) are, at the most fundamental level, modifying the body's internal environments and responses to a host of external environmental conditions in and across a range of variable settings and conditions.¹

In the main, such Mind-Tech capabilities can be parsed into three major categories: (1) methods and tools that are used to assess the brain and its functions; (2) those that access and affect the brain and its functions; and (3) those that capabilize assessments and interventions (i.e., force multipliers such as big data, machine learning [ML], and artificial intelligence [AI]; for overviews, see²). When addressing how these approaches are engaged, it may be instructive—and not at all improper—to utilize military terms, not necessarily to assume a bellicose posture, but rather because such terms are applicable and currently employed in medicine, having been used for example to describe “batting against disease” and/or creating “targets” for intervention. Could such terminology also infer the possible viability and value of employing neuroS/T in operations and agendas that are vital to national security, intelligence, and defense? Indubitably, the short answer is yes. To be sure, ongoing advancements in neuroS/T and the use of such terminology are relevant to proposals and/or descriptions of current and emerging applications of the brain sciences in national security and defense scenarios, both as regards assessments of and interventions upon one's own forces, as well as means of influence, disruption, deterrence, and in some cases destruction, of at least certain parameters of the functionality of others (i.e., opposing forces; see³).

Taking these categories of neuroS/T in turn, let us begin with a brief overview of assessment technologies. These include various methods of assessing individual genetics, as well as collectives' and populational genomics. While genetic information is important, it is critical to note that genetics provide a blueprint of one's potential physical structures and functions, the expression and extent of which

are often reliant to a significant extent upon environmental factors. In addition to genetic assessments, forms of neuroimaging (including structural and functional magnetic resonance imaging, tractographic methods, and electrophysiological technologies and techniques such as electroencephalography [EEG] and more advanced iterations of EEG, including quantitative EEG [qEEG] and magnetoencephalography [MEG]) can be used either singularly or in combination to provide structural-functional correlational views of brain activities involved in mental and behavioral processes. Genetics and neuroimaging can be paired with assessment of various biomarkers; samples of tissues, fluids, functions, and structures can be utilized that allow proxy metrics for brain mechanisms,⁴ and which can be used to develop indices and ratios (of relative proxy substrate-to-brain functions) that are far easier to access and assess than having to actually “sample” the brain directly.

But recall that these are reconnaissance missions of a sort. By assessing these elements, we can identify potentially valuable targets for the next category of neuroS/T—the intervention toolkit. Herein are advances in pharmacologic developments, not just new drugs with greater specificity but also the technical means to increase the delivery and specificity of select agents, for example, by utilizing nanoengineering to create scaffolds and molecular chaperones so as to enable component agents that can enter the brain more freely, and auto-assemble on-site to build molecules, and which can now be delivered in lower doses.⁵ In other words, current developments in technology are allowing pharmacological science to be more akin to “sharpshooting” rather than “buckshot.”

Genetic techniques that have allowed mapping the genome can also be used to modify the genome. Ongoing work with Dr. Diane DiEuliis of National Defense University has addressed the relative facility of some of the newer gene editing techniques, for example, CRISPR Cas-9, not taken and used alone but employed in combination with the extant tools of monitoring and manipulating genetics to be able to more easily and quickly modify genes.⁶ And, if and when coupled to the methods of synthetic biology (and nanoscience, as mentioned above), these approaches can then be employed to modify the protein products that are important to the structural and functional characteristics of cells, organs, and organisms.⁷ Simply put, current capabilities in science and engineering can be used to modify structure and function in living organisms from the genetic to the cellular to the social levels.

There are also interventions through which the electrical activity and physiochemistry of the brain can be modulated via donable and doffable technologies, such as transcranial electrical and/or magnetic brain modulation and/or vagal nerve stimulation (tES, TMS, and VNS, respectively). These approaches modify patterns of node and network activity by affecting the more superficial layers of the brain (i.e., cortical layers) or by modulating the activity of the vagus nerve, affecting “downstream” pathways with which neural networks interact. While these methods have been shown to affect particular types and aspects of cognition and behavior (e.g., vigilance, endurance, and, in these ways, facilitation of learning, memory, and performance of certain tasks), their effects are somewhat diffused and appear to be contextually dependent.⁸

A more precise approach to modulating nodes and networks of the brain is achievable through forms of indwelling neuromodulation. Deep brain stimulation (DBS) has been used for several years with relative success in treating a variety of neurological and psychiatric conditions (e.g., movement disorders, impulse control disorders, certain forms of depression and anxiety). Ongoing developments in bioengineering, biophysics, computational science, and the neural sciences are enabling ever more sophisticated and capable advancements in DBS to allow greater specificity of effects using semi-closed, closed, and open loop systems (for an overview of these iterative developments, see the proceedings of the annual deep brain stimulation think tank that are serially published in *Frontiers in Neuroscience*).⁹

Perhaps the most cutting-edge of these methods of DBS is the attempt to combine nanotechnology with current engineering capabilities in computational data communication technology and an evolving understanding of the physics and chemistry of the brain to create very small-scale implantables that can be nonsurgically delivered to the brain in ways that are minimally invasive (for an overview of the current state of this S/T, see descriptions of the Defense Advanced Research Project Agency’s [DARPA] Next-Generation Noninvasive Neuromodulation [N3] Project¹⁰). The goal is to establish a vast array system of sensing and transmitting electrodes to be able to remotely read from and write into the living brain in real time. This allows a quantum leap in linking brains (and the organisms in which those brains are embodied) to machines—and not just to machines, as a physical entity, but to machine culture: to machine learning, computational technologies, and systems and, in these ways, linking humans directly with the sum of civilizations’ entire corpus of information (via

Web-based connectivities and bio-cognitive access at the cells-to-machine systems' scale).¹¹

Mind-Tech as Multinational Enterprise and Effect

The possibilities and potential applications made apparent by the near-term probabilities of such developments are extensive and can be viewed both in their beneficial as well as burdensome, if not risk-laden, manifest effects on individuals as well as systemically sociocultural levels.¹² Diane DiEuliis, Charles Lutes, and I have described ways that big data, machine learning, decision technologies, and AI are being utilized to increase the capability of the brain sciences, and we have called attention to the reality that these, too, can be leveraged in dually usable ways.¹³ Neurodata, for example, can be manipulated and changed to alter the social, political, legal, and military regard and treatment of individuals and collectives.¹⁴ And these data can be used to develop “precision pathologies” to selectively affect targeted individuals and/or groups. An example of this is the recent demonstration that some of the AI algorithms that were oriented toward producing viable pharmacologic therapeutics also began to develop agents that possessed highly injurious properties (i.e., which could be used as novel, “personalized” biochemical weapons).¹⁵

As the COVID pandemic has illustrated, bioscience and technology are multinational, both in effort and effects.¹⁶ Mind-Tech capabilities are merely an exemplar of this trend; there are a number of countries that have invested billions of their national currency in initiatives focused upon the brain sciences. Of note is China's growing effort and presence in this space.¹⁷ And while the primary Mind-Tech activities are being engaged by a number of developed nations, the manifest effects of research and application in the Mind-Tech Nexus are impacting the bioeconomies of developing and nondeveloped nations as well in ways that are influential to public health—and national, if not global stability—on and across a variety of scales.¹⁸

Given this multinational engagement of brain sciences, it becomes essential to appreciate the *multicultural*ity of those nations involved and their different histories, values, philosophies, ethics, needs, and means.¹⁹ And while there are certainly domains and dimensions of ethical overlap, there are also areas of distinction in ethical norms and practices. In the increasingly multinational environment of neuroS/T

research and uses in practice, what ethical system—or system—is to be utilized? To be sure, other nations have the right to pursue their own philosophical and ethical norms and standards, particularly as these relate to intranational issues.²⁰ But what of *intranational* pursuits that are then considered—and/or leveraged—internationally?

This prompts consideration of what philosopher Michel Foucault referred to as biopower and biopolitics, namely, exercising power by the implicit or explicit control of individual and collective biologies.²¹ Indeed, deliberately affecting biologies in ways that affect peoples' survival and flourishing is a potent exercise of force capability that can be used to establish one political system's and polis's hegemony over another and, in so doing, affect the key elements in the balance of power. Such engagement need not be kinetic, and recent activities in the non-kinetic space have strengthened the need to appreciate the Mind-Tech Nexus as a factor affecting military and geopolitical biosecurity on the current and future world stage.²²

Consideration of these capabilities should recognize and address collaboration, which entails cooperation: literally operations that are integrated in performance and/or orientation toward some common goal(s) and under some common ethos. But it is vital to equally consider—and appreciate—competition as so much collaborative effort is aimed at establishing competitive advantage(s) in and across economic, sociocultural, geopolitical, and military domains and dimensions. Apropos the co-extant realities of collaboration and competition, there is value, if not need, to gain insight into and respect for what has been called *coopetition*: intentional cooperative competition to establish checks and balances of those realms of leverage and hegemony so as to establish shared dependencies and, in this way, create something of an implicit if not explicit form of mutualistic Mind-Tech governance.²³

Mind-Tech in National Power Contexts

This dictates a view to the contingencies of constituencies, culture, circumstance, capitalization, contacts, and control, which influence the dynamics of international power. Clearly, a focal arena for such exercise of power is in military and intelligence operations, as relevant to any nation's security and defense. Competition and cooperation are axiomatic to postures of national defense and security. How, then, can and perhaps should these factors be taken into account and in-

corporated into an ethical system or systems—to guide research and uses of Mind-Tech developments within national security initiatives and operations?

Any genuine attempt in this direction must acknowledge that ethics must be focal and germane to the enterprise it serves. What does that then mean in an open liberal democracy such as that of the United States and many of its allies? What does that mean when competitors are not open and liberal democracies, and their ethics may afford them freedom from certain constraints, and thus particular advantages, or at least capabilities, in advancing these techniques and technologies in ways that could, in fact, be disruptive to democracies' own national security and public safety?

Playing a fundamental role in developing and distributing Mind-Tech capabilities is the multinational commercial enterprise, complete with particular intellectual property (IP) laws that make surveillance (for economic tracking and forecasting, systemic effect(s), and possible dual-use) somewhat difficult.²⁴ A basic worry in this regard is the development of Mind-Tech products absent orientation to, and/or consideration or concern for, their impacts upon nations' and regions' public safety and security. Instead, the underlying imperative is advancing these business enterprises to sate financial goals, irrespective of the intentions and motivations of the greatest bidder.²⁵

This is already evidenced in current trends in research and medical tourism, which brings into stark relief how distinctions in ethico-legal standards, norms, and practices can be exploited to national advantage. Near-peer competitor nations are offering positions, economic capability, and measures of notoriety to those multinational scientists being attracted and solicited to conduct research under ethical conditions that differ from those in their home countries. This practice has derisively been referred to as “ethics dumping,” but is it? Might it be that this has become the character of a new scientific opportunism? But with that comes the need to be aware that as far as IP law is concerned, “what gets done there is owned there,” and the leveraging of intra-nationally favorable IP laws has been called “lawfare”: the influence and use of local to global laws to advance a nation's interests and power.²⁶

On the technologically enabled twenty-first-century world stage, things developed in one place rarely, if ever, remain there. Distributive effects occur by active intent and passive diffusion, and, thus, the development of various Mind-Tech methods and tools translates

into disseminable products and services in multiple arenas of practice and manifest influence.²⁷ This sheds light upon growing concerns about S/T quality control on the one hand and, on the other, the direct use of these technologies to incur socio-economic, as well as perhaps more far-reaching disruptive effects in and among countries to which certain products are distributed; and these are not necessarily mutually exclusive. Even without devolving into dystopian scenarios of mind-reading and control from a distance, it is critical to appreciate that those neuro-technological devices have electronics that allow the sharing of data, as such data acquisition and exchange are essential to realizing a convergent scientific approach.²⁸ Who has custodianship and provenance of those data? What does the growing domain of available data mean for medical and social ecology and biosecurity on the global stage?

Given these realities, how can—and should—forward movement occur with probity, both in the Mind-Tech Nexus and those pursuits that are instrumental to public safety and health, national defense, biosecurity, and economics? It is not a question of should there be forward movement; that is a given, and the multinationality of commitment and effects relative to iterative bioeconomic trends and potential (and the fortification of other dimensions of power such as bioeconomic capabilities foster) flavor and fuel such endeavors. Inarguably, this “ship has left the dock,” and the nautical analogy is useful to posit another issue, which can be considered as a variant of what has been called the “lifeboat dilemma,” namely, what stays “in the boat” and what goes “over the side” (and what criteria will be used and outcomes desired) when it comes to selecting what ethics, policies, and/or laws will be respected, retained, revised, or replaced.²⁹ And in deciding upon these ethics, how could the United States’ and its international allies’ enterprises in Mind-Tech capabilities—and perhaps more specifically Mind-Tech relevant to national security and defense operations—“fight for right and freedom, and [still] keep our honor clean”?

Toward Preparedness

Any genuine attempt in this direction demands preparedness and responsiveness to idiosyncratic, as well as systemic benefits, burdens, risks, threats, and harms of the Mind-Tech Nexus—in and across

all of the domains and contexts of use.³⁰ Important, if not essential, to effecting this approach is a four-thrust paradigm, which entails

- (1) increasing awareness of the Mind-Tech Nexus, its actual capabilities and limitations, and where, how, and why it is being developed and utilized;
- (2) quantifying (measurable) benefit(s), burdens, risks/threats, and harms within particular timeframes, so as to be inclusive of the reciprocal S/T-socio-economic-politico-military influences that shape the dedication of resources in accordance with (nations' and groups') local, regional, and global goals;
- (3) mitigating risks, threats, and harms by employing equilibrium methods, which, when employed within a *minimax/maximin* framework (i.e., minimizing identified risks while maximizing identified benefits; and maximizing the benefit-effect to those sectors, groups, and individuals that heretofore have had the least opportunity for such provision), can be utilized in multinational discourses with the explicit aim of fostering cooperation by consensus; and
- (4) preventing future risks and threats by employing this process continuously, so as to meet various contingencies and exigencies “left of bang” (i.e., early in the change-crisis chain of events, before potent and/or wide-ranging impact) and with appreciation for the factors that affect the trajectory and valence of possible outcomes and consequences.³¹

If there is to be a reasonable effort toward consensus, then we opine two cornerstones must be in place. First is cooperation within the factions of government (i.e., a whole-of-government orientation) that allows more efficient and effective conjoinment of diverse national (and multinational) resources (i.e., a whole-of-nation[s] approach). The latter is critically dependent, to a large extent, upon the former. Current peer-competitor nations have rather seamless connectivity and capability within the “triple helix” model of function (governmental/politico-military, research/academic, and industrial-commercial). This allows for alignment between all sectors of capability in the implementation of short-, intermediate-, and long-term national and world-stage goals. Of course, I am not advocating a shift to an authoritarian governmental structure; to the contrary, there is demonstrable “hybrid vigor” in diversity of resources, views, and *proximate* values that are

inherent to working democracies. But without a definitive strategic plan that explicates common, long-range national *values' desiderata* that can be adhered to and worked toward in and between political parties and across successive administrations (without devolving to partisan myopia), the best that could be hoped for is achieving some tactical advantage, or at least temporary parity (that is likely to be short-lived) in the face of competitors' long-range visions, planning, enterprises, and achievements.

Second, any such strategic plan, and the tactical means to achieve it, must establish operational definitions of those “goods” desired, burdens that are acceptable or unacceptable, and harms to be reduced or avoided. In other words, common ethical foundations are needed upon which extant and evolving risk assessment and mitigation protocols can be based and employed in various multinational contexts.³² This ethical foundation must be internally capable as well as externally responsive and responsible.³³ Simply put, ethics can differ, and the tongue-in-cheek version of the “golden rule,” namely, “those with the gold rule,” most certainly should be appreciated when considering how regnant geopolitical, economic, cultural factors—and power—exert influence upon what ethical system(s) are being advocated and/or would be best suited for the challenge and opportunities of global discourses.

Whence Ethics?

The growing economic fortitude of China and the military flexing of Russia have made the “three body” problem (of physics and as applied to social and political sciences) more apparent,³⁴ and this complicates the formulation of a positionally polyglot ethics that is reasonable to meet current and near-term contingencies of culture, capability, cooperation, and competition. Prior proposals to adopt purely “Western” ethics were regarded (by China and other Asian nations) as disingenuous and without consideration of long-standing Asian culture(s), histories, philosophies, and ethics. An unconstructed and/or unprincipled approach to using “whatever ethical system works” has been rightly viewed as far too relativistic, perhaps *laissez-faire*, unreliable, and therefore ineffective in situations of ethical heterogeneity and dissonance.³⁵

Some balance must be struck. Indeed, ethics is all about balance: achieving a balance of benefits and burdens in situations and contexts

of both common and distinct values and standpoints so as to guide the avoidance of risks/harms of commission (i.e., those incurred by “doing something”) as well as omission (i.e., those incurred by “not doing something”) in and across defined (environmental) settings and time periods. Summarily, those are the tasks, and a complete discussion of ethical toolkits feasible for informing and directing the use of Mind-Tech advancements is beyond the scope of this chapter. Suffice it to note that our ongoing work has focused upon developing a somewhat Heraclitan paradigm (of appreciating the separate and interactive value of wholes and parts) that entails a cosmopolitan palette of (neuro)ethics, which can be duly employed in particular community circumstances in ways that obtain local as well as global utility and identifiable worth.³⁶

But there is a need to reinforce that ethics must be focal to (the purposes, goals, intrinsic tenets, and community of) the effort which it serves, or else it will fail to fully apprehend the realities of the enterprise and therefore be of little applied value. Mind-Tech can be addressed in light of individual and collective ethical issues, yet any such regard must also appreciate the context of the collective endeavor and the roles of individuals—both as persons as well as members of the collective community. When considering the use of Mind-Tech in the defense and security milieu, neuroethical issues, questions, and approaches to their resolution can be focused through a civilian and/or a military lens, and there is some overlap between these contexts of application (e.g., ethically responsible conduct of research; safety and effectiveness of Mind-Tech; certain aspects of clinical ethics).³⁷ However, there are also aspects that are distinct (e.g., military preventive/occupational medical applications [viz. performance optimization], preparedness for emerging neuroS/T threats, neuroweapon development, etc.).

Let us not be Pollyannish; the function of the military is to sustain a power advantage over defined and potential adversaries. In an open society, the role of the military is to protect the polis (and its ideals, ideas, and ideologies). But, given this relationship, the responsibility of the military *to* the polis also has increasingly prompted calls for accountability. Is this antinomic? In contemporary society, the ubiquity of information available to the public and ease of public access to information can make complete transparency of operational methods in national security and defense highly visible and hence vulnerable to capricious and/or nefarious surveillance, interference, or disruption. How can this balance of protective task-effectiveness and some measure of transparency be achieved, especially given that (1) current near-peer competitor

nations are authoritarian, and therefore their militaries serve to defend and advance political aims that are autocratically defined and dictated, and (2) ethical concepts of transparency are not wholly constituent to these systems of governance and military operations?

To reiterate, the professional ethics of the military should provide the basis for the focus and conduct of all its constituent scientific and technological enterprises. Classical ethical precepts relevant to the activities of military forces are certainly appropriate. For example, just war theory, *jus ad bellum*, may support the use of Mind-Tech capabilities in national security, intelligence, and defense operations, and constructs of fair conduct in conflict (i.e., *jus in bello*) could serve to describe if and how Mind-Tech applications could be utilized in warfare or to prevent warfare. The use of Mind-Tech in biomedicine would obtain that these techniques and tools should not be regarded as “harmful unto themselves,” but their use in military and defense settings is nonetheless considered, at least to some extent, as a “fuzzy boundary.” This is because while some aspects of the brain sciences are within the purview of the current treaties and signatory conventions regulating biochemical weapons and dual-use research (e.g., the Biological, Toxins, and Weapons Convention [BTWC], Chemical Weapons Convention [CWC], and dual-use research of concern [DURC] policy), many neurotechnologies do not, a fact well-noted by the Australian Delegation to the 2016 Review Conference of the BTWC.³⁸

When considering current and emerging Mind-Tech in this light, we have proposed key questions to guide such discussions (and what we would hope would be a dialectical engagement of the issues), to include whether such uses of certain Mind-Tech approaches incur greater or lesser risks and harms than other methods of intelligence, security, and defense and what limits should be applied to any possible development and use of brain science in defense initiatives.³⁹ Given the activities and results of various international conventions that have sought to govern military methods and weapons, we believe it will be vital to work to establish realistic criteria for the development and use of specific types (and extents) of Mind-Tech approaches within military and defense operations in accordance with strictly defined and implemented ethico-legal parameters.⁴⁰ Adherence to these parameters would then require programs of surveillance and rules for enforcement on a variety of scales and levels.

But upon what particular philosophy, military ethic, international law, or some other extant new and/or combinatory approach should

these ethico-legal constructs be based, and who shall be involved in such judgments and pronouncements? Any contributory deliberations must be engaged by dedicated groups of multidisciplinary professionals from both the government and civilian sectors, with experience and expertise essential to the use, constraints, and outcomes of Mind-Tech in national security and defense initiatives on the global stage. We have opined that these individuals and groups must be task-agile, scientifically and situationally knowledgeable, and ethically responsible, and we have proposed methods for training the personnel and executing the process.⁴¹ Case-based analyses informed at least in part by historical information provide a basis from which to assess the potential effects of current and emerging developments in Mind-Tech that can be employed in national security operations. However, ethical oversight is not solely based upon retrospection; rather, it must be forward-looking, descriptive, predictive, and not simply proscriptive but rather preparatory for contingencies and exigencies that can occur as the Mind-Tech Nexus and global politics and military operations evolve. Moreover, such ethical engagement should not be a merely academic exercise. It must be conducted by groups that have the credibility and capability to inform and influence the formulation of international policies, treaties, and laws.

A necessary step toward these ends is determining what Mind-Tech is in use, being considered for use, and the technological readiness level (TRL) of those methods and tools under consideration, as this would establish prioritization for ethical address. Timelines of capability, development, and applications-in-practice can be determined by assessment of the current maturity and anticipated maturational trajectory of particular types of Mind-Tech in light of contingency factors that affect maturation to operationalization in defined contexts. These variables can be plotted against (a) levels of control of provision and access of use as established by existing treaties and laws; and (b) relevant markets' influence (i.e., demand and relative power to affect access and use). This timeline can then be fitted to estimations of probability, possibility, and potentiality of relative benefits, burdens, risks, and harms in defined circumstances, inclusive of non-kinetic and/or kinetic military settings.⁴²

To engage this process will require infrastructure(s) capable of the tasks at hand and those to come. The 2014 US National Research Council report on *Emerging and Readily Available Technologies and National Security* addressed ethical, legal, and social implications (ELSI)

relative to government agencies' work in disruptive technologies of potential interest to both state and non-state actors (for overviews, see⁴³). The committee's recommendations included a five-step process: initial screening of proposed research and development; further review of proposals that raise ELSI concerns; project monitoring and mid-course corrections as needed; public engagement; and periodic review of ELSI processes within an agency. This is a fine start and a protocol that continues to be of merit. But which agency, institutions, or organizations should be charged with these duties? How will their constituencies be decided, and what level and extent of interagency and public discourse can and should be engaged? Differing groups may have distinct views and goals, and, as with any approach to national defense, issues of security, operational readiness, and power will need to be evaluated and weighed in light of evolving geopolitical trends as well as global humanitarian concerns.

Axiomatically, security and defense operations require that some information remain classified in order to establish and maintain preparedness and readiness for risk/threat contingencies and exigencies posed by current and emerging S/T. Hence, public discussion of programs of this sort, while necessary, must be carefully engaged. Informing the public about the reality and growing potential for brain science to be used in security, intelligence, and defense operations is strongly contributory to fostering broad social awareness of the importance, if not necessity, of these projects vis-à-vis meeting clear and present current and near-term global threats.

Toward these ends, we have proposed a "prudent parentalist" approach wherein the protective (i.e., parental safeguarding) role of the military (in an open society) extends to providing information necessary for public insight and consent to the tasks, ends, and means conducted within and by the military in exercising its duties.⁴⁴ In this sense, prudence entails particular restraint in what information remains classified and what "low side" knowledge can and should be provided to uphold the charge of protection (both [a] writ-large—viz. defending the nation and its people and [b] as regards making available information that is satisfactorily sufficient to meet public interest and concern, so as to enable the public to remain secure in the knowledge of the military's capability, comportment, and conduct, in this case, as relates to research and uses of Mind-Tech).

Conclusion

It is often the social impact of—and response to—the use or misuse of the tools and methods of military operations that gives rise to ethical and legal issues, questions, and concerns. There will always be a “court of social judgment” when it comes to the probity of military conduct. Thus, we do not see military and civilian silos of ethico-legal deliberation and guidance as mutually exclusive. Current intramural efforts at various national agencies (e.g., DARPA, the National Institutes of Health, and the National Science Foundation in the United States; Defense Research and Development Canada; UK Ministry of Defense; North Atlantic Treaty Organization, etc.) employing military and civilian subject matter experts dedicated to examining current and future ELSI generated by neuroS/T are noteworthy for implementing such integration. And while it is important to elucidate the ethical issues that arise in and from such research and its use, attention to ethics alone is insufficient. Ethics must inform and promote the formulation of policies, regulations, and laws that guide and govern how Mind-Tech capabilities are studied and used in military contexts.

As we have noted, rapid developments in Mind-Tech (together with other fields of bioscience) should encourage the re-examination and revision of extant treaties and conventions of bioweapon and dual-use research oversight and constraint.⁴⁵ As well, it may be that kinetic or certain types or gravitas of non-kinetic uses of Mind-Tech in military and/or intelligence operations may be viewed as provocative of conflict. Hence, it is likely that much of what will precede or follow in discussions of such use of Mind-Tech will likely center upon current *jus ad bello* (viz. just war) and *jus in bellum* (i.e., justifiable conduct of warfare) constructs. But while such discourse—and consideration and revisitation of these constructs—are worthwhile, a premier effort should be placed instead upon examining, defining, and enforcing those ways that Mind-Tech can and should be employed *jus contra bellum*: to prevent conflict and sustain peace.

Acknowledgments

Aspects of this work have been supported by funding from Award UL1TR001409 from the National Center for Advancing Translational Sciences (NCATS), National Institutes of Health, through the Clinical and Translational Science Awards Program (CTSA), a trademark of

the Department of Health and Human Services, part of the Roadmap Initiative, “Re-Engineering the Clinical Research Enterprise”; National Sciences Foundation Award 2113811—Amendment ID 001; the Henry Jackson Foundation for Military Medicine; the Institute for Biodefense Research; and Leadership Initiatives.

Notes

1. “Brain~mind” is used to denote a (true) complementarity of brain and mind in that they are interactive and bidirectionally effective, whereby one can exert effect upon the other (i.e., they are reciprocally supervenient, at least on certain levels and in particular dimensions). For further discussion, see James Giordano, “Complementarity, Brain-Mind, and Pain,” *Forschende Komplementärmedizin* [Research in complementary medicine] 15, no. 2 (2008): 71–73, <https://doi.org/10.1159/000121106>; Rachel Wurzman and James Giordano, “Explanation, Explanandum, Causality and Complexity: A Consideration of Mind, Matter, Neuroscience, and Physics,” *NeuroQuantology* 7, no. 3 (2009): 368–81, <https://www.academia.edu/>; Kathinka Evers and James J. Giordano, “The Utility—and Use—of Neurotechnology to Recover Consciousness: Technical and Neuroethical Considerations in Approaching the ‘Hard Question’ of Neuroscience,” *Frontiers in Human Neuroscience* 11 (2017): 564, <https://doi.org/10.3389/fnhum.2017.00564>; and Peter A. Moskovitz et al., “The Problem with the Hard Problem: Thoughts on an Oscillatory Theory of Consciousness,” *EC Neurology* 10, no. 4 (2018): 323–33, <https://www.researchgate.net/>.

2. James Giordano, “Integrative Convergence in Neuroscience: Trajectories, Problems and the Need for a Progressive Neurobioethics,” in *Technological Innovation in Sensing and Detecting Chemical, Biological, Radiological, Nuclear Threats and Ecological Terrorism*, NATO Science for Peace and Security Series, ed. Ashok Vaseashta et al. (Springer, 2012), 115–30, https://doi.org/10.1007/978-94-007-2488-4_10; James Giordano, “Neurotechnology,” in *Encyclopedia of Global Bioethics*, ed. Henk ten Have (Springer, 2016), 2010–17, https://doi.org/10.1007/978-3-319-09483-0_308; James Giordano, “Neurotechnological Progress: The Need for Neuroethics,” in *The Next Step: Exponential Life*, ed. Francisco González (BBVA Press, 2016), 295–312; and Diane DiEuliis and James Giordano, “Neurotechnological Convergence and “Big Data”: A Force-Multiplier Toward Advancing Neuroscience,” in *Ethical Reasoning in Big Data: An Exploratory Analysis*, ed. Jeff Collmann and Sorin Adam Matei (Springer, 2016), 71–80, <https://doi.org/10.1007/978-3-319-28422-4>.

3. James Giordano, ed., *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (CRC Routledge, 2015); and Joseph DeFranco et al., “Redefining Neuroweapons: Emerging Capabilities in Neuroscience and Neurotechnology,” *PRISM* 8, no. 3 (2019): 48–63, <https://ndupress.ndu.edu/>.

4. Kathinka Evers and James J. Giordano, “The Utility—and Use—of Neurotechnology to Recover Consciousness: Technical and Neuroethical Considerations in Approaching the ‘Hard Question’ of Neuroscience,” *Frontiers in Human Neuroscience* 11 (2017): 564, <https://doi.org/10.3389/fnhum.2017.00564>.

5. James Giordano et al., “Implantable Nano-Neurotechnological Devices: Consideration of Ethical, Legal, and Social Issues and Implications,” *Journal of Long-Term Effects of Medical Implants* 19, no. 1 (2009): 83–93, <https://doi.org/10.1615/JLongTermEffMedImplants.v19.i1.80>.

6. Diane DiEuliis and James Giordano, “Why Gene Editors Like CRISPR/Cas May Be a Game-Changer for Neuroweapons,” *Health Security* 15, no. 3 (2017): 296–302, <https://doi.org/10.1089/hs.2016.0120>; and Diane DiEuliis and James Giordano, “Gene Editing Using CRISPR/Cas9: Implications for Dual-Use and Biosecurity,” *Protein & Cell* 15 (2017): 1–2, <https://doi.org/10.1007/s13238-017-0493-4>.

7. Diane DiEuliis and James Giordano, “Regarding and Reducing Risks of the Biotechnology Revolution,” *NCT Journal*, no. 6 (June 2022): 2–6, <https://nct-cbnw.com/>.

8. James Giordano et al., “Mechanisms and Effects of Transcranial Direct Current Stimulation,” *Dose-Response* 15, no. 1 (2017), <https://doi.org/10.1177/1559325816685467>.

9. For example, see “Proceedings of the 10th Annual Deep Brain Stimulation Think Tank: Advances in Cutting Edge Technologies, Artificial Intelligence, Neuromodulation, Neuroethics, Interventional Psychiatry, and Women in Neuromodulation,” *Frontiers in Human Neuroscience* 16 (2022), <https://doi.org/10.3389/fnhum.2022.1084782>.

10. See DARPA, “N3: Next-Generation Nonsurgical Neurotechnology,” accessed January 2, 2025, <https://www.darpa.mil/>.

11. Roland Benedikter and James Giordano, “The Outer and the Inner Transformation of the Global Social Sphere through Technology: The State of Two Fields in Transition,” *New Global Studies* 5, no. 2 (2011), <https://doi.org/10.2202/1940-0004.1129>; and James Giordano and Roland Benedikter, “An Early – and Necessary – Flight of the Owl of Minerva: Neuroscience, Neurotechnology, Human Socio-cultural Boundaries, and the Importance of Neuroethics,” *Journal of Evolution and Technology* 22, no. 1 (December 2011): 110–15, <https://jetpress.org/>.

12. James Giordano and John R. Shook, “All Ethics Is Global: New Neuroethics in a Multipolar and Multicultural World,” in *Re-Globalization: New Frontiers of Political, Economic, and Social Globalization*, ed. Roland Benedikter et al. (Routledge, 2022), 106–16; and Prashant Desai et al., “Addressing and Managing Systemic Benefit, Burden and Risk of Emerging Neurotechnology,” *AJOB [American Journal of Bioethics] Neuroscience* 13, no. 1 (2022): 68–70, <https://doi.org/10.1080/21507740.2021.2001087>.

13. Diane DiEuliis et al., “Biodata Risks and Synthetic Biology: A Critical Juncture,” *Journal of Bioterrorism & Biodefense* 9, no. 1 (2018): 159, <https://doi.org/10.4172/2157-2526.1000159>.

14. Joseph P. DeFranco et al., “Neurodata: Realities and Risks,” *DefenceIQ* 13, no. 4 (2020).

15. James Giordano, “Weaponizing the Brain: Neuroscience Advancements Spark Debate,” *National Defense* 6 (2017): 17–19, 20, <https://www.nationaldefensemagazine.org/>; and Diane DiEuliis and James Giordano, “Balancing Act: Precision Medicine and National Security,” *Military Medicine* 187, Supplement 1 (2021): 32–35, <https://doi.org/10.1093/milmed/usab017>.

16. Diane DiEuliis and James Giordano, “COVID-19: Lessons to Be Learned for Biosecurity and Future Operational Environments,” *Journal of Defense Research and Engineering* 8, no. 3 (2020); Diane DiEuliis et al., “Of Nemesis and Narcissus: Lessons COVID May Provide for Enterprises – and Ethics – of Global Health Promotions and Biosecurity,” in *Medicine and Ethics in Times of Corona*, ed. Martin Woesler and Hans-Martin Sass (LIT Verlag, 2020), 323–29, <https://www.researchgate.net/>; and Vikram Venkatram et al., “The COVID Crisis: Implications and Lessons for United States’ – and Global – Biosecurity,” in *COVID-19: Analysing the Threat*, ed. Ajey Lele and Kritika Roy (Pentagon Press, 2020), 397–405.

17. Celseste Chen et al., “Biotechnology, Commercial Veiling, and Implications for Strategic Latency: The Exemplar of Neuroscience and Neurotechnology Research and Development in China,” in *Strategic Latency: Red, White and Blue: Managing the National and International Security Consequences of Disruptive Technology*, ed. Zachary

S. Davis and Michael Nacht (Lawrence Livermore Press, 2018), 12–32, <https://cgsl.llnl.gov/>; and L. R. Bremseth and James Giordano, “What COVID-19 and China’s Grand Strategy May Teach About a History of the Future,” in *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order*, ed. Zachary S. Davis et al. (Lawrence Livermore Press, 2021), 109–20, <https://cgsl.llnl.gov/>.

18. Joseph P. DeFranco et al., “The Emerging Neurobioeconomy: Implications for National Security,” *Health Security* 18, no. 4 (2020): 66–80, <https://doi.org/10.1089/hs.2020.0009>.

19. John R. Shook and James Giordano, “A Principled and Cosmopolitan Neuroethics: Considerations for International Relevance,” *Philosophy, Ethics, and Humanities in Medicine* 9, no. 1 (2014): 1, <https://doi.org/10.1186/1747-5341-9-1>; Elisabetta Lanzillo et al., “Advancing Neuroscience on the 21st-Century World Stage: The Need for and a Proposed Structure of an Internationally Relevant Neuroethics,” *Ethics in Biology, Engineering and Medicine: An International Journal* 4, no. 3 (2013): 211–29, <https://doi.org/10.1615/EthicsBiologyEngMed.2014010710>; and James Giordano, “Looking Ahead: The Importance of Views, Values, and Voices in Neuroethics—Now,” *Cambridge Quarterly of Healthcare Ethics* 27, no. 4 (2018): 728–31, <https://doi.org/10.1017/S096318011800021X>.

20. John R. Shook and James Giordano, “Toward a New Neuroethics in a Multipolar and Multicultural World,” *Global-e* 13, no. 56 (2020), <https://globalejournal.org/>.

21. Michael Foucault et al., ed., *Security, Territory, Population: Lectures at the Collège de France 1977–1978*, trans. Graham Burchell (Palgrave, 2007).

22. Joseph P. DeFranco, “Emerging Technologies for Disruptive Effects in Non-kinetic Engagements,” *HDIAC* [Homeland Defense and Security Information Analysis Center] *Currents* 6, no. 2 (2019): 49–54, <https://hdiac.dtic.mil/>.

23. Adam Brandenburger and Barry Nalebuff, *Co-Opetition: A Revolution Mindset that Combines Competition and Cooperation* (Crown, 1996), 34; and V. Frank Asaro, *Universal Co-Opetition: Nature’s Fusion of Cooperation and Competition . . . and How It Can Save Our Finances, Our Families, Our Future and Our World* (Betty Youngs Book Publishers, 2011).

24. Chen et al., “Biotechnology, Commercial Veiling”; and Joseph DeFranco and James Giordano, “Mapping the Past, Present, and Future of Brain Research to Navigate the Directions, Dangers, and Discourses of Dual-Use,” *EC Neurology* 12, no. 1 (2020): 1–6, <https://ecronicon.net/>.

25. DeFranco et al., “Emerging Neurobioeconomy.”

26. Charles J. Dunlap, “Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts” (paper presented at the Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy, Kennedy School of Government, Harvard University, MA, November 29, 2001), <https://people.duke.edu/~pfeaver/dunlap.pdf>.

27. Guillermo Palchik et al., “Monkey Business? Development, Influence, and Ethics of Potentially Dual-Use Brain Science on the World Stage,” *Neuroethics* 11, no. 1 (2018): 111–14, <https://doi.org/10.1007/s12152-017-9308-9>.

28. James J. Giordano, ed., *Neurotechnology: Premises, Potential, and Problems* (CRC Press, 2012), <https://doi.org/10.1201/b11861>.

29. John R. Shook and James Giordano, “Ethics Transplants? Addressing the Risks and Benefits of Guiding International Biomedicine,” *AJOB* [American Journal of Bioethics] *Neuroscience* 8, no. 4 (2017): 230–32; and Daniel Gerstein and James Giordano, “Rethinking the Biological and Toxin Weapons Convention?” *Health Security* 15, no. 6 (2017): 638–41, <http://dx.doi.org/10.1089/hs.2017.0082>.

30. Desai et al., “Addressing and Managing Systemic Benefit.”

31. DeFranco et al., “Emerging Technologies for Disruptive Effects”; and DeFranco and Giordano, “Mapping the Past, Present, and Future.”

32. James Giordano, “Battlescape Brain: Engaging Neuroscience in Defense Operations,” *HDIAC Journal* 3, no. 4 (Winter 2017): 13–16, <https://hdiac.dtic.mil/>.

33. John R. Shook and James Giordano, “Neuroethical Engagement on Interdisciplinary and International Scales,” in *Debates About Neuroethics*, ed. Eric Racine and John Aspler (Springer, 2017), 225–45, https://doi.org/10.1007/978-3-319-54651-3_16.

34. David Belorizky, “Application Pratique des Méthodes de M. Sundman à un Cas Particulier du Problème des Trois Corps” [Practical application of Mr. Sundman’s methods to a particular case of the three-body problem], *Bulletin Astronomique* 6 (January 1930): 417–34; and Cixin Liu, *The Three-Body Problem*, trans. Ken Liu (Macmillan, 2006).

35. Lanzilao et al., “Advancing Neuroscience.”

36. Shook and Giordano, “Principled and Cosmopolitan Neuroethics”; Lanzilao et al., “Advancing Neuroscience”; and Shook and Giordano, “Neuroethical Engagement.”

37. Michael Tension et al., “Security Threat Versus Aggregated Truths: Ethical Issues in the Use of Neuroscience and Neurotechnology for National Security,” in *Neuroethics: Anticipating the Future*, ed. Judy Illes and Sharmin Hossain (Oxford University Press, 2017), 531–53, <https://doi.org/10.1093/oso/9780198786832.003.0027>.

38. Gerstein and Giordano, “Rethinking the Biological and Toxin Weapons Convention?”; DiEuliis and Giordano, “Why Gene Editors Like CRISPR/Cas9”; and DiEuliis and Giordano, “Gene Editing Using CRISPR/Cas9.”

39. Giordano, *Neurotechnology in National Security and Defense*.

40. Gerstein and Giordano, “Rethinking the Biological and Toxin Weapons Convention?”; DiEuliis and Giordano, “Why Gene Editors Like CRISPR/Cas9”; and DiEuliis and Giordano, “Gene Editing Using CRISPR/Cas9.”

41. Rochelle E. Tractenberg et al., “Emerging Neuroethical Issues Generated by the Use of Neurotechnology in National Security and Defense: Toward Process, Methods, and Paradigm,” in Giordano, *Neurotechnology in National Security and Defense*, 259–78.

42. DeFranco et al., “Emerging Neurobioeconomy”; and DeFranco and Giordano, “Mapping the Past, Present, and Future.”

43. Rachel Wurzman and James Giordano, “‘NEURINT’ and Neuroweapons: Neurotechnologies in National Intelligence and Defense,” in Giordano, *Neurotechnology in National Security and Defense*, 79–114.

44. James Giordano et al., “Neuroscience, Neurotechnology, and National Security: The Need for Preparedness and an Ethics of Responsible Action,” *AJOB* [American Journal of Bioethics] *Neuroscience* 1, no. 2 (2010): 35–36, <https://doi.org/10.1080/21507741003699397>.

45. Gerstein and Giordano, “Rethinking the Biological and Toxin Weapons Convention?”

Part 2

**COMMAND, CONTROL, AND
INTELLIGENCE IN THE NEW
FOG OF WAR**

Chapter 3

Intelligence and the Mind-Tech Nexus

History and Futures

Sir David Omand, War Studies Department, King's College London; former director, GCHQ (the UK Signals Intelligence and Cyber Security Agency).

Abstract

The history of intelligence has lessons for the Mind-Tech Nexus. Successive waves of scientific and technological innovation, from the introduction of the electric telegraph to the Internet and digital mobile devices, have been quickly exploited by intelligence agencies to provide access to the secrets of adversaries. Future scientific breakthroughs in the Mind-Tech Nexus (for example, generative AI and exploiting quantum computing at scale) must be expected similarly to provide a novel information advantage. Intelligence history also shows how powerfully technologies are developed when they have dual military and commercial applications and how even highly classified capabilities eventually become commercialized.

We can be sure that our intelligence communities will be in the forefront in exploiting current developments related to the interface of human and machine—what we are calling the Mind-Tech Nexus. Intelligence officers have creatively exploited successive scientific and technological breakthroughs over the last 150 years in the hope of establishing information dominance over the adversaries of the day. I write as a former British defense, security, and intelligence practitioner now teaching intelligence studies in the War Studies Department at King's College London. From this 150-year history, I suggest insights relevant to the current Mind-Tech debate. To give an outline of this history, we can begin with the symbiotic relationship between tech and intelligence that took shape during the American Civil War and the later Franco-Prussian war of 1870 as the products of the first industrial revolution were applied to large-scale armed conflict. The First World War then deepened that relationship

of technology with warfare and with the supporting arm of intelligence. That was when we saw the start of the intelligence exploitation of radio interception, direction finding, and aerial reconnaissance. The search for ever more advanced methods for conducting these activities dominated the US, Soviet, and UK intelligence budgets during the Second World War, Korean War, and Cold War. The Second World War also saw advances in machine-assisted cryptography that were central to establishing the US-UK relationship in signals intelligence and other forms of tech-enabled intelligence. As communications moved from the radio age to the Internet and World Wide Web, digital technology provided vital intelligence leads for counterterrorism and combatting criminality and cyberattacks, expanding the discipline of secret intelligence.

The Uses of Intelligence

This impression of historical progression, especially under the spur of conflict, should not surprise us.¹ Over the course of history, gifted human beings, learning of the latest scientific developments, have sought to find novel ways of applying technological innovation to improve their knowledge of the external world beyond the range of what their immediate senses could tell them about the Mind-Tech Nexus. More often than not, the challenge of supporting armed forces in war or impending conflict has forced innovation. The development of scientific intelligence as a discipline came directly from the experiences on both sides of the Second World War, first in technological innovation and subsequently in developing countermeasures.²

The fundamental evolutionary advantage of human intelligence can be thought of as enabling safer, more timely decisions by reducing the ignorance of decision-takers of the dangers they face and the opportunities they may seize. We can imagine that premise being the case for our hunting ancestors, helping to explain the evolutionary path that has shaped our reasoning faculties, such as the ability to think fast when in danger.³ Today, military commanders, government ministers, police officers, and business leaders—and all of us—must also think slowly, benefitting from knowing more about the context and history of the threatening situations we face and the potential opportunities that, if given strategic notice, we may be able to seize.

Science has assisted in that objective—indeed, that need to understand and control the world around us could be considered the main driver behind scientific exploration and its exploitation through technology. In that sense, I could have started this account at any point since the Renaissance. To illustrate, in 1608, remarkable developments in the science of optics engendered the invention (and patenting) of the telescope in the Netherlands. Galileo used it in Italy the following year to expand his knowledge of the universe and, in that quest, discover the existence of Jupiter’s moons. Military commanders were quick to adopt the technology to spy out the land (with improved binocular vision from 1825 onward to add depth of field) and to assess the dispositions of enemy and friendly forces on the battlefield. Sea captains were obvious early adopters, using the technology to detect hostile ships appearing over the horizon. They rapidly adopted another extraordinary breakthrough—John Harrison’s timekeeper that, for the first time, allowed determining a ship’s longitude at sea. This example shows how the prospect of financial reward can force innovation: Harrison’s invention came in response to a national competition under an act of Parliament offering prize money for a solution.⁴

If the general purpose of intelligence lies in improving the quality of decisions, that of *secret* intelligence is to achieve that objective with respect to a special kind of knowledge—secrets. This category comprises information that others want to hide from us—and may go to violent lengths to prevent us acquiring. Here the intelligence-tech nexus is about how technology can help overcome the obstacles that adversaries deliberately place in our path to obscure our clear view of their capabilities and intentions, such as concealment, camouflage, deception, encryption, encipherment, and steganography.⁵

Secrets are usually entrusted only to a few carefully chosen people. The more people a secret is shared with, the more likely that a weak link will be found where an attacker can gain access. We can think of this outcome as an inverse form of Metcalfe’s law that relates the value of a network to the square of the number of nodes in it.⁶ In the case of keeping secrets, fewer nodes reduce the likelihood of successful recruitment of secret and double agents. Such human intelligence gathering carries all the dangers of discovery. But General George Washington well understood its value during the War of Independence, for example, from his Culper spy ring, including being tipped

off that the American officer and war hero Benedict Arnold was going to turn traitor.

The Requirement Not Just for Information but for Timely Information

The smart application of technology has helped intelligence officers overcome the will of those determined to keep their secrets by providing ever more ingenious ways of stealing the information, preferably without that fact being known by the owner of the secret. Technology has also been ransacked for ideas on how to shorten the latency of such information, the gap between the time and date associated with the information itself and when the analyst can safely receive it in useable form after transmission, processing, decryption, and translation.⁷ The two key parameters, latency and safety, are often in conflict in covert intelligence operations.

Radio sets built into suitcases became standard issue during the Second World War for communication between agents in France, Norway, and other Nazi-occupied territories and their controlling organizations in London. But the race was on as countertechnology was developed to enable mobile detection vans to pick up and triangulate even brief Morse high-frequency transmissions. Risks increased when tactical intelligence had to be passed quickly to be of value (such as when the German battleship *Tirpitz* was spotted by the Norwegian resistance leaving the shelter of a fjord in Norway). Security of human sources also demands some form of Cold War “Moscow Rules”⁸ to minimize the risks of agents being spotted meeting their intelligence case officers and the use of cutout tradecraft (such as brush contacts, dead drops, and microdots hidden under stamps on letters with messages encoded with onetime cypher pads). The Cold War spy versus counterspy battle illustrates a truism of the application of the Mind-Tech Nexus to the domains of defense, intelligence, and security: an arms race is always going on as adversaries innovate in turn to try to frustrate any advances being made.

Six and a Half Scientific Revolutions

At the risk of oversimplification, the principal lines of development of secret intelligence over the last 150 years can be ascribed to the ap-

plication of six scientific revolutions—with a seventh underway, and with the Mind-Tech Nexus possibly a further technological upheaval just beginning as I write. No doubt there will be others yet to be imagined.

The first scientific revolution was triggered by the invention of the electric telegraph. In 1844 Samuel Morse sent the first public communication over the new electric telegraph from Washington to Baltimore (“What hath God wrought” was the message), and the technology passed quickly into commercial use. A decade later, the advantages of swift long-distance communication were obvious to Union and Confederate armies during the Civil War as they sought to track the movements of their opponents. The telegraph certainly changed the relationship between President Abraham Lincoln and his generals during the Civil War, providing for the first time the ability to quickly turn strategic direction into campaign plans and then swiftly adjust as the telegraph carried back the results from the battlefield.

Another remarkable example of how the pressure of war encourages the exploitation of technology was the Union and Confederate forces’ deployments of balloons for battlefield observation. In the case of the Union Balloon Corps, observation results were relayed back to the ground in near real time using cables and Morse code. Although the value of such tactical reconnaissance was evident, it took the early twentieth-century coincidence of the discovery of radio and heavier-than-air flight to allow mobile aerial reconnaissance to be developed during the First World War.

Lincoln took a keen interest in the innovation of long-distance telegraphic communication—and significantly, in its interception—and spent more of his presidency in the War Department’s telegraph office, where he had a bed, than anywhere else outside of the White House.⁹ We can compare Lincoln with Prime Minister Winston Churchill during the Second World War spending long periods during the afternoon (with the cover story of sleeping off lunch) studying the Enigma decrypts of German strategic communications obtained by Bletchley Park. Both cases provide a lesson in the advantage of having top-level political support for rapid development of the tech-intelligence nexus.

We should also recognize that any new technology, such as the electric telegraph, always brings with it risks and vulnerabilities as well as offering opportunities. The improved speed of communications, carrying both intelligence and battlefield situational awareness, could tempt political leaders and their legal advisers to insert their long screwdrivers and demand a say, for example, in tactical target selection

or in second-guessing operational theater decisions, thinking—usually mistakenly—that they have all the information they need to take such decisions. Today—even with digital broadband communications—high command should set the strategy while field commanders and the chain of command should execute it. This delegation assumes that commanders have timely access to strategic and tactical intelligence generated by their own forces. Mission command can then provide the vital advantage of flexibility, as in the case of Ukrainian forces versus the rigid, top-down doctrine hampering the responsiveness of Russian forces.

In the United States, the president's role as commander in chief may nevertheless push operational decisions to the top, as President Jimmy Carter found when, from the White House, he had to order abandoning the 1980 Iranian hostage rescue operation. One hundred and fifty years after Lincoln, we have the iconic photograph of President Barack Obama in the White House Situation Room with his Secretary of State and senior advisers watching the Navy SEALs' raid on bin Laden's hideout unfold in real time. Thankfully, despite the crash of one of the helicopters, no intervention from the White House was necessary during the operation.

The second scientific revolution that I see as foundational in modern intelligence practice follows the discovery of what today we know as radio waves with Hertz's 1886 experimental vindication of Clerk Maxwell's equations. Less than a decade later, in 1895, Marconi demonstrated practical radio transmission to the British government and, two years later, achieved the first transmission over open water.¹⁰ The German Navy was an early adopter of radio in their capital ships, and the Royal Navy quickly recognized that radio transmissions from warships could be triangulated to reveal their position at sea. The world's first signals intercept station was established in 1914 by naval intelligence at Scarborough on the English North Sea coast to determine when the German High Seas Fleet was at sea.¹¹ By the time General Pershing landed in London in May 1917 to organize the American Expeditionary Force's arrival the following year, his plans already included trucks equipped as mobile radio interception units and a cryptographic team led by the brilliant young William Friedman (the first to coin the term *cryptanalysis*). Friedman later distinguished himself as the US end of the Enigma partnership with the UK's Government Communications Headquarters (GCHQ).

Today's Mind-Tech Nexus also concerns how to use information to the greatest advantage. An early example is German foreign secretary Arthur Zimmerman's offer to the president of Mexico in 1917 that the lost territories of Texas, New Mexico, and Arizona would be returned if Mexico joined the war on Germany's side. British naval intelligence intercepted Zimmerman's telegram to that effect from the transatlantic cable and decoded it. Subsequently, the message was shared with President Woodrow Wilson, who promptly made it public to justify US entry into the war. We can see the British operation as an early example of what today is termed exploiting "malinformation."¹² Fast-forward to the White House statement in February 2022 that Russia was preparing a false-flag operation to provide a pretext for the imminent Russian invasion of Ukraine.¹³ The statement deliberately made public the content of intelligence reporting to shape Western opinion.

A third transformational era of intelligence comes with the technological advances made during the Second World War. Alan Turing's early theorizing about how a universal machine could be constructed to solve a problem evolved into the first practical use of machines for cryptanalysis. That breakthrough led to the concept of the programmable computer, with the Colossus cypher-breaking machine developed at Bletchley Park as the very first. The underlying technology to allow faster, more powerful machines quickly developed in parallel, including the construction of thermionic valves, first for radar and then for communications and computing. A general lesson learned during that war was the value of "industrializing" intelligence processes in ways familiar from Henry Ford's pioneering prewar motor car manufacture. By 1945 more than 10,000 people worked at Bletchley Park, and probably even more were employed in the systematized collection and transmission of raw intercept back to Bletchley Park from the many collection sites that had been built.

Yet at the same time as Alan Turing and his colleagues at Bletchley Park were envisaging how new technology could help win the battle of the Atlantic, German cryptographers were routinely reading the cyphers of the Royal Navy during the failed British campaign in Norway.¹⁴ Not enough effort went into thinking about *our* vulnerabilities; enemy capabilities were underestimated, and it is doubtful whether those in charge of naval cyphers even knew what advances Bletchley Park was making in attacking machine cyphers. The enduring lesson is that the application of technology for the offense should not blind us to our own vulnerabilities or to the same technology being deployed against us.

A contemporary example is the way that zero-day vulnerabilities in software discovered and deployed can rebound against the attacker.¹⁵ Russia's notorious use of the NotPetya virus (causing over \$10 billion of damage to global industry) was enabled by the EternalBlue vulnerability, said to have been discovered by the National Security Agency but then stolen.¹⁶ I am tempted to call this the quintain effect after the device used to train medieval knights on horseback, where they attempted to hit a shield on a rotating arm with a heavy weight on the other end. Anything other than a perfect hit would result in the swinging weight knocking the rider from his saddle. We need to therefore assess how technology we pioneer can come to represent a vulnerability for us.

Nor does the latest technology stay exquisite for long. Once used, it can be reverse engineered or simply copied. Over time, it becomes commonplace and is more easily and cheaply replicated. The pioneering combination of the Reaper drone with Hellfire missiles proved devastating against al-Qaeda's senior leadership after 9/11. Today, Iranian kamikaze drones applying the same technologies are relatively cheap (certainly when measured against the cost of air defense systems) and in Russian hands are seriously damaging the Ukrainian power infrastructure. A key lesson in considering the Mind-Tech Nexus that comes from such examples is how cutting-edge technology, often emerging from defense research labs, quickly becomes ubiquitous and often finds dual uses in the commercial marketplace.

A fourth revolution that transformed intelligence activity started in the early 1950s with William Shockley and the invention of the transistor as a replacement for the vacuum tube or valve. Vacuum tubes had powered Colossus at Bletchley Park and the radio receivers in the early Cold War intercepting the communications of the Warsaw Pact. Emitting heat, bulky, and fragile, valves were a limiting factor. But by applying knowledge of quantum mechanics, it proved possible to design semiconductors that sandwiched together could create a device that allowed electricity to flow only in one direction—creating what became known as the transistor. Small yet rugged, these devices could be miniaturized and packed tightly together to create solid-state electronics. It became feasible to build complex sensors that could be fitted on reconnaissance aircraft and, eventually, placed in orbit in satellites.

The result was a transformation of espionage as both sides in the Cold War launched constellations of satellites—geostationary, low Earth, and elliptical orbiting—to collect every kind of electromagnetic

emission, communications, radar, visual and infrared. The cost was astronomical and dominated intelligence budgets for decades. One consequence was an imbalance in the ratio of expenditure on the collection of intelligence to that spent on analysis to interpret and understand the data. Those involved in Mind-Tech development will need to avoid the danger of not having sufficient capability to exploit technological breakthroughs.

Another lesson from that period of history is how the very existence of such space surveillance (and its capabilities in terms of resolution and dwell time) started as highly classified compartmented secrets. But the technology had huge commercial applications, incentivizing private sector investment and thus creating a new marketplace for imagery. Today, commercial imagery and mapping comprise important classes of open-source intelligence, available to anyone for a fee or, in the case of Google, for free at the point of use and paid for by advertising revenues.

A fifth scientific revolution with transformational effects still being felt was the first quantum revolution of the early 1950s, which I associate especially with Nobel laureate Richard Feynman's discovery of quantum electrodynamics (QED—the theory that governs the interaction of light with matter). By the 1960s, that new knowledge had led to the tunable laser, enabling writing, storing, and retrieving data—a vital capability for intelligence and security agencies—at volumes and speeds far exceeding earlier devices. The laser also fostered the precision manufacture of printed circuits, packing increasingly more components into integrated microchips, following Moore's Law.¹⁷

An understanding of QED also led by the 1970s to laser diodes able to transform electricity into photons of light capable of being pumped into fiber-optic cables made of ultra-transparent glass. Now, fiber-optic cables circle the earth and enable global communications, commerce, and capital markets to flourish. Data can be stored in bulk and rapidly communicated, greatly benefitting the “Five Eyes” signals intelligence partners.

One striking feature of this optical revolution was dual-use technologies. Research and development were no longer confined to highly classified projects in defense laboratories. The technology had huge commercial value, first in business and then quickly in the mass market, where compact discs and DVDs became popular with music and entertainment consumers. Consequently, intelligence agencies have become increasingly dependent on the results of commercial investment in the relevant technologies, and they now look to external suppliers

for expertise and products. This is likely to also become the case for developments in the Mind-Tech Nexus.

We can also see the outlines of how the so-called second quantum revolution that followed (one that I associate with the theorem named after the Northern Irish physicist John Stewart Bell¹⁸) has led to the technology of “unbreakable” quantum encryption. China already has in space the Micius satellite capable of relaying quantum encryption keys to a network of ground stations separated by more than 1,000 kilometers. Quantum computing on the other hand has only been demonstrated at small scale. The technology does not yet exist to allow large-scale computations with efficient error correction. When that day arrives, in addition to its immense value in tackling previously infeasible computations, quantum computing may render transparent much of the public key encryption protecting global finance and commerce as well as diplomatic and military activity of intense intelligence interest. More fundamentally, for the Mind-Tech Nexus, quantum computing at scale opens up the likelihood of previously computationally infeasible calculations being tractable. That result would allow large multiscale simulations for the brain itself.¹⁹

A sixth wave of twentieth-century technologies has now transformed secret intelligence—as it has the fabric of everyday life—with the development of the Internet and the World Wide Web. We are living through the age of the Internet, packet-switched networks, mobile devices, public key encryption, and the web that started to take shape in the 1990s. This technology provides constant connection, abolishing barriers of time and space. By 2030 the Internet of Things is expected to comprise over 40 billion individual devices that have an IP address.²⁰ The key enablers have been

- digitization, enabling all forms of information—text, pictures, video, sound, experimental results, Internet usage, DNA, and much else—to be rendered into numbers that can be cheaply stored, communicated, data mined, and correlated;
- open protocols so that any network using TCP/IP, BGP, etc., requires no permission to connect seamlessly to the Internet;
- the built-in anonymity of the Internet with the domain name system connecting devices, not individuals;
- the packet-switched networks allowing global connectivity at unparalleled scale and pace; and

- public key encryption enabling online commerce and finance but also capable of providing strong end-to-end protection for private communications.

As the Cold War came to an end, demands increased for intelligence on individuals of interest (autocrats, serious criminals, terrorists, money launderers, cyber criminals, etc.). By a global coincidence, the Internet started to be widely used in this era, with the personal data of users being captured and mined for its advertising value. Intelligence and security agencies began to access information on individuals of interest—such as their location, identities, movements, Internet usage, and spending—producing unprecedented insights into the private lives of their suspects. The downside of the technology has been the vulnerabilities it creates for the exploitation of personal data for criminal gain and the opportunities offered to hostile states to interfere covertly in democratic debates and processes.

In the early twenty-first century, therefore, the intelligence and security activity of democratic states began to impact at scale the privacy rights of their citizens. The ethics of activities such as bulk data interception have become contested. The response of the liberal democracies has been to legislate and regulate such intrusions under the rule of law and introduce independent judicial oversight to provide a check on the use of this potential state power.²¹

The ethical lesson is a general one that applies to future developments in the relationship between mind and technology. When intelligence draws on technology capable of affecting citizens and their everyday rights, then (in the democracies) there needs to be trust in the motives of the authorities in allowing the technology to be deployed. There must be a transparent ethical code governing the application of the technology. Work needs to be conducted under the rule of domestic law with regulation and oversight under the ethical code to ensure public confidence in those conducting the activity. As new technologies are harnessed, including artificial intelligence programs, public support depends on applying that principle.²²

Looking Ahead

The pace of innovation has not slackened following the six science and tech revolutions. We are already in the early stages of a further wave of innovation with machine learning and AI algorithms being applied

for intelligence, security, and law enforcement purposes. The rapid advances in AI will have profound implications, and we must expect controversy over the use of these technologies for routine intelligence, security, and law enforcement purposes. Advanced AI-driven facial recognition software provides a current example.

The experience of past scientific revolutions should prompt questions about how we can speed applications through dual-use technology. Today, the United States has the Defense Advanced Research Project Agency (DARPA), the Intelligence Advanced Research Project Agency (IARPA), and the DOD Defense Innovation Unit (DIU). They can set up Mind-Tech sandboxes to test the second- and third-order effects of new ideas and run imaginative exercises with cognitive experts and technologists—and even some science fiction writers.

Looking ahead, we can be confident there will be scientific breakthroughs in fundamental research and in bringing together disparate fields to create new insights. Neuroscience—at the heart of speculation about the development of the Mind-Tech Nexus—is one such area. More efficient and direct person-machine interfaces, for example, and visualization technologies in virtual reality would transform the work of the intelligence analyst. Who knows, one day it may speed up the maximum processing speed of the human brain (currently estimated to be around 60 bits per second). But the lessons from the past will still apply.

Points to Ponder

Many lessons can be drawn from these examples of technology interacting with the worlds of intelligence and security. We can see the rapidity with which each scientific advance has been turned into useable technologies for espionage and military reconnaissance. Otherwise traditionally minded intelligence agencies have displayed remarkable open-mindedness in harnessing these technologies—not least in the ingenuity demonstrated by the real-life counterparts of James Bond's Q in using the latest technology to support the craft of espionage.

We should continue to expect a dynamic interaction between the changing demands of the users of intelligence—civilian and military—for more detailed and current information on their adversaries, on the one hand, and the supply opportunities offered by technological advance on the other.²³ Sometimes the driver of change will be new and more urgent demands leading to the development of novel

technological solutions exploiting new science (such as the way that the need to find intelligence from inside the vast Soviet Union stimulated the creation of space reconnaissance capabilities). Sometimes it will be the other way around, where new commercial technologies become available that the intelligence world adapts to use for its purposes (such as recent steps to derive intelligence from the use of social media). More often it will be a dynamic interaction between supply and demand factors that spurs innovation.

Other lessons that can be drawn from the past include the following:

- Technology gives commanders the ability to get inside the adversary's OODA loop. If intelligence on the enemy can be obtained, understood, and distributed fast enough, then military dominance follows.
- Amid our techno-optimism, we must not forget that adversaries can copy us and sometimes innovate in ways we have not. Nor will they have the ethical constraints that as democracies we rightly impose on ourselves. Technology always carries risks as well as offering opportunities.
- Published ethical codes help maintain public support for new technological applications, but they must be internalized—as they are in the medical profession—and not be an add-on acting as a damper on innovation.
- Compensatory steps in doctrine, training, and exercising help ensure that the advantages we enjoy today in initiative, boldness, and daring are not inadvertently weakened by our dependence on having superior technology.
- Innovation will be enhanced by applying as wide a diversity of minds and personal backgrounds as possible to problem-solving. As in wartime, intelligence agencies benefit from the stimulus of outside talent.
- Dual-use technologies are likely to dominate future waves of innovation.
- The application of new science can be accelerated through the sandbox approach and using exercises to stimulate thinking.

Notes

1. David Omand and Mark Phythian, “Intelligence, Ethics and Digital Technology: Towards a Technoethics of Intelligence,” in Seamus Miller et al., *National Security Intelligence and Ethics* (Routledge, 2022), chap. 3, <https://www.taylorfrancis.com/>.

2. Reginald V. Jones, *Most Secret War: British Scientific Intelligence 1939–1945* (Hamish Hamilton, 1978). Professor Jones dedicates his memoir of the birth of scientific intelligence to “all those in Nazi-occupied Europe who in lone obscurity and of their own will risked torture and death for scientific intelligence.”

3. Daniel Kahneman, *Thinking, Fast and Slow* (Penguin Books, 2011).

4. In 1737 John Harrison was awarded a prize of £500 (£250 up front, the rest on completion of an improved model)—worth over £129,000 today. It was awarded under the parliamentary Longitude Act that offered money in return for a solution to the problem of finding a ship’s precise longitude at sea.

5. *Steganography* is the practice of representing information in another message or physical object in such a manner that the presence of the information is not evident to human inspection.

6. Metcalfe’s Law is one of several that seek to describe the increasing value of a network as the number of participants rises. See Scott Hogg, “Understand and Obey the Laws of Networking,” *Network World*, October 5, 2013, <https://www.networkworld.com/>.

7. David Omand, “Spy Time: The Hunt for Chronophages,” *Intelligence and National Security* 36, no. 5 (2021): 709–20, <https://doi.org/10.1080/02684527.2021.1882807>.

8. Jack Devine, *Spymaster’s Prism* (Potomac Books, 2021), gives the original definition of “Moscow Rules” as the understanding between US and Soviet agencies that they would not assassinate each other’s officers or interfere in their domestic politics. In the International Spy Museum in Washington, DC, the “Moscow Rules” are given as follows:

- Assume nothing.
- Never go against your gut.
- Everyone is potentially under opposition control.
- Do not look back; you are never completely alone.
- Go with the flow, blend in.
- Vary your pattern and stay within your cover.
- Lull them into a sense of complacency.
- Do not harass the opposition.
- Pick the time and place for action.
- Keep your options open.

9. See Tom Wheeler, *Mr. Lincoln’s T-Mails: How Abraham Lincoln Used the Telegraph to Win the Civil War* (Harper Collins, 2008).

10. Transatlantic radio communication followed, marked in 1903 by Marconi arranging to send a transatlantic message from President Theodore Roosevelt to King Edward VII.

11. Scarborough is still a GCHQ signals intelligence outstation.

12. Misinformation is wrong but originated through innocent error; disinformation is false and knowingly so; and malinformation is true but obtained and made public without authority or used maliciously.

13. White House, “Remarks by President Biden Providing an Update on Russia and Ukraine,” February 18, 2022, <https://www.whitehouse.gov/>.

14. John Robert Ferris, *Behind the Enigma: The Authorised History of GCHQ, Britain’s Secret Cyber-intelligence Agency* (Bloomsbury, 2021).

15. A zero-day vulnerability is a computer software weakness previously unknown to the software vendor and to cybersecurity companies and that hackers can therefore exploit to access a network or device or for other malicious purposes.

16. See Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Anchor Books, 2019).

17. In 1965, Gordon Moore of Intel predicted that the number of transistors on microchips could double roughly every two years, enabling computing to become ever faster and more efficient. The latest Graphcore chip, called an intelligence processing unit (IPU), has about 60 billion transistor equivalents in the chip. See Gregory Arcuri and Sujai Shivakumar, "Moore's Law and Its Practical Implications," Center for Strategic and International Studies (CSIS), October 18, 2022, <https://www.csis.org/>; and "Next Generation Compute," Graphcore, accessed October 2022, <https://www.graphcore.ai/>.

18. Bell's theorem (or inequality) demonstrates in a way that can be experimentally verified that entanglement between the polarized states of photons and other elementary particles cannot be explained by classical physics. Entanglement forms the basis of quantum encryption, and related results support the work into quantum computing.

19. Melanie Swan et al., *Quantum Computing for the Brain* (World Scientific Publishing, 2022).

20. Satyajit Sinha, "State of IoT 2024: Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally," IoT Analytics, September 3, 2024, <https://iot-analytics.com/>.

21. In the UK, this process culminated in the 2016 Regulation of Investigatory Powers Act and the provision for judicial and parliamentary oversight of all forms of digital surveillance.

22. It is significant that a number of tech entrepreneurs, artificial intelligence (AI) experts, and scientists—including Elon Musk, Jaan Tallinn, Yuval Noah Harari, and Yoshua Bengio—signed an open letter calling for an immediate pause for at least six months on the training of AI systems more powerful than OpenAI's language model GPT-4, saying such systems should only be developed "once we are confident that their effects will be positive and their risks will be manageable." Tim Bradshaw and Ian Johnston, "Elon Musk and Other Tech Experts Call for 'Pause' on Advanced AI Systems," *Financial Times*, March 29, 2023, <https://www.ft.com/>.

23. David Omand and Mark Pythian, *Principled Spying: The Ethics of Secret Intelligence* (Oxford University Press, 2018), chap. 5.

Chapter 4

Emergent Operational Complexity and the Need for Human-System Synergy

Andrew D. Gainer

Johns Hopkins University Applied Physics Laboratory

Karl F. Van Orden

Naval Information Warfare Center (NIWC) Pacific (retired)

Jamie R. Lukos

Naval Information Warfare Center (NIWC) Pacific

Abstract

Military operational planning has been criticized in recent years for failing to address many factors contributing to greater complexity in that arena. These include emerging technologies, sociocultural-political matters, non-state actors, social media influences, and other global interdependencies (addressed in the 2023 Joint Staff publication Joint Concept for Strategic Competition). While our military must be prepared to win violent wars, we must also deny our adversaries strategic advantage gained through methods short of overt warfare. Doing so creates new challenges for operational planning and command and control (C2). Operational commanders and their teams will need to efficiently and effectively use input from highly disparate sources, including intelligence agencies, the State Department, coalition partners, and others that may be unknown to them at the outset. Systems designed to accelerate operational decision-making in this environment require advanced analytics to detect increasingly subtle data stream correlations and trends. These systems must be controlled and accessed within new C2 architectures that shift human burden away from—and leverage computing advantage toward—sensing, processing, and intelligent filtering. This change represents a new paradigm for human-system synergy, which must be deliberately engineered. This chapter outlines some past lessons, enablers required today to make human-system synergy plausible, and a vision

for what human-system synergy will look like to ensure we outpace our strategic competition.

Although it may be widely understood that the Chinese Communist Party has a strategy to expand its global influence—and the tactics to realize it—no Western power has yet applied the necessary imagination and creativity to meaningfully limit that expansion. In his 2020 book *The Kill Chain*, Christian Brose (former staff director for Sen. John S. McCain, the late Senate Armed Services Committee chairman) wrote that the problem is not a lack of technical or operational imagination. Rather, it is the inability of the American people and their elected representatives to imagine something more painful than the change required to implement it.¹

While military, industrial, and political leaders wrestle with the geopolitics, in this chapter we assess the technical and cognitive drivers of the military problem, apply some of the many lessons in history for thinking about revolutionary technical change, consider the major factors enabling and impeding that change today, and envision some milestones and a technical end state for a new human-system synergy to restore and secure America's military primacy in the twenty-first century.

The Problem – A New Era of Complexity

“‘War,’ wrote Clausewitz, is simply ‘the continuation of policy by other means.’ Today, those ‘other means’ have expanded beyond recognition—and at the same time, the increasing complexity of the world we live in has made American policy goals ever more difficult to define,” states Rosa Brooks in her book *How Everything Became War and the Military Became Everything*.² Brooks views sensing and making sense of this “increasing complexity” as the fundamental impediment to national security today.³ She points to the observations of two colonels in China's People's Liberation Army (PLA), Qiao Liang and Wang Xiangsui, “When ‘all the boundaries lying between the two worlds of war and nonwar, of military and non-military’ are destroyed,” the world's traditional militaries—constructed of human beings and their physical machines—will become inadequate to the task of understanding war, much less conducting it independently.⁴

Brooks leaned on the much earlier work by Qiao and Wang, whose book *Unrestricted Warfare* was published in 1999. In the twenty-six years since their predictions about the disappearing boundaries that had always defined warfare, the world has watched those predictions come true. America's traditional military still managed several victories during that time without changing much to account for those projections. However, those victories were against vastly inferior state or even non-state adversaries, and while they all should have been won handily, most were not. Brooks enumerates the risks and opportunities inherent to unrestricted warfare in her own book, so we will say only that they are many and varied and still almost wholly unaccounted for in America's way of war. That has been a largely survivable mistake, until now.

More recently, thought leaders like Jeremiah Monk and Ben Zweibelson have been critical of the military joint planning process. They claim it is too linear and inadequate for situations where an end state is not readily apparent and that intertwined sociopolitical and cultural facets are poorly considered.⁵ The term "gray zone" has been adopted to describe the current era. Gen. Joseph Votel et al. explain the concept: "A Gray Zone 'win' is not a win in the classic warfare sense. Winning is perhaps better described as maintaining the U.S. Government's positional advantage, namely the ability to influence partners, populations, and threats toward achievement of our regional or strategic objectives. Specifically, this will mean retaining decision space, maximizing desirable strategic options, or simply denying an adversary a decisive positional advantage."⁶

Consistent with the gray-zone concept, Joe Miller et al. contend that because the US and its allies have successfully deterred nuclear and large-scale conventional war, actors and adversaries have adapted and developed alternative approaches to pursue their objectives and secure their interests short of war.⁷ In essence, they will employ all the tools of statecraft to maximize outcomes in their favor without direct conflict.

Moving from Complicated to Complex Decision-Making

The Cynefin Framework was developed by Dave Snowden in 1999 while working for IBM Global Services to help manage intellectual capital for knowledge management purposes (see fig. 4.1).⁸ Pronounced

kuh-NEV-in, a Welsh word for habitat, the framework is a sensemaking device to help managers perceive and better understand various environments. The domains proceed in a counterclockwise direction from *simple* and predictable (lower right) to *chaotic* (lower left). In the center and unlabeled is *disorder*, where the appropriate domain cannot be determined. Once understood, complicated environments are largely predictable. However, complex environments are noisy and do not behave similarly over time. The current era of unmanned craft of all sizes and shapes, non-state actors, and state-sponsored militia groups places our current military environment into this domain. Per Snowden, the recommended course of action is “Probe-Sense-Respond” to better understand the complexity and noise and to take appropriate steps therein.

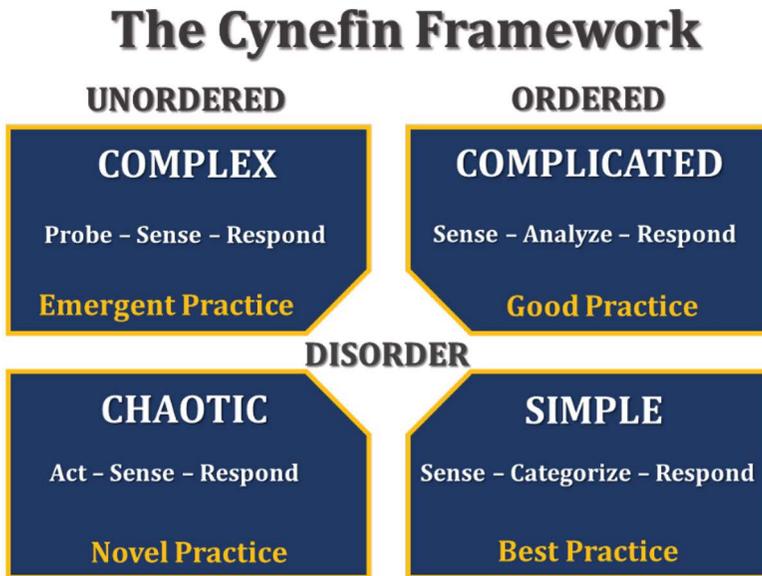


Figure 4.1. The Cynefin Framework. (Adapted from David Snowden and Mary Boone, “A Leader’s Framework for Decision Making,” *Harvard Business Review* 85, no. 11 (2007): 68–76, <https://hbr.org/>.)

The Joint Chiefs of Staff 2023 report *Joint Concept for Competing* expands these thoughts on operational complexities, including climate change, economic factors, and human migratory patterns. Up front, it states that “our adversaries have studied our military strengths and way of war. They have implemented approaches that pursue their strategic objectives while avoiding the deterrent tripwires upon which

our national security posture is based. Simply put, U.S. adversaries intend to ‘win without fighting.’”⁹

The role of the joint force in the era of strategic competition is to protect and advance US national interests by applying military power to deter aggression, prepare for armed conflict if necessary, counter adversaries’ strategies threatening our national interests, and support our interorganizational partners. Interagency coordination is of paramount importance. The Department of Defense must be able to assess and act on information that is much more global and interdependent than in the past to understand where the United States stands in the strategic competition arena.

Today we strive for incremental improvements—and exhaust our human capacity—in assessing and acting on everything we *can know* and accounting for what we realize we *cannot know*. But both of these information sets are comparatively smaller and less relevant in the information age than they were in the industrial age. Now it is the much larger span of human ignorance that should mostly guide military planning, and nothing about today’s processes or systems is suited for that. Information age warfare elevates the scale, impact, and asynchronous timing of the “unknown unknown” into the domain of operational decision-making. That challenge constitutes a planning problem we are overdue in solving.

Unlike the US military, China’s PLA—which secures the expansion of the Chinese Communist Party’s global influence—has become the first well-funded, state-sponsored military to be integrated into a whole-of-government strategy that embraces the opportunities of unrestricted warfare. What has China done? Jonathan D. T. Ward’s summary of his 2019 book *China’s Vision of Victory* captures it well: “China’s leaders, from Mao Zedong to Xi Jinping, have passed along a vision of ‘national resurrection.’ . . . This means breaking apart the US and Allied world order and replacing it with a system in which China’s values, power, and restored national glory emerge victorious. *In pursuit of this ‘historic’ vision, China’s leaders have assembled a thoroughly modern strategic program that encompasses virtually every aspect of human industry and endeavor—from dominancy in quantum computing to diplomatic engagement with Latin America*” (emphasis added).¹⁰

Specific military elements of China’s program that concern us in this chapter are bold moves into asymmetric capabilities, including artificial intelligence and unmanned systems (UxS) and cyber warfare,

and a proclivity to test the ever-diminishing boundaries between war and nonwar by employing them in the gray zone.

America's military must develop skills, systems, and habits today to Probe-Sense-Respond as the *most common decision cycle* in a high-end (i.e., highly automated, machine-speed) fight while simultaneously learning, with urgency, how to Act-Sense-Respond using help from our warfare development centers and research laboratories. Enabled by the right decision aids, these complex and chaotic processes will facilitate fleeting but essential insights into the aforementioned span of human ignorance, which must be illuminated for our nation to compete at any level in unrestricted warfare.

Striving for Human-System Synergy

Digitized, intelligent sensors, computers, and networks (i.e., machines more than people) are necessary to deal with the complexity, size, and speed of a potential conflict with China, Russia, and other adversaries. America may already lag behind China in integrating these technologies into our way of war, and our fundamental ethics and morals create an extra burden of superiority needed to win a truly unrestricted war while preserving them intact. The need to make decisions quickly and the volume of information required to make informed choices are among the drivers of new technologies and edge computing and data correlation processes that will change the roles and responsibilities of humans and machines. Such factors require shifting how we view human-machine relationships and command-and-control architectures required for sufficiently rapid and accurate operational decisions.

The concept of bringing machines into human decision spaces is not new but is still often far from optimal. In "Ironies of Automation: Still Unresolved After All These Years," Barry Strauch revisits and expands on Lisanne Bainbridge's earlier paper, "Ironies of Automation." Several critical issues emerge:

- Automation can leave operators with an unclear understanding of system status, such that when a system is failing and automation cannot compensate, an operator may be woefully unprepared to engage.

- Alarms and warning signals may exacerbate operator confusion and overload, leading to perseveration on a problem at the expense of attending to other important information.
- Because designers of automation can rarely consider all possible anomalies that may occur within a system, human operators must have a clear understanding of how the automation works and the state of the overall system at all times.¹¹

When confronted with complex, fast-moving problems, these issues can quickly metastasize into widespread misinformation, confusion, and, ultimately, mistrust by human operators. The story of the USS *Vincennes*'s shootdown of Iran Air Flight 655 on July 3, 1988, is rife with examples of this outcome. In summary, a highly capable Aegis Weapon System—thrust into service in a much different environment than designed for—automated some things that contributed to the accident and failed to automate others that may have prevented it. Of particular interest, however, are the dynamic tactical, operational, and strategic environments in which this accident occurred. Several recent changes in these environments were partially or wholly absent from the commanding officer's decision process during the highly charged seven minutes it took him to shoot down that aircraft. In 1988, the fundamental technology did not exist to help him with that. Today, it does.

Accounts written in the near aftermath of the *Vincennes* shootdown incident reflect the conventional wisdom of the time regarding technology limits. In a 1989 *Naval Proceedings* article, Norman Friedman indicates that although the Aegis SPY-1A radar “performs surveillance . . . , it is primarily a means of effective fire control, and the design is probably biased in that direction, naturally.”¹² His assertion that moving away from surveillance was “natural” reflects the SPY-1A's development for industrial age, blue-water combat with the Soviets, as do his other assertions about the contributing Aegis bugaboos in this accident. That fundamentally restricted view of warfare (and of the demands it might reasonably place on combat systems) would persist for nearly thirty more years, and it still does today in most of the platform-oriented acquisition community. It is unsurprising to find this view in Friedman's assessment. While describing the human error in labeling Iran Air as “diving” toward the *Vincennes*, he states that “no command system can be designed to check and recheck such data—which, after all, are supplied up the chain of command by trusted subordinates.”¹³ While describing the human error in assigning a military identification

of friend or foe (IFF) to the unknown target, Friedman concedes that such a function could, and should, be automated. However, his technical vision seemed to end there. That vision may have been ahead of his time, but it is way behind ours.

Friedman went on to articulate environmental factors that—not having been surveilled and updated during the unfolding of this incident—might have changed either its outcome or characterization in the public eye as a mistake. In so doing, he essentially forgave the commanding officer. To be clear, we do too, but we think there is more to the story. In 1989, it was unimaginable that a single decision-maker could know such factors, especially in just seven highly stressful minutes. But could a single decision-maker in that environment today be aware of this information?

There are signs in Friedman's account that even he suspected underlying Iranian motives. He seemed deliberate in describing how the United States had been set up for this incident, including Iranian threats against the United States for that July 4th weekend and specific training the ship had received about suicide air attacks and ongoing Iranian attacks against US and friendly shipping in the Gulf (including a surface battle between *Vincennes* and Iranian small craft that was ongoing *during this incident*). There was also the unexplained proximity of an Iranian P-3 that could have been providing targeting information for the unknown, presumed attacker. He went further, edging right up to and then, ostensibly, backing away from a direct accusation: "It would be fatuous to imagine that the Airbus had been sent into danger in order to create a climate in which the ceasefire became acceptable for Iran."¹⁴ "Fatuous" indeed. In 1989, such an accusation would have seemed entirely baseless. Then, when the world did not do all its business on the Internet with networks that create enormous volumes of uncorrelated data, such a theory could only be described as fatuous precisely because it was unknowable technically.

Today, with the benefit of modern data science, sophisticated artificial intelligence, and high-powered computing, the intelligence community looks for, and often discovers, data streams that bear out just the types of strategy Friedman may have hinted at. With that knowledge, the rest of the "setup" does not seem far-fetched.

Adapting these technologies to human-machine teaming in tactical warfare requires a smaller step than many imagine. Friedman's article describes specific errors that day in machine design and human execution, the correction or reliable automation of which would be trivial by

today's standards. The Aegis program office has likely addressed these issues (we did not check). The error that interests us most in this chapter, however—the error we want to correct—is Friedman's conclusion that *Vincennes'* shootdown of Iran Air 655 was a *fait accompli*, that “the Navy and its crews on the front lines cannot really do that much better,” that “wars beget accidents, and that accidents . . . are unavoidable.”¹⁵

Regardless of whether, or to what degree, Iran's government planted the plane for *Vincennes* to shoot down in 1988, there is every reason to believe China and Russia are motivated and able to manufacture such traps for US naval vessels today and that public opinion could be the first weapon employed in a larger offensive. Both adversaries have demonstrated facility with information manipulation toward this end, and only superior information warfare will illuminate the traps they employ. Key to superior information warfare is the appropriate assignment and sharing of duties between humans and machines.

The history of warfare reflects a continuously expanding and contracting gap between technology and operational capability—think sail to steam to nuclear power, carrier pigeons to radios to satellite communications, or battleships to naval aviation to distributed maritime operations.

While assertions about what may be fundamentally new in such a long history can be risky, it is true that human warfare until now has been conducted entirely with human intelligence. Tools have almost always been involved, but even the most sophisticated machines in warfare have been deterministic and observable in their function. The complexity of unrestricted warfare in the information age overwhelms human-only intelligence, demanding a new teamwork between humans and machine “partners,” which is no longer entirely deterministic and observable. The maximum theoretical potential of human-machine teaming could be described as a state in which the human being is completely unburdened of all tasks except for the moral/ethical work of war. As the capabilities of machines and AI continue to advance, progress toward this maximum theoretical potential is heterogenous across domains, missions, and decision spaces. This inconsistency has resulted in challenges to enlisting intelligent machine teammates into the warfighting arena.

Enabling Human-System Synergy

To prevail in today's highly complex operational planning environment with humans and machines working seamlessly side by side, we

have to think and act differently about national defense than in the past. With new technologies defining a more expansive playing field, the players on that field—the warfighters—will have to change how they think and act too. They already have too much data and too little time to relay useful information to higher echelons for analysis and decision. To correct this dilemma, edge computing and ad hoc data analytics capabilities on deployed assets are becoming more and more common. However, the ability to analyze, interpret, and make decisions on complex data streams are skills not yet selected or trained for in most personnel ratings today. With intelligent systems taking on various roles, from relieving humans of mundane tasks to augmenting humans to performing advanced information pattern recognition, accelerating technologies already outpace traditional military school-house training, and the gap is growing.

These automation issues and other obstacles impeding more seamless human-system synergy need to be tackled from a more holistic perspective. First, we must better understand the information we need from *all* domains to make good decisions in *one* domain. Then, we must be able to measure the quality of that information and turn it into knowledge. Next, we must have a means to understand how to act on that knowledge and what the consequences of our decisions will be. Importantly, we must have a better means to rigorously test the human-system interactions iteratively throughout the development and sustainment life cycle to consistently make the interactions more seamless and adaptable to changing situations.

Although substantial challenges to this new way of thinking exist, they have been more thoroughly examined in the literature than factors that could enable it, which we focus on here. Examples of such challenges include a last war mentality, our current peacetime environment, and the decades-long breakdown in trust and partnership between American industry and the government. Just like the new paradigms we require to embrace unrestricted warfare, these challenges demand cooperation across previously sacrosanct boundaries. Only cross-organizational, intragovernmental coalitions of the willing can illuminate these obstacles sufficiently to break them down and solve them. Such a chicken-and-egg dilemma exceeds the scope of this chapter, so, again, we focus instead on enablers for a new way of American warfare. We acknowledge that enablers may exist mainly in the eye of the beholder, but one goal of this chapter is to enlighten a few new optimists!

Although rarely used to enable warfare development, the state of *not* being at war is, strictly speaking, one of the greatest enablers available to us. The massive cost of being at war—and the attendant risk of losing one—makes it a horrible time to learn how to do it (war) correctly, but that is generally when countries do so. One particularly notable exception, however, was the interwar period between World Wars I and II. Major players in those conflicts did a lot of learning and development, particularly in aviation and amphibious warfare. Even in the years following World War II, advances in missile technology and nuclear propulsion appear to have been monumental in scope and speed compared to today's mired acquisition system. There are no laws preventing that sort of progress today. In the early 2010s, Congress passed a host of acquisition-related laws expanding authorities in agile acquisition and rapid prototyping and development. A thorough description of what still *does* prevent rapid development at scale is best left to the previously quoted Brose work, *The Kill Chain*, but suffice to repeat, it could be overcome if Americans would just imagine something harder than the political work of that change—for example, the replacement of today's rule-based international order with authoritarianism.

America's military-industrial-congressional complex seems perpetually and inevitably deadlocked by politics and ideological division, but *it still comprises one of the most powerful national defense systems in the world*. It absolutely should be thought of as an enabler for a new way of American warfare, not simply because no one else will do it but also because it *does* have the necessary resources, which are almost trivial next to what we spend on a platform-centric Navy alone.

Lessons from the past can also be enablers, not so much from our own past conflicts, most of which have only industrial age wisdom to impart, but from recent and current conflicts around the world like the one between Russia and Ukraine. In a 2022 brief, Seth Jones (senior vice president and director, International Security Program, Center for Strategic and International Studies) offers lessons to be learned from Russian failures in operational planning.¹⁶ Some of these, like logistics, appear on their face to be traditional military failures. But artfully portrayed by Mr. Jones as operational planning failures, they represent ideal problem sets for command-and-control architectures that leverage new human-system synergy for planning decisions.

To appreciate this synergy's potential value, first consider some of the challenges Russia faced. For instance, its command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR)

systems failed due to chronic neglect. It also ran out of precision-guided munitions early, and it never achieved air superiority because its domestic industry could not replenish missiles and unmanned aircraft systems. Further, its cyber and electronic warfare attacks were largely blunted because Ukraine had extensive help from US Cyber Command, the National Security Agency, Microsoft, and SpaceX.

This list is not exhaustive, but ask yourself whether technology could have helped predict those problems during Russia's initial operational planning. Could intelligent algorithms have correlated data streams from their own military networks to illuminate the risk of unmaintained systems crumbling under the pressure of live warfare? Could similar technology applied across the larger global Internet have provided a more accurate picture of the massive state, non-state, and commercial support Ukraine would enjoy; how crippling third-party sanctions would be, not least because of US/UK parts in their critical supply chains; or how the Ukrainian people would rise up to help their military so substantially?

We contend that the answer to all these questions is resoundingly yes! The state of artificial intelligence, data fusion, edge processing, and decision support technologies is sufficient today to build systems that inform operational planning of all those risks, not just in advance but in real time during a conflict. The imperative of doing so is a lesson our military-industrial-congressional complex should learn from Russia's ongoing struggle in Ukraine.

The final enabler for reimagining the American way of war that we will cover here, historically the most reliable one, is the American warfighter and their supporting cast of defense laboratory, industry, and affiliated academic institutions. Our nation's all-volunteer force has an almost perfect record of rising to insurmountable odds, even with a last war mentality and, often—at the outset of hostilities—with last war technologies. If called upon, it will do so again in a conflict with China, but unrestricted warfare drastically worsens those odds. Empowering our warfighters and their supporting cast with permission—by which we mean the time, budget, and requirements space—to *build, train with, and learn to trust* systems that can contend with unrestricted warfare is, in our opinion, the only winning strategy.

The enablers for a new American way of war also include uniquely technical advantages that our science and engineering community is poised to leverage. Holistic information operations can be enabled by comprehensive data sources, advanced analytics, expert fusion and

parsing algorithms, and autonomous and self-healing networks in all physical and security domains. Such mechanisms can be infused throughout these domains with user-centered design, not as gold-plating but as *fundamental* to any new development. While this approach has yet to be common practice, examples exist, like the Tactical Tomahawk Weapons Control System (TTWCS).¹⁷

Robust development, testing, and training environments can be formed through seamless integration of constructive, virtual, and live capabilities. Such environments are critical for continuity and continuous, recursive, and iterative progress *across acquisition life cycles*. The same environments should be used to vet new concepts; develop and test prototypes; solicit and incorporate user feedback; refine, verify, and validate requirements; integrate subsystems; perform acceptance testing; train human decision-makers and nourish their trust in these systems; and even drive budget decisions, adjustments, and war plans. Perhaps the most critical long-term advantage such environments will confer, however, is the ability to deal with emergent future complexity in measured yet decisive ways. Our adversaries will innovate, and we will need to understand their new capabilities quickly to posture and act appropriately.

As long as the functions described above remain stovepiped in separate program offices using their own environments, America will continue to optimize individual domains and platforms that are, as previously argued, incapable of dealing with the complexity of unrestricted warfare.

Conclusion

The Department of Defense is unlikely to replace twentieth-century platform-centric requirements, budgeting, and acquisition wholesale with a new model of human-system synergy, but it could and should evolve toward this goal. The timeline for a potential China conflict has already displaced most of the appetite for basic science and technology research with urgency around integrating mature technologies into existing human-only command-and-control architectures and decision-making.

The good news is that we do not have to be perfect about human-machine teaming to deter or defeat China. Something short of its maximum theoretical potential will almost certainly be better than whatever China achieves, particularly considering recent news about

political and economic moves to limit its access to the most sophisticated technologies. The argument here is not that America and her allies and partners are doomed to Xi Jinping's vision for a new world order. Rather, we argue that they must deliberately act on the arrival and complexity of unrestricted warfare and do the work necessary to survive and win it. We must not be paralyzed from beginning this effort due to fears that we may not complete it in a specific time frame. We must pursue this goal to guarantee our security in the foreseeable future.

Notes

1. Christian Brose, *The Kill Chain* (Hachette Books, 2020), 250.
2. Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales from the Pentagon* (Simon & Schuster, 2016), 22.
3. Brooks, 22.
4. Brooks, 22.
5. Jeremiah Monk, "End State: The Fallacy of Modern Military Planning" (research report, Air War College, 2017), <https://apps.dtic.mil/sti/pdfs/AD1042004.pdf>; and Ben Zweibelson, *Beyond the Pale: Designing Military Decision-Making Anew* (Air University Press, 2023), <https://www.airuniversity.af.edu/>.
6. Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (1st Qtr 2016): 101–9, <https://ndupress.ndu.edu/>.
7. Joe Miller et al., "Harnessing David and Goliath: Orthodoxy, Asymmetry, and Competition," *Small Wars Journal*, February 7, 2019, <https://archive.smallwarsjournal.com/>.
8. David Snowden and Mary Boone, "A Leader's Framework for Decision Making," *Harvard Business Review* 85, no. 11 (2007): 68–76, <https://hbr.org/>.
9. Chairman of the Joint Chiefs of Staff, *Joint Concept for Competing* (Department of Defense, February 2023), <https://s3.documentcloud.org/>.
10. Jonathan D. T. Ward, *China's Vision of Victory* (Atlas, 2019), 1.
11. Barry Strauch, "Ironies of Automation: Still Unresolved after All These Years," *IEEE Transactions on Human-Machine Systems* 48, no. 5 (2017): 419–33, <https://doi.org/10.1109/THMS.2017.2732506>; and Lisanne Bainbridge, "Ironies of Automation," *Automatica* 19, no. 6 (1983): 775–79, <https://ckrybus.com/>.
12. Norman Friedman, "The Vincennes Incident," *Proceedings* 115, no. 5 (1989): 72–79, <https://www.usni.org/>.
13. Friedman, 72–79.
14. Friedman, 72–79.
15. Friedman, 72–79.
16. Seth G. Jones, "Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare," CSIS Brief (Center for Strategic and International Studies, June 1, 2022), <https://www.csis.org/>.
17. Sarah Rigsbee and William B. Fitzpatrick, "User-Centered Design: A Case Study on Its Application to the Tactical Tomahawk Weapons Control System," *Johns Hopkins APL Technical Digest* 31, no. 1 (2012): 76–82, <https://secwww.jhuapl.edu/>.

Chapter 5

Breaking the OODA Loop

Human-Machine Symbiosis to Manage Complexity and Accelerate Decision-Making as a Decisive Warfighting Advantage

*Timothy Grayson, Senior Vice President, Chief Architect,
Defense Systems Sector, Leidos Corporation, and former Special
Assistant to the Secretary of the Air Force**

Abstract

The US military is currently the most powerful fighting force in human history, and the combination of its capabilities, strong alliances, resiliency of mission command, and overall warfighter ethos enable it to prevail against any potential adversary. However, we cannot become complacent. History is filled with dominant organizations that seemed untouchable—until they were not! Upstarts appeared, seemingly out of nowhere, and through agility and adaptation quickly brought them down in unexpected ways. This is an example of winning by “getting inside the OODA loop.” John Boyd’s OODA stands for “observe,” “orient,” “decide,” and “act.” What Boyd accomplished by identifying these discrete steps was to provide a trainable discipline to planning, decision-making, and execution—and it offers the additional benefit of providing a template for distributing the cognitive burden of decision-making between humans and machines. The US military fully understands the force multiplier provided by the speed of the OODA loop. We train our operators to achieve this speed at the tactical level and our commanders at the operational level. As the pace becomes faster and the problems of greater scale and complexity, we are just beginning to develop models of human-machine symbiosis to continue to stay inside the loop. As we move toward ever more complex theater, strategic, and enterprise problems, we need to think like

* The author held the former position at the time of writing and is with the Leidos Corporation at the time of publication.

operators, develop similar AI-driven decision aids, and act with the same operational practicality and speed, avoiding the institutional traps of overcomplicating our already highly complex challenges. Otherwise, we risk going the way of the twentieth-century industrial titans.

Most people who spend any time thinking about military strategy have heard reference to John Boyd's famous "OODA loop" (fig. 5.1).¹ In a culture that loves acronyms, OODA stands for "observe," "orient," "decide," and "act," and it is a decomposition of a decision process that most of us subconsciously execute to varying degrees many times an hour and yet do not consider in these discrete steps. What Boyd accomplished by identifying these steps was to provide a trainable discipline to planning, decision-making, and execution that has helped military leaders and operators avoid foolhardy actions driven by intuition and emotion.² It has offered the additional benefit of providing a template for distributing the cognitive burden of decision-making between humans and machines.

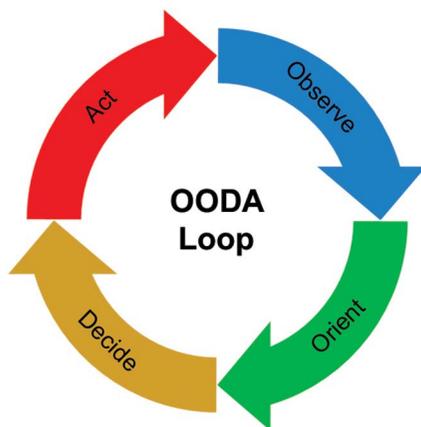


Figure 5.1. John Boyd's "OODA loop": Observe, Orient, Decide, Act. The fastest OODA loop wins.

In the tactical environment, warfighters accept that speed is victory and frequently talk about "getting inside the OODA loop" as a fundamental model for success. To prevail in great power competition in an increasingly complex world, we need to apply this same principle of disciplined speed of decision to multiple time scales, not just the tac-

tical but also the operational and strategic. We will be faced with ever more complex challenges and greater uncertainties. Our legacy approach to dealing with this environment is overprovisioning, mostly in terms of weapons system performance. But as we overprovision, we inherently become more risk-averse: The risk of each action grows with the magnitude of the decision and the impact of a negative outcome. This correlation leads to a negative feedback cycle.

We can reverse that trend by helping warfighters make decisions faster. Today, there is a push across the Department of Defense (DOD) to drive faster decision-making with technology. Commissions have been chartered and whole organizations created to manage and promote the development of artificial intelligence (AI).³ While these efforts are important and the resulting AI-based tools will indeed help warfighters decide faster, this chapter's focus is on rethinking the decisions themselves. AI tools applied to a bad set of options will only marginally speed up decisions and possibly not make the outcome any better. The technology is simply trying to accelerate a fundamentally flawed workflow. Conversely, if more choices can be made available and the consequences of a bad decision minimized, warfighters can make decisions faster, converge on better conclusions, and reverse the negative feedback cycle.

Structuring for faster decision-making requires a discipline not just on the steps of the process but also on the scope and scale. We must manage and contain the complexity of the OODA loop. AI can help mitigate complexity, but even the biggest computers and best AI will eventually succumb to nonlinear growth in complexity. This chapter will unpack the OODA loop to examine how humans and machines can share the cognitive burden, how complexity can be managed for both, and how the resulting speed can be applied for success at all timescales.

Boyd's OODA Loop and the Tactical Fight

“There I was diving out of the sun. The guy in the other plane couldn't see me, and before he knew what happened, I was on his tail with guns blazing!” This is a common fighter pilot story. The poor victim was blinded by the sun and never saw the death that was about to descend upon him. He was never able to “observe.”

The now-famous military strategist John Boyd realized the importance of the decision cycle when studying the success of US F-86s

against MiGs of comparable performance.⁴ He broke the process into a four-step OODA loop:

- *Observe*: An initial insight of Boyd's was that the F-86 had a larger canopy than the MiG. The F-86 pilot thus had a clearer view of the sky and a greater opportunity to see the adversary. He was also, obviously, aware of his location and situation. For the Korean War dogfight, this was what amounted to sensing and data gathering, but it provided the foundation for making decisions.
- *Orient*: Data without analysis is at best meaningless and can even be a distraction. For Boyd's F-86 pilot, orienting meant processing those visual observations to determine if an adversary plane was a threat to avoid or a viable target to engage. This orientation included physical orientation and geometry but also knowledge of his own state, for example speed and available energy. It may have also included higher-level orientation to the type of target. Is this a high-value asset that is a priority to engage? Is this a combat aircraft that can threaten me? If there are multiple targets, how might they line up in relative priority?
- *Decide*: The orientation step informs the creation of one or more courses of action. In MiG Alley this might have first involved a choice of attempting to flee versus engage. If the choice is to engage, but there is more than one target, which is best to engage first? Regardless of the top-level course of action, what is the best specific tactical maneuver? The pilot needed to create a mental collection of these actions based on the analysis (orient) of the available data (observe) to select what he believed at that moment was the best course of action.
- *Act*: Having decided on a course of action, the pilot needed to execute this decision. This point is where physical reality meets the cognitive process. In Boyd's assessment of the F-86 advantage, a key insight was the superior maneuverability and turn radius of the F-86 over the MiG. There were also likely large variations in individual pilots' ability to fly specific maneuvers with precision. But regardless of the uncertainties and physical constraints involved, the action step was about carrying out the decision.

This sequencing never stops, which is why it is called the OODA loop. The outcome of Act becomes the new state to Observe and so on. Of course, in a dogfight, the loop is continuous and blindingly

fast and would not appear as a series of discrete steps or a loop. The steps blur and may not even be conscious cognitive processes, defaulting to what we think of as the intuition of the pilot. Yet Boyd's decomposition still provides a systematic framework for training that intuition. It also provides initial clues toward human-machine collaboration and, ultimately, symbiosis.

Sharing the Cognitive Workload

Let humans do what they do best, and let machines do the same. This classic division of labor led humanity toward civilization, and it applies today in how we leverage technology to augment humans. Generally speaking, computers excel at so-called closed world decision-making.⁵ In this context, the inputs, outputs, and option space of decisions are discrete, and decisions are concrete. A simple example of this concreteness is chess, one of the first games in which AI bested the most accomplished humans. The decision space is highly discrete: sixty-four squares, sixteen pieces on each side, a rigidly defined movement ability for each piece, and a binary outcome of a movement (take a square with or without taking another piece). The initial conditions are rigidly fixed and known by the board setup, and there is a singular, concrete output objective: Take the king.

Despite the seeming simplicity of chess, the combinatoric complexity is still immense, and three decades ago it seemed absurd that a computer could beat a grand master—until one did. In a now-famous 1996 chess match, IBM's Deep Blue defeated grand master Garry Kasparov.⁶ The chess and AI worlds were stunned. Since then, it has become commonplace for computers to best humans in these closed world games. The complexity can grow as the size of the option space grows and options become less bounded to the point that decisions may not appear closed, yet they still are. DeepMind's AlphaGo highlights this concept. The game of Go feels more open than chess because of the size of its decision space, yet it is still discrete and closed. Here too, advanced AI excelled, besting a human 9-dan (highest Go level) for the first time in 2016.⁷ Just like Deep Blue's defeat of Kasparov, this AI win was considered stunning. Today, these kinds of AI victories are viewed as almost predictable as one seemingly impossible task after another is done better by a computer.

Why is this? There are many technical answers to this question based on how AI technology has matured, but the fundamental reason is that computers are really good at managing discrete complexity. Computers exceed humans in the number of “logic gates” (e.g., transistors for a computer, neurons for a human) and the speed of those gates by many orders of magnitude, and the disparity is constantly growing as increasingly powerful chips are designed and computers are built. To humans, with their limited number of slow neurons, Go might appear to be a continuous, open decision space. However, to a computer, the combinatoric option increase between Go and chess is small compared to the growth in computing power between 1996 and 2016. For a computer, victory in such arenas is easy.

So, is it all over for humans? Not yet! The opposite of a closed world problem is an “open world” problem. If closed decision spaces are discrete and concrete, then open world decision-making is characterized by an unbounded, continuous decision space, uncertain and ill-defined inputs and outputs, and perhaps not even a precisely known objective. Concreteness is replaced with abstraction. This is the realm of cognition where humans still excel over computers: abstraction, ambiguity, context, intuition. The most recent advances in generative AI based on large language models (LLM) are providing some tantalizing hints that computers may be getting better at open world decisions, but this capacity is still something of a facade.⁸ LLMs are fundamentally based on statistical number crunching of past data in a closed world space—only the size of that space continues to grow with the immense size of the models, making it appear that the AI is reasoning in an open world. Nevertheless, it is really just the next jump in discrete complexity that we saw between chess and Go. ChatGPT seems to carry on an open-ended conversation until it goes stupid. Cognitive science still does not fully understand how our limited number of noisy, slow neurons perform this function, but humans are still the grand masters at unstructured abstract reasoning.

How does this cognitive division of labor apply to the OODA loop, and who is the lead partner in each step? Consider the application of OODA to a dogfight:

Observe

Give this step hands down to the machines. The first advantage they have is the ability to collect information. In a digital environment,

computers with access to a global cloud can collect data from a much greater scope than their human partners even know exists. In a tactical environment, a radar may be able detect targets at ranges of tens or even hundreds of miles, while the “Mark I Eyeball” of the most eagle-eyed human ace will be lucky to get good detection well less than ten miles out.

The computer advantage in the “observe” step goes beyond data collection and into the processing of information. That radar sensing one-hundred miles out can also measure millisecond position changes and precise range and velocity that can convert sensor data into a 9-degree-of-freedom track vector. Humans can intuitively eyeball distance, although not quantitatively, and maybe get some feel of relative velocity but certainly cannot calculate high-order kinematic tracks (consider the fun of trying to zipper merge your car on a busy highway interchange). This observation advantage even extends toward the seemingly more open-ended problem of object recognition. Over the past two decades, “automatic target recognition” has gone from an esoteric research area to tools available on our phones, thanks to advances in AI such as “deep learning.”

Orient

This step is more of a draw between human and machine but with a slight edge to the machine. Much of orientation is highly mathematical and closed. In a tactical dogfighting environment, a computer can more easily ingest a quantitative state vector of the adversary (taken from the radar tracker in the “observe” step) and own-ship state vector and make the time-speed-energy calculations to determine if a merge is possible and at what geometries. Some highly skilled humans can perform at this level, but these finely honed capabilities are not readily available to everyone versus being almost trivial for the computer. The same comparison applies in other domains, such as the trafficability of ground terrain, maneuver of satellites, and flow of cyber data on a network.

However, we humans may still have some game in certain elements of “orient.” As alluded to earlier, part of “orient” may be associated with target prioritization. While a prioritization rubric might enable more advanced AI to make some of those types of decisions, humans still have an advantage in such abstract, contextual processes—especially in the face of uncertainty that may go beyond the bounds of the rubric.

Decide

Score one for the human—although not entirely. In this phase, human intuition, understanding nuanced context, and abstract reasoning play critical roles. At one level, “decide” is not hard for the machine, even amenable to rule-based logic tables. There is a prescribed prioritization of targets: “Observe” and “orient” have identified an aircraft as one of the highest-priority targets, so I am deciding to engage.

But the process of even tactical combat is not that straightforward. What was the commander’s intent? When the commander provided that target list, what was the overarching strategy, and how did that list relate to theater-level objectives? Could the situation alter priorities? And this logic flow is just one element of the decision process. When I was cued to the target, how confident did the air battle manager seem? What are my own combat identification systems telling me about that target? Is the situation such that there seem to be inconsistencies? Are there opportunities for the adversary to try to deceive me? What is the friendly situation, and is there a risk of confusion? Layer on top of all of this the knowledge of one’s own-ship state. Am I in a defensive or offensive posture? What are my levels of fuel and munitions, and is there a steep opportunity cost of going after one target over another?

These considerations are just a limited set of variables and uncertainties that must be considered in one simple decision scenario. “Decide” is a largely open world process, and thus humans have the upper hand. This author’s personal assessment is that AI technology is a long way from reasoning contextually about open world decisions, and there is an ethical question as well. Do we as humans want to hand over decisions to take lethal action to machines? The general consensus of ethicists is no.

That said, there is still a role in “decide” for the machine. Humans can easily succumb to bias and make bad decisions as a result, reasoning, “This is how we’ve always done it.” And humans may not have access to as much information at a moment in time as the machine can access (see the “observe” step). Additional information, if available, may change the human’s decision. Therefore, an “AI assistant” for a human operator is not a bad combination. The AI assistant is not making decisions but is instead only making suggestions. The human must be trained properly not to over- or undertrust these suggestions, but they could be a strong augmentation to human decision-making. Additionally, who knows what the continued maturation of AI will

bring, even from the current advances with large language models, so perhaps someday in the not-too-distant future, machines will be better at these kinds of open world decisions.

Act

Here, the machine has the clear victory, certainly in a dogfight. Controlling an aircraft is the ultimate closed world problem. It is governed by specific control option inputs with measurable states, and the output is tightly governed by physics and the performance of the aircraft. At the same time, it is highly dynamic, nonlinear, and sensitive, making it a heavy cognitive burden for humans. This is why so much time and money are spent on flying hours. Much of that is focused on training and maintaining pilot proficiency in tactics and flying maneuvers. This is also why, for decades now, almost all new military and civil aircraft have “fly by wire” digital flight control systems. These control systems provide better, safer performance while reducing the pilot cognitive load, freeing the human to focus on other mission elements.

The conclusion of this walk through the OODA loop is that human-machine symbiosis will result in faster and better execution of the loop, and again, speed = victory. Imagine a not-too-distant future in which the machine is doing all of “observe” and “act” and advising on “orient” and “decide.” In the dogfighting example, that human could just be along for the ride and function more as a battle manager than a pilot. At the time this chapter is being written, the US Air Force is initiating the first true autonomous combat aircraft development program, the Collaborative Combat Aircraft or CCA.¹⁰ At first, while operators develop trust in CCAs and fly their legacy aircraft, this human-machine symbiosis will happen truly as a discrete set of players in a team—a force package where the CCA is an autonomous wingman. In this early model, the machine is entirely focused on “act” under orders from the human. As AI matures and operators develop more trust in their machine partners, a next logical step is to push more of that AI into the crewed platform. Doing so enables the human pilot to start being more of a battle manager. Ultimately, when this human-machine team becomes a full-faith partnership, does there need to be a pilot forward at all? Could the human teammate be a true battle manager at a remote location?

Besides the evolution of AI technology and trust, other elements of a distributed warfighting architecture need to mature to reach this ultimate remote human team, but we are already on the path to human-machine symbiosis. Accelerate the OODA loop by letting the machines do what they do best, freeing up humans' cognitive capacity to do what they do best. While this example concerned fighter aircraft tactics, the premise applies to other types of tactical operations. But what about higher-level decision-making, say for theater-level operations? Does the same model apply there? As the next section discusses, the answer is a resounding yes but in different ways.

Accelerating the Operational Level OODA Loop = More Options Faster

There are arguably few examples of endeavors that simultaneously combine a greater magnitude of scope and complexity than operational-level command in modern warfare. The many considerations include the number of assets, the physical geography and scale, the diversity of capabilities and actions, the warfighting domains, joint and coalition forces, the magnitude and diversity of targets, adversary deception, and the myriad paths to victory. The decision space is immense, and it is the ultimate open world problem. Now throw in the need for speed. The decisions supporting theater-level operations still follow the pattern of the OODA loop. "Observe" in this case may be gathering all-source intelligence. "Orient" might be creating a common operating picture. "Decide" could involve determining tasks to be assigned to a given asset, and "act" would then be disseminating those orders. While this process might seem simple, imagine a thousand decision factors occurring simultaneously and continuously, most interdependent, all having implications for the next future decisions and against a backdrop of extreme uncertainty. Further, a commander cannot afford to take time to deliberately and thoughtfully ponder these critical decisions. As in the tactical example, the side that can execute this OODA loop faster will gain a significant advantage regardless of its capabilities.

Militaries (and for that matter, all large human endeavors of a similar scale) have managed this complexity through the hierarchical division of labor. This allocation keeps the decisions that need to be made at each rung on the ladder simpler. A theater commander does not need to know the details of individual platforms, and a tactical

unit commander does not need to know what is happening across the whole theater. Unfortunately, a rigid hierarchical construct comes with its own major regrets, namely, that the very act of simplifying the cognitive burden at a rung simultaneously takes away options. Militaries have typically overcome a loss of optionality by overprovisioning their force, with the perspective, “I don’t need many options when I have high confidence that the one I have will kick b---.” But overprovisioning is not an option in great power competition. Competitors are generally evenly matched, and a slight advantage in the quality and speed of decisions is likely what wins the war. While a small portion of the decision space, there may be a few options available to the commander that would provide the decisive move if only they were not buried in the hierarchical abstraction and the commander could discover and execute them.

So, the conflict is between reducing complexity, which is critical for speed, and expanding optionality, which is critical for quality. To decompose this challenge, consider two metrics in this decision space as “span” and “depth.” Span relates to the number of things to make decisions about and could incorporate values like the physical area, number of assets, and diversity of capabilities. Depth relates to the fidelity and amount of detail involved in a decision. At a very high, coarse degree of depth, a theater-level decision could involve something as abstract as a generic theory of victory. At a slightly deeper level, it could mean assigning general commands to certain units. As one goes further in-depth, the decisions comprise more fine-scale details, such as route planning, individual target-weapon pairing, or taken to extremes, even actuating flight controls or sensor modes. When one attempts to maximize both span and depth, the numerical measure of complexity explodes, as depicted in figure 5.2A. Generally speaking, and consistent with the hierarchical model, we want commanders with a tremendous span of authority and responsibility to exercise decisions with minimal depth. Leader attempts to violate this principle would be referred to as micromanagement in the business world, and the military pejoratively refers to generals with “a 1,000-mile screwdriver.” Disdain for this type of leadership behavior is practically motivated since no human beings can manage the resulting degree of complexity and make good decisions. Thus, the hierarchal structure is a proven way to manage this complexity (see fig. 5.2B).

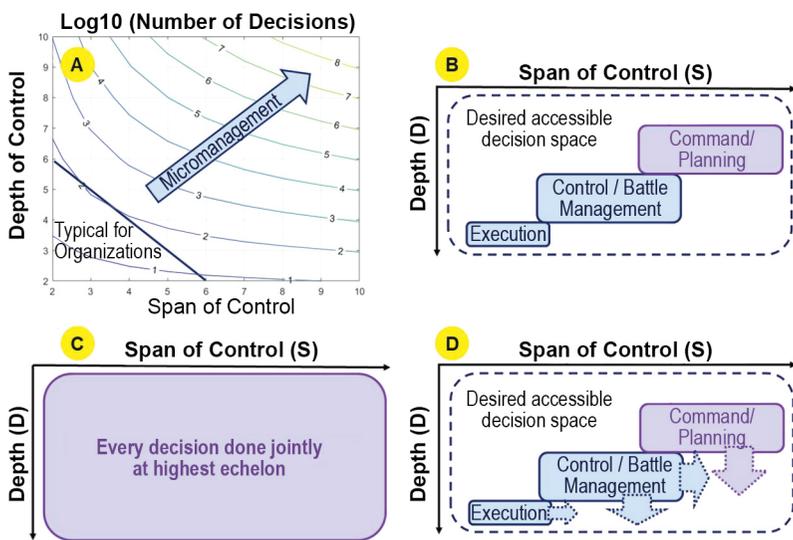


Figure 5.2. Managing complexity while maximizing the decision space.

(A) There is value to maximizing the span and depth of decision-making, but expanding both simultaneously causes complexity to explode geometrically beyond that which a human or machine can manage. (B) A traditional hierarchical structure limits the depth of control inversely to the span of control, minimizing complexity to enable speed. (C) Commanders may have regrets and concerns that an ideal solution to a nearly intractable problem exists somewhere in a broad decision space if only they had the ability to discover and implement the solution. This potential leads commanders to desire the ability to make every decision jointly at the highest echelon, no matter how minute. This approach does indeed maximize warfighting capability and resiliency but unfortunately collapses and destroys speed due to the resulting explosion of complexity. (D) Dynamic management of span and depth of control (“C2 of C2”) provides the ability to access most of the physically realizable decision space to manage contingences (adaptability) and mitigate losses (resilience) with a level of complexity only slightly worse than the baseline hierarchical approach (speed).

Unfortunately, modern warfare is inherently complex, and ignoring that complexity is a pathway to failure. The one war-winning option may be some finely detailed, precise action buried in one element of the decision space. This factor has led recent commanders to covet more information and an increasing ability to finely create every detailed-level decision. It is at the heart of the ongoing

evolution of the Combined Joint All-Domain Command and Control (CJADC2) strategy. In a sensor-to-shooter kill chain example, there is a strong leadership desire that at a centralized location, the senior command can assign a kill chain to every target and have full flexibility to pair sensors, weapons, and platforms for each kill chain. It is a philosophy of “any and all” permutations made available to the commander to maximize the decision space (see fig. 5.2C). This desire is understandable because the only way to neutralize a key target might be a single target-sensor-weapon pairing unachievable through the normal hierarchy. But always fighting a war like this is impractical, and, in fact, most of those options will not add value, with many being physically unachievable.

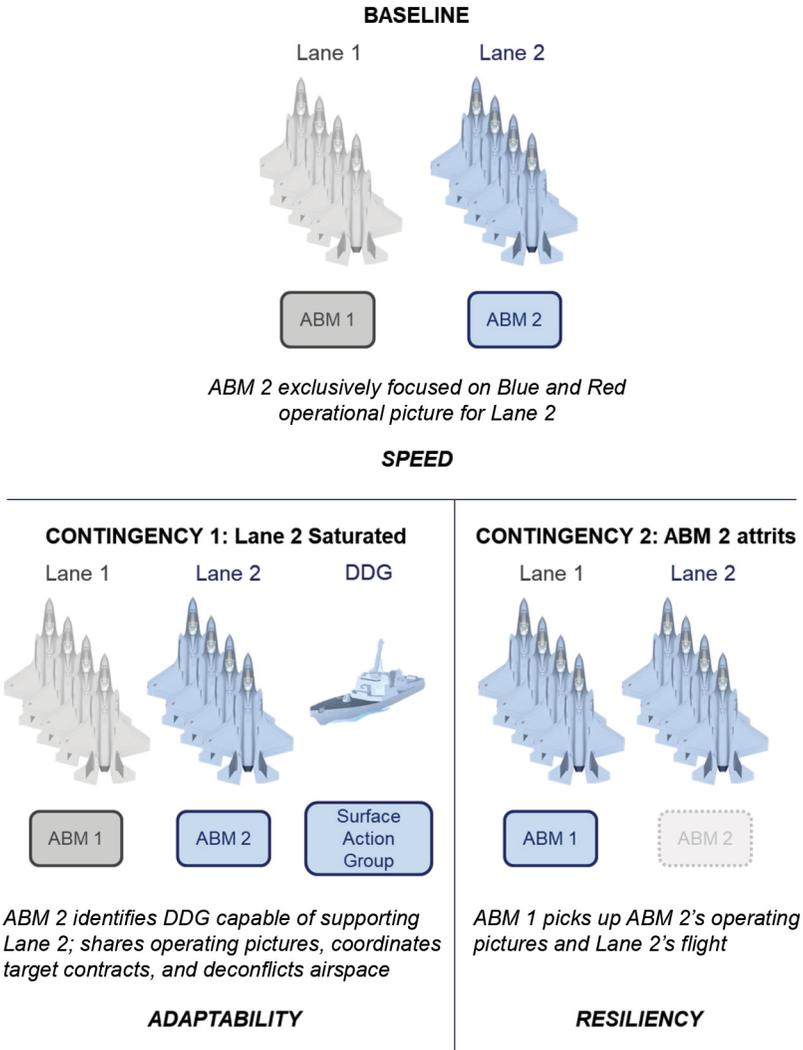
What is needed is a means of moving about this decision space, and here, human-machine symbiosis can again help to share the cognitive burden. A commander, or for that matter lower-echelon tactical operator, needs the ability to dynamically vary the level of complexity to move in the decision space to meet the reality of current mission needs. In figure 5.2D, theater commanders might spend the majority of time in the “command/planning” box with a large span but minimal depth. In this box, they spend most of their time giving out general mission orders to functional commanders who pass this commander’s intent down and across the force. However, suppose a high-value target materializes unexpectedly and no units are postured to prosecute this target under their current orders. This target may be critical enough that the theater commander now needs to temporarily get into the details. They may need to identify a particular platform that can be assigned to the target, and if that platform cannot neutralize the target with its own weapon systems, the theater commander may need to discover and task multiple assets to provide the sensors and connectivity to create a long-range kill chain to prosecute the target. The commander needs the flexibility to accept and manage a greater degree of complexity to temporarily explore the corners of the option space outside their baseline scope and then return to nominal, lower-complexity decision-making. This process needs to occur faster than the high-value target can understand it is being targeted and take evasive action or simply complete its mission and return home. This scenario demonstrates “getting inside the OODA loop” at an operational level.

The same concept of variable complexity to expand options applies from the bottom up with the tactical operator. In figure 5.2B, this op-

erator lives in the “execution” box. The operator’s span is limited—perhaps an air battle manager controlling a lane of fighters—but highly specific, detailed decisions must be made: which targets are valid, which blue asset should attack each target, warnings of threats to blue assets, and so forth. Additional insights into other blue forces or targets outside that lane are superfluous information that makes the operator’s job unnecessarily more complex. However, if that lane starts getting saturated, that battle manager may suddenly need more options. If another lane of fighters or a surface action group is available to help, the operator may now want to dynamically expand their span of control and accept a little more complexity for a limited period to call for help and manage a now-joint engagement package, given the flexibility of the C2 of C2 model in figure 5.2D. The key is the dynamic flexibility of the span of C2. The baseline limitation to span is set to one lane of fighters under control to minimize complexity and uncertainty and optimize efficiency, but for a moment in time, the operator may want to expand that span to include the destroyer or another lane of F-35s to provide options for operational resiliency.

How is the above scenario a human-machine symbiosis opportunity? In the open/closed world cognitive model, most of the operational-level decisions are abstract, open world problems, but it turns out that exploration of the option space is more closed. At the same time, option exploration, “orient” in the OODA loop framework, is a mostly closed problem. The status of blue assets is a discrete, knowable set of information, as is their physical ability to execute a new, unplanned task. The machine helps manage the temporary complexity of expanding the optionality space to discover and assess options, but the human makes the “decide” decision, selecting which machine-generated option is most appropriate given the context of the current problem.

To make this scenario even more specific, consider the air battle management example in more detail. Figure 5.3 shows three tactical echelon units, two fighter air battle managers (ABM) and a destroyer; for a moment, let us focus on the second ABM. The ABM needs information about only their lane of fighters: blue information—position, fuel, and weapons, and red—location, identification, and priority. Any information about the other two units or anything else in the battlespace is superfluous at that moment and adds an unnecessary cognitive burden. However, in this example, our second ABM starts getting overrun and needs help. In this situation, additional information—greater optionality—is invaluable and is where the machine comes in.



Legend

DDG refers to a guided missile destroyer class of ship

Figure 5.3. An air battle management example of how variable control models enable adaptability and resiliency while minimizing complexity and maintaining speed. Human-machine symbiosis leverages machine intelligence to manage data flow and exposure in response to the mission situation to enable this kind of variable decision-making.

Today, if humans are left to manage this fight themselves, they do not even know two other units might be able to help. (This is why many leaders demand a common operational picture or COP be distributed to everyone in the fight, but back to worries about cognitive overload.) They will either do their best with what they have or put out pleas for assistance, once again, manually through voice or chat. They are unlikely to get help because the other units do not have enough information to determine if they can assist or the impact to their missions. If they offered to help, they would have to manually coordinate who will engage which target, how tracks will get passed to different weapon systems, how airspace will be deconflicted, and possibly how platforms will be rerouted. Implementing this collaborative OODA loop manually is time-consuming and if too slow, the fight could be over before help arrives.

Fortunately, the machine is perfectly positioned to add speed and pick up the complexity burden in several key steps of this process. Start with finding and curating information. This is a machine-manageable, closed world cognitive process. AI could be applied to information and network management, ensuring that information related to a COP is known and accessible even if it is not relevant to the human partners at that time. This application is the automation of “observe.” Next, when the ABM humans decide to ask for help, AI is also well suited to search the data it has already found to identify possible assisting units and pre-assess the physical suitability of those units to help (e.g., are they in range of their weapons?). This assessment is also a closed world problem but complicated for a human based on the computations involved. The machine relieves a significant cognitive burden by simply presenting the humans with a list of already evaluated options (e.g., Green = high confidence, Red = impossible, Yellow = maybe but risky and complicated). This type of problem-solving is the automation of “orient.” The humans can then negotiate between their units to determine if anyone can help and “decide” to share targets. Many factors and risks are associated with this decision on both sides of the negotiation, so it is a more open world problem better suited to humans; however, the machine can still help answer questions quickly about quantitative risk and reward. Finally, the process of handing off targets, managing and deconflicting tasks, and performing other detail-level replanning is an operational “act” function given almost completely to the machine. Again, while the computations involved can be complicated, the problem is in a concrete, closed world context.

In this example, human-machine symbiosis is making the joint force more effective. It can also make the force more resilient. In the same scenario, suppose that instead of being overwhelmed, the second ABM unit attrits. The same information and decision management process described above for engaging targets more effectively can be used to enable the first ABM unit to pick up the attrited unit's mission, making the force more resilient. These examples are instances of CJADC2 implementation at the edge without the complexity of a centralized upper-echelon command to make dynamic, joint force decisions. The cost of this operational model is a momentary increase in complexity at the edge, but the machine can help the human manage this.

Note that this model of adaptive management of a joint, all-domain force, continuously tailored to the current situation, is at the heart of DARPA's "Mosaic warfare" strategy.¹¹ DARPA has been developing the adaptive communications and autonomy technology needed to implement scenarios such as those just described. In 2019, DARPA sponsored the Center for Strategy and Budgetary Analysis (CSBA), a defense policy think tank, to conduct a war game to assess the value of Mosaic warfare tools and concepts.¹²

The war game considered combat between two reasonably matched forces and was conducted with two distinct strategies. A "traditional" engagement was run as an experimental control. It employed a conventional force with monolithic capabilities that used a manual decision-making process. In contrast, the "Mosaic" engagement used a more diverse force mix with some simple machine decision aids to assist the human commander in managing the complexity inherent with this type of force. (While the Mosaic force was more diverse, it represented net firepower equivalent to the traditional force's in the number of assets and weapons. It was arguably weaker in that some of the diverse Mosaic assets were lower performing than those of the traditional force when comparing them at the platform level.)

Machine tools managing complexity to provide more options was a war-winning approach, at least in this war game. We can glean several key insights. The first is a tangible representation of the notional examples presented previously. Machines helping humans manage complexity provided greater optionality, and within this greater set of options were actions that led to achieving the scenario objectives (whereas the traditional force could not achieve them).

In addition, there was a fascinating outcome regarding the speed of the OODA loop. Complexity management not only helped with the

speed of decision-making but also accelerated it by the nature of the decisions being made (fig. 5.4). Let us unpack this counterintuitive result. It all has to do with risk management. For the Mosaic force, the types of decisions associated with a more diverse force and set of options tended to be more incremental and lower risk than the big, heavy-commitment movements of the traditional force. Since the decisions were fast, incremental, and lower risk, the Mosaic force commander did not need to ponder each decision as deeply. This notion of decision aids enabling diversity generated a virtuous feedback cycle where the speed of incremental decisions enabled overall faster decision-making. With just a little help from the machine, the human partner became a faster decision-maker *because of*, not in spite of, more complexity!¹³

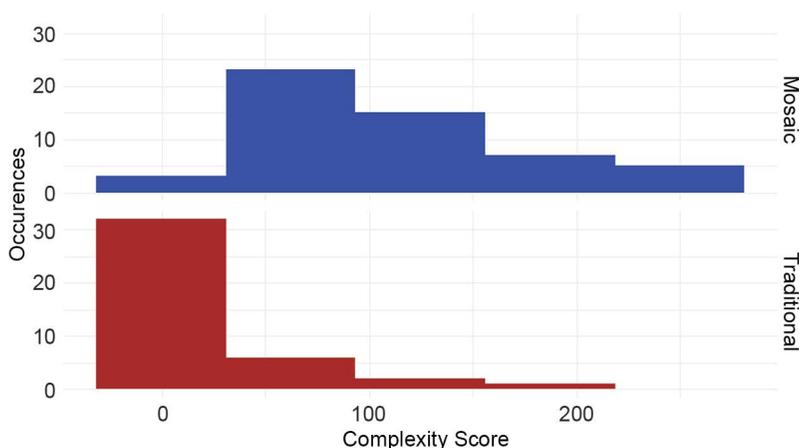
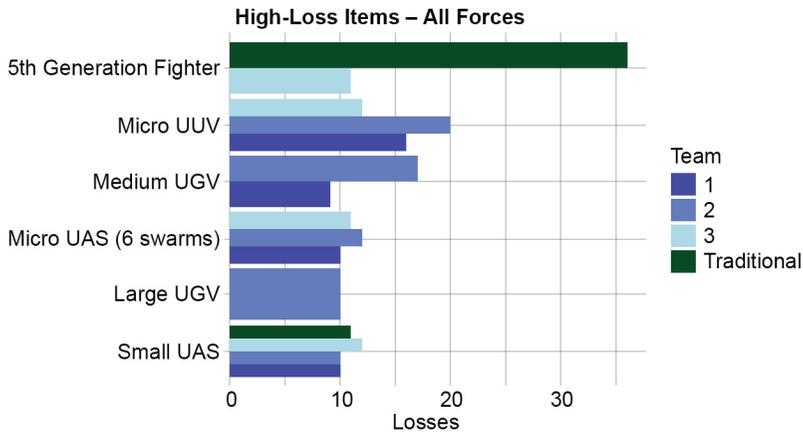


Figure 5.4. Data from the Mosaic war game showing the number vs. complexity of decisions made by Mosaic and traditional force commanders. (Reproduced from Bryan Clark et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* [Center for Strategic and Budgetary Assessment, February 11, 2020], 48, <https://csbaonline.org/>.)

Most Mosaic force decisions had a greater overall complexity, yet the Mosaic force commander could make significantly more decisions overall. In addition to simpler decision aids, representing rudimentary human-machine symbiosis, each Mosaic force decision tended to be lower risk, and this lesser regret also accelerated decision-making.¹⁴

Another interesting insight also relates to managing risk, but in this case, survivability of the force (fig. 5.5). The Mosaic force experienced greater attrition, but force diversity enabled the commander

to tailor attrition more strategically. Greater losses of lower-value assets were accepted more freely in exchange for achieving objectives while enhancing the survivability of higher-value assets. The traditional force experienced lower losses overall but at the cost of losing more high-value assets—and failure to achieve victory. Once again, a faster OODA loop = victory.



Legend

UAS – unmanned aircraft system

UGV – unmanned ground vehicle

UUV – unmanned underwater vehicle

Figure 5.5. While various Mosaic force commanders consistently lost more assets, they were overall much lower value. This lower risk of loss and proportionately lower regret associated with each decision contributes to accelerated decision-making. (Reproduced from Bryan Clark et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* [Center for Strategic and Budgetary Assessment, February 11, 2020], 54, <https://csbaonline.org/>.)

Accelerating the Strategic-Level OODA Loop = Fielding More Options Faster

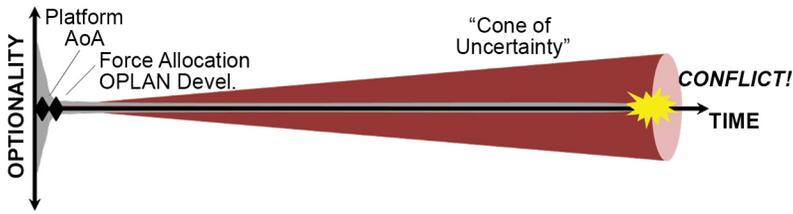
Regardless of echelon, all the examples presented so far involved OODA loops in conflict, but the same OODA principles apply to strategic-level decision-making. Just as in conflict, speed = victory. Developing

the future force needed to prevail in great power competition requires developing policy, allocating resources, and making acquisition decisions—the strategic OODA loop—more quickly and adaptively than the adversary. Despite the prowess of US warfighters at speed of decision in conflict, fast, adaptive acquisition and fielding of the force is unfortunately not a quality typically associated with the DOD.

One can make a case that our lack of speed and agility in force design and capability development is heavily linked to risk management associated with complexity. We have evolved to a force with incredibly complex, capable individual platforms. This complexity drives the cost of the platform and the time it takes to field a new one. Therefore, we have fewer platforms, and they are planned with long operational life cycles. These factors combine to produce a negative feedback cycle that is the inverse of that described in the Mosaic war game. Being committed for a long time to a limited number and diversity of expensive, complex platforms means we cannot afford to make a mistake. This fear drives a risk aversion that goes beyond culture: it is actually logical if this is our force design strategy. Force design also runs into yet another conflicting issue, that of uncertainty.

Warfare and international security strategy are inherently uncertain. No one knows when a conflict may occur, what events trigger it, what the nature of the conflict will be, and what the exact capabilities and strategy of the adversary will be. Despite strategists' attempts to forecast, this uncertainty is also highly nonstationary; the farther out one projects, the greater the uncertainty grows. In strategy circles, this correlation is sometimes referred to as the “cone of uncertainty.”¹⁵

How the US DOD tends to manage this cone of uncertainty actually produces yet another negative feedback cycle. Because of the generally long process to field new capabilities and our subsequent long-term commitment to them, we need competencies far out on this cone, where the uncertainties are great. The direct way to try to mitigate this uncertainty is by overprovisioning capability, making the force so good with such high performance that it can accommodate whatever the future holds—high performance replaces high optionality. The negative feedback cycle is amplified because a high-performance system becomes yet more complex and expensive, rightly drives greater risk aversion, takes yet longer to field, and pushes us even further out on the cone of uncertainty (see fig. 5.6).



Legend

AoA – analysis of alternatives

OPLAN – operation plan

Figure 5.6. The “cone of uncertainty.” In a statistically stationary system, uncertainty grows linearly over time. If an irreversible decision about the design and fielding of a military is made years or decades before its intended employment, the uncertainty it must address grows enormously. There is therefore a high probability that the chosen system design is not optimized to that need. Therefore, its performance must be provisioned to far exceed the cone of uncertainty, driving the cost and complexity of most of our systems.

Following the example of the Mosaic war game, optionality combined with speed wins fights. A force composed years, if not decades, before intended employment and comprising small numbers of high-value assets increases risk, slows the OODA loop, and leaves us with a high probability that our forecasts are wrong. In contrast, what if we could design a force that could maximize optionality until the precise need was much clearer (fig. 5.7)? In the software design world, this concept is sometimes referred to as “deferred concretization.”¹⁶ There is always the need for some initial general consideration of requirements or product attributes to focus efforts—a demand signal that, in DOD capability development, might be an analysis of alternatives (AoA) study for a platform family of systems. However, instead of concretizing a specific design of a limited number of platforms and their roles in a force design, the whole family may be maintained for an extended, perhaps indefinite, period.

In the context of warfighting capabilities, deferred concretization leads directly to managing complexity—or at least transferring complexity from the platform to force design. Individual platforms, weapons, and mission systems are defined to simple requirements. They still must be designed to meet a near-term, specific warfighting function.

Doing so helps identify their immediate requirements but without the need to overprovision for all future, high-end contingencies. This type of limited, simple capability is analogous to the efficiency and task effectiveness delivered by lower-echelon units in the traditional hierarchical force structure discussed earlier. Then, just as in the examples of managing operational complexity, we need to be able to generate new force-level capability by repurposing and integrating these simple systems to produce much more capable effects.

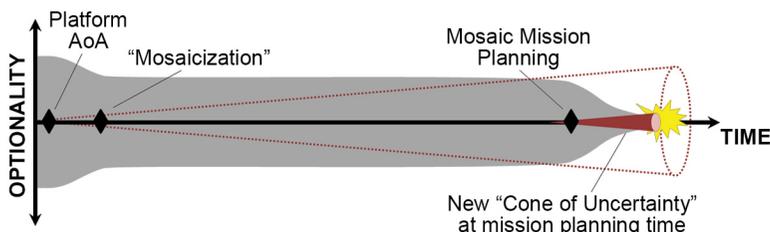


Figure 5.7. Decreasing the “cone of uncertainty.” If the decision of how a new capability is going to be used and the resulting system of systems capability can be deferred until closer to the time of need, the cone of uncertainty will be much smaller, and the net capability can be tailored much closer to optimization. This approach avoids the need to overprovision, as when the cone of uncertainty is forecast decades into the future, allowing the advantages of simpler, cheaper systems.

While the technical details are beyond the scope of this chapter, the ability to defer integration and repurposing is referred to as “Mosaicization” in figure 5.7 and includes approaches such as open standards, reference architectures, and software-defined networks. The optionality trade space is now some permutation of all the individual capabilities into “kill webs.” Just as operational complexity is managed by limiting the number of times battle managers and commanders need to make decisions outside their normal span and depth of control, the decision to integrate simple “Mosaic tile” weapons systems into a mission thread can be deferred to the exceptional times when the additional capability becomes critical. This paradigm enables creating kill chains by exception near the time of need when that need is much less uncertain.

Just as AI can potentially speed up the OODA loop at the tactical and operational levels, it may also be advantageous at the strategic level. Suppose we have the integration capabilities required to truly realize this vision of warfighting capabilities focused on specific threats

and composed at the time of need. Humans will still need decision support from machines in defining the requirements for the “Mosaic tiles” and for planning the kill web architecture at the time of concretization. For the former, one can imagine AI simulations helping to measure the value of a newly proposed system “tile.” It has its own limited performance requirements, but the simulation evaluates how well it stochastically contributes to the ensemble of capabilities that might be used in a kill web without overconstraining its specific role. For the latter, AI and other software analytics can help explore the optionality trade space against a specific need at the time of concretization to help the human select the best available set of “tiles,” construct the specific warfighting architecture, and model its effectiveness. This process is human-machine symbiosis at a strategic capability development level; if it can become fast enough, it can be pushed to the operational level as part of theater C2 for just-in-time kill web generation.

Further, just as our legacy approach to capability development leads to a negative feedback cycle, this AI-enhanced strategy development leads to a virtuous positive feedback cycle. Individual platforms and systems are now simpler and cheaper. They can be delivered on shorter timeframes and built to shorter mission lifetimes. This combination means they can be updated and replaced much faster, which means we can accept greater risk in defining and delivering them—which makes them cheaper and gets them here quicker; thus, the cycle continues to improve.

As a final thought, this same approach to an AI-enabled flexible hierarchy can be applied to the design of organizations themselves to achieve greatest utility while managing their complexity. There is a cycle in institutional design strategy to start with agility using small, ad hoc teams to get things done fast. As an enterprise grows, these teams become inefficient and, even worse, unable to address big, enterprise-level problems because they are stovepiped. To fix this situation, new organizations are created that either absorb the teams or add a management layer above them to manage them. Unfortunately, as enterprises grow, these organizations with expanding breadth and depth begin to die under the weight of the resulting complexity and bureaucratic drag that comes with it. The most effective model is one similar to the operationally flexible hierarchy—organizational units that can be focused and specialized but can bridge their resulting seams through dynamic, federated integration. But this organizational model is difficult to manage in practice, especially at scale. While this author

is not aware of any existing AI-driven tools for this kind of enterprise management, they are not beyond conception. Perhaps one day in the not-too-distant future, AI can help the human develop the institution that will develop the AI!

Conclusion

The US military is currently the most powerful fighting force in human history, and the combination of its capabilities, strong alliances, resiliency of mission command, and overall warfighter ethos enable it to prevail against any potential adversary. However, we cannot become complacent. The business world is filled with examples of dominant corporations that seemed untouchable in their industries—until they were not! Upstarts appeared, seemingly out of nowhere, and through agility and adaptation quickly brought them down in unexpected ways. They exemplify winning by “getting inside the OODA loop,” in this case the business market OODA loop. The US military fully understands the force multiplier provided by the speed of the OODA loop. We train our operators to achieve this speed at the tactical level and our commanders at the operational level. As the pace accelerates and the problems escalate in scale and complexity, we are just beginning to develop models of human-machine symbiosis to continue to stay inside the loop. As we move toward ever more complex theater, strategic, and enterprise problems, we need to think like operators, develop similar AI-driven decision aids, and act with the same operational practicality and speed, avoiding the institutional traps of overcomplicating our already highly complex challenges. Otherwise, we risk going the way of the twentieth-century industrial titans.

Notes

1. Mike Ryder and Carolyn Downs, “Rethinking Reflective Practice: John Boyd’s OODA Loop as an Alternative to Kolb,” *International Journal of Management Education* 20, no. 3 (November 1, 2022): 100703, <https://doi.org/10.1016/j.ijme.2022.100703>.

2. “Leeroy Jenkins,” undated post by Micah Shippee, YouTube, 2 min., 25 sec., <https://www.youtube.com/>.

3. Congress.gov, “Text – H.R. 4223 – 18th Congress (2023–2024): National AI Commission Act,” June 20, 2023, <https://www.congress.gov/>; and Terri Moon Cronk, “New DOD Chief Digital Artificial Intelligence Office Launches,” Department of Defense, February 4, 2022, <https://www.defense.gov/>.

4. Scott E. McIntosh, “The Wingman-Philosopher of MiG Alley: John Boyd and the OODA Loop,” *Air Power History* 58, no. 4 (2011): 24–33, <https://link.gale.com/>.

5. Christian Janiesch et al., “Machine Learning and Deep Learning,” *Electronic Markets* 31, no. 3 (September 1, 2021): 685–95, <https://doi.org/10.1007/s12525-021-00475-2>.
6. Mark Tran, “Deep Blue Computer Beats World Chess Champion,” *Guardian*, February 12, 1996, sec. Sport, <https://www.theguardian.com/>.
7. Tanguy Chouard, “The Go Files: AI Computer Wins First Match Against Master Go Player,” *Nature*, March 9, 2016, <https://doi.org/10.1038/nature.2016.19544>.
8. Lev Craig, “Enterprises Weigh Open Source Generative AI Risks,” *TechTarget*, November 17, 2023, <https://www.techtarget.com/>.
9. Bruce J. Schachter, *Automatic Target Recognition*, 4th ed. (SPIE Press, 2020), <https://spie.org/>.
10. “Collaborative Combat Aircraft (CCA), USA,” *Airforce Technology*, June 21, 2024, <https://www.airforce-technology.com/>.
11. “DARPA Tiles Together a Vision of Mosaic Warfare,” Defense Advanced Research Projects Agency, accessed December 20, 2023, <https://www.darpa.mil/>.
12. Bryan Clark et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Center for Strategic and Budgetary Assessment, February 11, 2020), <https://csbaonline.org/>.
13. It is interesting to note that this model of speed of decision is analogous to how the venture capital world operates. Each round of investment tends to be only incrementally larger than the previous, based on equally incremental growth in the company. However, this model still scales rapidly because the pace of the increments is fast, so start-ups can grow quickly despite lagging funding. Investors can afford to move rapidly because the risk associated with each small increment is low and kept low as absolute dollars of a round grow due to a company’s incremental progress. See Eric Ries, *The Lean Startup: How Today’s Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses*, 1st ed. (Crown Business, 2011).
14. See Clark et al., *Mosaic Warfare*, 48.
15. Steve McConnell, *Software Project Survival Guide*, 1st ed., Developer Best Practices 20 (Microsoft Press, 1997), <https://www.microsoftpressstore.com/>.
16. Awanish Pandey et al., “Deferred Concretization in Symbolic Execution via Fuzzing,” in *Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis*, ISSTA 2019: 28th ACM SIGSOFT International Symposium on Software Testing and Analysis, Beijing, China (Association for Computing Machinery, 2019), 228–38, <https://doi.org/10.1145/3293882.3330554>.

Chapter 6

Mind-Tech Teaming in Defense

Integration and Imagination

Michael Groen, former Director, Joint Artificial Intelligence Center

Abstract

The evolution of military effectiveness has largely been a continued search for “competitive advantage.” Until recent decades, that advantage has come through augmentation by increasingly capable machines and the growth of human staff organizations to expand the scale of operations. The onset of digital transformation and the emergence of applied artificial intelligence (AI) has now made the augmentation of humans with intelligent machines a reality. This integration has enormous implications for gaining competitive advantages through scaled cognition, precision lethality, and accelerated tempo. It also raises issues regarding the ethical boundaries of human-machine teaming on the modern battlefield. Future success will require new imagination in the roles and processes of machines and humans in integrated warfighting.

This chapter describes how the introduction of modern digital technologies, including AI, has already changed the character of military decision-making architectures and promises even more. It discusses the continued trajectory toward “competitive advantage” gained by combining the virtues of data scale, machine speed, and human decision-making. This promising combination of virtues potentially achieves awareness, tempo, and scale through newly designed processes that replace older methods. Perhaps most importantly, this chapter describes the necessity to inspire imagination to understand and visualize the opportunities of a complex military decision environment transformed by changing roles among humans and machines.

Competitive Advantage—Humans and Machines

The trajectory of military capability has been one of continued advancement through technological artifacts. From Archimedes on

the ramparts of Syracuse to the rise of AI, technology and success in war have always been entangled but never equivalent. Technology does not stand alone in military modernization. Adoption of new technologies into weapons systems has been necessary but not sufficient to gain competitive advantage. New insights into better organizations, tactics, processes, and relationships have often brought old technology to bear in new ways. The emergence of blitzkrieg (or “lightning war”) in the early days of World War II was not the outcome of a new technology. Rather, it was a creative combination of existing technologies to achieve new capabilities.¹ These new combinations, enabled by technology, proved devastating to opponents who operated at a much slower tempo. Through the ages, nations and militaries have competed for a technological edge that could bring about victory on the battlefield. In war, but also in peace, this continued spiral of military technology can be thought of as a continuous posturing for competitive advantage over an opponent.

From the beginning, warfare’s evolution (and the search for competitive advantage) has been closely aligned with the physical artifacts of lethality. From bronze to iron to steel, advances in warfare technology have been linked to the management of physical power. For the ancients, competitive advantage was centered on the ability to apply physical technology more effectively than one’s opponent. That approach has been applied across increasingly larger scales. As the scale of modern war continued to grow, the effectiveness of the mind of the human commander was increasingly challenged. Instead of coup d’oeil,² the “inner eye” of battlefield understanding, modern commanders became entangled in managing and directing a variety of physical enterprises to achieve positional, logistical, or lethality advantage in each aspect of the battle. Command and control thus expanded from the brilliance of a singular commander directing the action to larger and more diffuse decision environments. It was no longer sufficient to manage *each* aspect of the battle when competitive advantage required the integrated application of *all* of them.

The arrival of the digital age saw rapid gains in competitive advantage and operational integration through better organization, communication, and digital integration. Physical weapons and platforms remained the center of lethality, but competitive advantage increasingly began to emerge from the ability of humans to perceive their threat environments, collaborate with human teammates, and develop more complex plans. With increasing volumes of data available, battles and campaigns began

to exceed the ability of a single commander to track all relevant aspects of operations, intelligence, logistics, and the host of functions that serve as the skeleton of a successful campaign. Large staffs were required to effectively integrate a more complex command and control environment.³

The addition of legions of clerks, drivers, communicators, paymasters, and other noncombatant roles provided “cognitive mass” to operate these large-scale functions. Competitive advantage now came from incorporating more humans into ever-larger enterprises. While this scaled the decision environment, the resultant fragmentation of staff functions also reflected a “fragmentation of cognizance.” The limitations of the commander’s mind led to dealing with complexity by distributing cognition to other subordinate (human) enterprises. Competitive advantage increasingly came from the distributed operations of a large staff of individual functional enterprises, held together by the articulated commander’s intent. The primary role of commanders shifted from individual tactical brilliance to the management of a complex human enterprise. Timing, integration, air support, infrastructure, casualty management, fuel flow, and ammunition became the day-to-day artifacts of command and control. With increasing predigital information flows coming from increasingly complex supporting enterprises, the ability of a commander (even with a large staff) to truly understand and manage all aspects of a successful military campaign was in doubt.

The successful commander became the one who could absorb large volumes of information and act on the broad range of opportunities being generated by a true “army” of staff functions. Individual battlefield heroics were admired, but campaign success came from a commander’s ability to articulate campaign intent, priorities, sequencing, and integration. Legions of humans created a distributed intellect that executed priorities, but these often remained opaque, segmented, or selfishly guarded by functionaries. While segmented enterprises had lots of data, it was not effectively shared, actioned, or integrated outside the mind of the commander. The mind of the commander remained the singular point of integration for battlefield information.

Going Digital—Machines and Humans

The broad digital transformation of the 2000s began to reveal some of the opportunities for a Mind(s)-Tech Nexus in defense. In the context

of campaign advantage, early office automation tools blazed a trail of information efficiency and an ability to better manage large-scale functional enterprises. The maturation and growth of more advanced digital networking now began to leverage data in ways previously impossible. “Information machines” became more prolific, but these were generally digital manifestations of manual processes. Digital technology began to achieve efficiency, but not yet in a way that was transformative. The early introduction of military digital technologies largely mimicked older paper processes. Information machines were largely focused on either managing individual functional processes or providing specialized software for particular weapons systems. The integrative opportunities for data and information to drive competitive advantage remained latent, as the “killer app” that would make data and information truly a competitive advantage had yet to emerge.

Competitive Machine Advantage Through “Narrow AI”

The emergence of practical applications of AI in the late 2010s represented a transformational change, as “cognitive mass” could now be achieved with a combination of the human intelligence of large staffs and the opportunity of integrated machine intelligence. With this change, it was possible to consider the replacement of some level of cognitive workload from large staffs to machine-assisted applications. The earliest new manifestations of machine intelligence in defense were “narrow AI” applications. These simple algorithms were employed for detecting objects, identifying threats, triggering conditions-based actions, and other simple applications.⁴ Narrow AI algorithms were trained to monitor individual data flows, detect patterns, and alert human decision-makers when a defined indication was detected. Narrow AI could relieve cognitive burdens (e.g., counting, watching, detecting) while presenting humans with alerts or warnings. These applications shifted cognitive burdens to machine-executed subprocesses that informed later human decision-making. Machines began to substitute for the cognitive mass previously supplied by many human minds.

As information applications began to flourish, new potential uses for narrow AI began to proliferate. If narrow AI could monitor battlefield conditions for an operational use case, why could it not also be used to monitor supply inventories and compare them to expected

demand? Could these narrow applications not also assess patterns in threat activity, predict impacts of weather, or send an alert when a trigger was reached? The proliferation of narrow AI for use in a broader range of cases rapidly ensued. It also quickly became obvious that even narrow AI had significant dependencies. To be effective, narrow AI depended on functional expertise, reliable data inputs, clear process definition, distributed networks, and shared data availability across platforms or military services.

Emerging Opportunities Through “Scale”

A growing imagination for thousands of narrow information processes monitored by virtual machine agents illuminated the opportunities for application at a larger scale. Visualizing functional processes through the lens of digital automation allowed clear advantages in efficiency, speed, and integration. These benefits implied initiating a new way to think about information challenges. Rather than a focus on the technology to be adopted, attention to the processes to be optimized generated new insights. It became apparent that an integrated enterprise operating on a host of narrow AI applications created a baseline of shared understanding that could accelerate human decision processes. Process integration produced the integration of insights across multiple staff functions. The insights available to a human decision-maker through dozens (or thousands) of narrow AI applications could be thought of as “eyeglasses for the mind.”⁵ Layers of machine-curated data flows allowed layered cognition. It extended a commander’s or staff’s ability to gain a sense of all aspects of a complex battlefield situation—without diverting precious human cognitive capacity to continuously monitoring each relevant factor.

In this environment, the Mind-Tech Nexus leaned on core processes—not as a definitive set of plans and actions but as a continuous curation of baseline information that facilitated better decision-making. As common understanding grew, leaders began to recognize the opportunities for broad enterprise management operating on a common knowledge baseline. Process management, data insights, and integrated knowledge of friendly and enemy forces on the battlefield accelerated *integrated* understanding.⁶ Layered cognition of the individual functional enterprises (previously hidden from broader view) also became possible. Distributed functional enterprises, previously left to manage

their own functions without reference to the others, were now shared and illuminated for better integrated decision-making.

Generative Insights

As technology advanced, opportunities to build on nascent human-machine relationships came into view. Humans have come to accept AI technologies for narrow automated functions or machine-assisted cognitive tasks. In time, these have become an almost invisible component of modern information flow and knowledge management. “Generative AI” now demonstrates an ability to take on even more complex cognitive tasks. Narrow AI has the ability to do simple tasks in a deterministic environment (observation/programmed response). Generative AI added the ability to generate original responses through its understanding of data relationships in its underlying training data set (typically words, but other data types are also used). Where conventional computing manipulated data to retrieve deterministic outputs, generative AI could now formulate original outputs through its “most probable understanding” of the relationships between data elements it had been trained with. Outputs of this process are probabilistic rather than deterministic. Thus, generative AI produces the “best probable” answers given the data environment. Generative insights move the Mind-Tech Nexus from deterministic outputs of narrow AI to a generative environment much more conducive to collaboration with human minds. If narrow AI relieved the human mind of data management drudgery, generative AI allowed the human mind to extend its imagination into potential future states and the unknown. Put another way, narrow AI manages enterprise data that defines what “is.” Generative AI fills a new role, as it helps the imagination of what future states “*could be*” based on its training data set. (In either case, a robust ecosystem of testing, validation, and governance is clearly required.)

Generative AI remains in its early stages of maturity but is rapidly expanding to encompass a wider range of commercial and government applications. The Mind-Tech Nexus is already shifting from a deterministic generation of answers based on classical computing to a proactive, innovative partnership that can predict new opportunities, intuit relevant information, optimize decision environments, and proactively address risks to future plans. As generative AI matures, it will play a key role in forecasting, anticipating, alerting, and creative problem-solving.

Human(s)-Machine(s) Teaming

With new types of computing and larger-scale challenges to understand, the combined skills of human imagination and machine calculation require more complex relationships. Human-machine teaming (HMT) presents a new range of possibilities and opportunities in the Mind-Tech Nexus. HMT brings the calculation power of machines and matches it with the intuitive knowledge of humans.⁷ Often, HMT conjures images of robotic systems executing missions with some degree of preprogrammed autonomy. In fact, the vast preponderance of human-machine teams are virtual software agents operating with humans within large data environments or specific battlefield functions. It may be more appropriate to talk about human(s)-machine(s) teams, as these relationships will be much more complex than the “robot dogs” or semiautonomous drones that populate today’s battlefield environments. A battlefield with (perhaps) thousands of virtual and physical machine agents will require an entirely new lexicon and policy environment. The Mind-Tech Nexus must now evolve to optimize the role of both the human mind (creativity, judgment, values, self-perception) and machine efficiency (scaled information, fast calculation, unlimited memory).⁸

In this partnership, a one-to-one relationship between a human and a single machine agent would be a poor allocation of human intelligence. Individual humans might continually manage hundreds of virtual machines. Virtual agents will perform continual optimization and monitoring to alert human users of relevant changes in the information environment. Physical machines with some degree of autonomy may respond to threats, perform noncritical battlefield tasks, evacuate humans from danger, or operate in domains that cannot support human presence. The difference between an artificially intelligent “teammate” and a dumb “tool” may differentiate HMT from other machine artifacts on the battlefield.

Ethical Applications

The Department of Defense (DOD) has led in articulating ethical AI principles consistent with the law of armed conflict. It has been an international leader in expanding communities of practice to gain alignment in the ethical uses of AI and autonomy in defense within a

growing partnership among nations. Similarly, the DOD has been at the forefront of communicating practice for a professional targeting community (with an associated body of ethical best-practice). In the 2023 update of Defense Directive 3000.09, the DOD established the process, format, participants, and approach for issues of lethal autonomy in weapon systems.⁹ These policies will surely be tested as increasingly complex autonomy proliferates within weapons systems, command and control processes, and support processes.

The Future of the Mind-Tech Team

The role and authority of commanders, staff officers, machine assistants, and algorithms will each require careful consideration. If a future commander chooses not to adhere to an algorithmically determined optimal course of action, what liability does that commander inherit? If a human soldier becomes a casualty when a robot could have executed the mission, how will that decision be judged? Who can approve the commitment of an expensive robotic system to a mission that will likely result in its destruction? Are robotic systems to be protected at the expense of human lives? The authority and efficacy of machine-generated recommendations are likely to be questioned for a variety of human reasons. Even with commanders articulating a clear course of action, the hundreds of micro-decisions that support the execution of a complex operation will require new rule sets and processes. Practical considerations will also be a driving force in the evolution of HMT and the Mind-Tech Nexus. Can a machine change its “master” (to a different human) when circumstances suggest or some notional battlespace line is crossed? Can machines organize their own partnerships (e.g., swarm) to achieve a defined effect? What risk is the machine allowed to take with its own well-being? When a friendly machine operates in physical space, who does it deconflict with? What if a specialized robot has a greater operational “value” than a human soldier? The challenges associated with battlefield machine teammates are not manageable through a purely technical or isolated mission lens. Colloquially, it is noted that “humans are good at asking the right questions, while machines are good at finding the right answers.” With generative AI articulating possible future states, the HMT partnership potentially gains the ability to take advantage of better questions and answers to achieve systemic warfighting

optimization. These observations suggest the need for an “operating system” and operating norms for HMT and the Mind-Tech Nexus.

A complementary relationship between machine and human functions, integrated in a way that optimizes the advantages of both, offers the promise of gaining opportunities at a much greater tactical and operational tempo than humans alone can generate. The outcome might be new processes, optimized operational design, or evolving training to match evolving technological opportunities and more. The DOD and its international partners have demonstrated a strong commitment to responsible AI and related technologies. HMT offers an additional area for the consideration of a body of approved practices, limitations, and policies. For the Mind-Tech Nexus, a similar approach to capturing how we think about HMT and the roles of humans and machines deserves a similar effort.

The Mind-Tech Team and Change

As we recall from the opening paragraphs of this chapter, warfare first progressed through advances in physical lethality. It took years to recognize and accept the role of advances in cognitive applications as a natural extension of human cognition against an accelerating and broadening character of war. Not only the character of war is evolving. The blurring of lines between human and machine functions in HMT will likely also raise questions about the efficacy and value of both humans and machines in combat environments. In time, it may be more than “roles” and “missions” that will differentiate humans and machines in partnership. Already, advanced research into human augmentation may disrupt our narrow categorizations of humans “or” machines. Teaming implies a degree of moral agency on both sides of the partnership. While human character can be frail, the utilization of machines in sensitive tasks may be equally morally fraught. Defining the degree and types of agency that must be considered for machines on the battlefield requires a new set of rules. Agency raises the question of permissible machine actions on a modern battlefield grounded in legal imperatives, moral imperatives, and “com-paratives.”¹⁰ Extending the technological into domains currently governed by ethical and moral rule sets is sure to create challenges for the Mind-Tech team.

The world is entering a transformative period, the likes of which are unprecedented. Digital transformation, artificial intelligence, and

comprehensive digital integration will change the form of (i.e., *transform*) our processes, industries, economies, security, and societies. Managing the evolving Mind-Tech environment is essential to ensure the safety, health, prosperity, and defense of our citizens and our nations. In the face of a hurricane of technological change, it will be easy to fall into the slipstream of comfort and ease while autocrats, democrats, plutocrats, and algorithms reshape our decision environments. It is for the practitioners of national defense and security to ensure we approach new technology, habits, and possibilities with the right ethics, policies, and oversight. Only then will we gain the transformational advantages our current environment offers and preserve them for those who follow in our footsteps.

Notes

1. History.com, “Blitzkrieg,” History, December 12, 2022, <https://www.history.com/>.
2. Carl von Clausewitz, *On War*, trans. J. J. Graham, 2nd ed., vol. 1 (Kegan Paul, Trench, Trubner & Co., 1909), <https://www.icct.nl/>.
3. James D. Hittle, *The Military Staff: Its History and Development* (Military Service Publishing Company, 1944; repr. Barakaldo Books, 2020), <https://www.everand.com/>.
4. Vijay Kanade, “What Is Narrow Artificial Intelligence (AI)? Definition, Challenges, and Best Practices for 2022,” *Spiceworks* (blog), March 22, 2022, <https://www.spiceworks.com/>.
5. Department of Defense, “Honorable Robert O. Work, Vice Chair, National Security Commission on Artificial Intelligence, and Marine Corps Lieutenant General Michael S. Groen, Director, Joint Artificial Intelligence Center, Hold a Press Briefing on Artificial Intelligence,” transcript, April 9, 2021, <https://www.defense.gov/>.
6. Department of Defense, “Joint Artificial Intelligence Center Director Briefs Reporters on Efforts to Scale AI,” transcript, November 24, 2020, <https://www.defense.gov/>.
7. Patricia McDermott et al., *Human-Machine Teaming Systems Engineering Guide* (MITRE, December 11, 2018), <https://www.mitre.org/>.
8. J. E. (Hans) Korteling et al., “Human- versus Artificial Intelligence,” *Frontiers in Artificial Intelligence* 4 (March 25, 2021), <https://doi.org/10.3389/frai.2021.622364>.
9. DOD Directive 3000.09, *Autonomy in Weapon Systems*, January 25, 2023, <https://www.esd.whs.mil/>.
10. “Com-paratives” contemplate the limitations of human abilities in functions that machines could handle more accurately, faster, and with greater care/fidelity. Thus, is it “ethical” to put a sleepy, tired, scared human on watch when a machine would be demonstrably more accurate? Does the comparison to human performance under expected conditions favor a machine? Will employing a machine contribute to the preservation of human life?

Chapter 7

Artificial Intelligence and Perception in Crisis and Conflict

Mating Twenty-First-Century Technologies with Eighteenth-Century Minds

*Lt. Gen. John (Jack) N. T. Shanahan, USAF, Retired, former
Director, DOD Joint Artificial Intelligence Center*

Abstract

We are now witnessing the early outlines of the third major revolution in our species' history—a digital revolution. As new technologies—especially AI-enabled capabilities—diffuse throughout militaries, they will change the character of warfare. The impacts of emerging and disruptive technologies on human perception and cognition, to include the use of information as a precision weapon, could be momentous but are not yet well understood. I argue that there are fundamental differences in the effects generated by new technologies as compared to previous technologies. This is due to the unique self-learning capability innate in AI models along with the unprecedented pace of change, the breadth and depth of diffusion, and the rate of adoption of new technologies to include generative AI. I contend that optimizing the integration of humans and AI-enabled machines, which in turn depends on redesigning the interfaces between humans and machines and recalibrating human and machine roles and responsibilities, will be one of the most important and defining features of future military and intelligence operations in the digital age.¹

Now the partial end of the postulated superiority of human reason, together with the proliferation of machines that can match or surpass human intelligence, promises transformations potentially more profound than even those of the Enlightenment. Even if advances in AI do not produce artificial general intelligence (AGI) . . . the advent of AI will alter humanity's concept of reality and therefore of itself.

—Henry Kissinger, Eric Schmidt, and Daniel Huttenlocher
The Age of AI and Our Human Future

Since I will argue that emerging and disruptive technologies such as artificial intelligence (AI) can have an outsized influence on the *Orientation* stage of the Observe-Orient-Decide-Act (OODA) Loop,² it is fair to begin by acknowledging how my own professional and personal experiences have shaped my views of the Mind-Tech Nexus in crisis and conflict. I accept that how I view an AI-enabled future is influenced by a lifetime spent in the never-ending feedback-feed forward loops between my own personal orientation, observations, and decisions. Orientation shapes observations, and observations affect orientation and decision-making. In considering the impacts of disruptive technologies on cognition, I have been shaped by a unique thirty-six-year career in uniform in fields as diverse as aviation, intelligence, command and control, policy, a combatant command headquarters, and command at the squadron, group, wing, agency, and numbered air force (NAF) levels. More specifically, my views on this topic have also been guided considerably by five distinct experiences over the past decade: as the Joint Staff J39 or Deputy Director for Global Operations (DDGO) from 2011 to 2013, where I was responsible for DOD-wide information and influence operations; as the commander of the United States Air Force's Twenty-Fifth Air Force in San Antonio from 2013 to 2015, where I worked to set the conditions for Twenty-Fifth Air Force to become the Air Force's first information warfare numbered air force; as the inaugural director of both the Algorithmic Warfare Cross-Functional Team (Project Maven) and the DOD Joint AI Center (JAIC) in my final two positions before I retired in the summer of 2020; and my post-retirement completion of a third master's degree—a two-year period that was invaluable in allowing me to reflect on topics at the intersection of national security, foreign policy/international studies, US-China relations, and technology. All these experiences have, perhaps paradoxically, both expanded and constrained my understanding of the environment around me.

This chapter begins with a preambulatory section about emerging technologies in general, then lays out a scene-setter, poses a question about the effects of technology on perception and cognition in military operations, seeks to answer my own question, and offers concluding thoughts.

Technological Change and Paths Taken

The arrow of time is unidirectional. The march of technological advancement is, notwithstanding historical examples of temporary reversals, mostly inexorable. To be clear, I am not claiming that new technological developments lead invariably to universal or even prevalent societal benefits. Progress for some is rarely progress for all. Yet the story of humankind contains an omnipresent, invariant theme: the continual search for means—often new technologies—that will lead to better and more fulfilling lives. Almost immediately, and inevitably, there will be attempts to adopt and adapt those same technologies for military purposes. When military technologies are developed first, the opposite occurs: Such technologies subsequently diffuse throughout civil society, almost always in the form of spin-offs.

In broad terms, technological changes throughout history have been incremental, integrative, and cumulative and have diffused relatively slowly across the globe.³ We often refer to technology “inflection points” when, instead, it is far more accurate to describe these periods as “inflection eras” that unfolded over the course of a century or more. And few if any periods of major disruptive technological change throughout history were recognized instantly at the outset as harbingers of the global transformation that followed. Still, I argue that we are now witnessing the early outlines of the third major revolution in our species’ history—a digital revolution.⁴ When viewed in historical terms, the AI era descending upon us has the potential to be as consequential as the agrarian and industrial revolutions. As a general-purpose, dual-use, and dual-nature enabling technology, AI is expected to have sweeping effects across societies, to include national security and economic strength.⁵

The actual path we take on this journey is anything *but* inevitable. History is critically dependent upon the interplay of contingencies, conjunctures, and accidents. It is no different in war and warfare. But seemingly stochastic interactions can never serve as an excuse for failing to take proactive steps to account for the anticipated and potential societal impacts of truly disruptive technologies. We must not view technology as deterministic.⁶ Humans conceive of, design, develop, and modify technology. In principle, there is little difference between the technologies that enhance democratic values and encourage a more participatory democratic process and those that enable dictators and authoritarians. Likewise, few differences exist between technologies

that classify objects to improve the consumer shopping experience and those that detect, classify, and track objects on a battlefield. The same holds true for those that suggest movie recommendations and those that might offer course of action recommendations for military commanders during conflict. And little differs between technologies that enable fully autonomous, self-driving vehicles and those that enable lethal autonomous weapon systems.

The difference is in how people decide to use those technologies—leaders, policymakers, end users, and, at least in democracies, through the consent (or objections) of the governed.⁷ As these technologies spread across societies and militaries,⁸ direct and frequent human intervention is critical to shaping future outcomes. States that act first and comprehensively to adopt AI and similar disruptive technologies are expected to gain major, perhaps even decisive, geoeconomic and geopolitical advantages. Such states could wield considerable influence in shaping the global future—for better or for worse. It is already evident that AI will fundamentally alter the landscape of warfare and impact national security on a grand scale. The national and international ramifications are profound. We still lack a comprehensive understanding, however, of AI-enabled technologies, with scant appreciation or at times outright dismissal of the societal-wide effects those capabilities could generate because of their exponential rates of change and speed of adoption as they diffuse nationally and globally.⁹

In addition to changing the character of warfare, an AI-enabled future will create global winners and losers.¹⁰ It will present tremendous opportunities for societal advancement while also threatening to widen existing technology gaps, already looming large in many regions of the world. It will challenge existing power structures and give rise to new power differentials. Paradoxically, AI will enable unprecedented decentralization of power while also potentially facilitating dangerous strains of authoritarianism.¹¹ AI is already triggering personal disorientation and apprehension. It will almost certainly reshape long-standing social contracts between governing bodies and their constituents.

Since the focus of the current effort is on the Mind-Tech Nexus—and specifically here on perception—I contend that AI and related technologies, as they become more widely integrated into weapon systems, information systems (to include social media), command and control systems, augmented and virtual reality (AR/VR) systems, and eventually the so-called metaverse¹² will also force a thorough reassessment

of the meaning of “reality.”¹³ That reassessment will be as germane to military operations as anywhere else in society.

A Question About the Technology

Is there something so fundamentally different about today’s emerging and disruptive technologies, especially AI, that makes the problem of deleterious effects on human cognition and perception for military forces more serious than we experienced with any past technologies? My answer, qualified somewhat, is yes, for two reasons. First, this effect is due primarily to the temporal dimension associated with today’s new disruptive technologies along with the unique self-learning capability innate in AI models.¹⁴ In basic terms, the unprecedented pace of change, the breadth and depth of diffusion, and the rate of AI adoption have been accelerating. All three characteristics are poised to continue proliferating for the foreseeable future.¹⁵ As we used to say in the flying world, the faster you go, the faster you go faster. It is becoming increasingly difficult to keep mentally oriented. Second, a more sophisticated, even highly personalized way of targeting and shaping human perception and cognition has emerged.¹⁶ Micro-targeted information can be used as a precision weapon, as it were.¹⁷ Given how humans have been shaped by roughly 200,000 years of evolutionary selection pressures, perception is often indistinguishable from—or at least often accepted as—reality. Consequently, we are likely in for a rough ride over the next decade until we sort out how best to deal with the problem through rapid detection, classification, protection, and counteraction.¹⁸ We cannot afford to wait for Darwinian evolutionary processes to solve it for us.

Technology Plus Minds

Thus, one of the biggest challenges we face today is the mating of these twenty-first-century technologies with human minds that have not, in biological terms, changed appreciably since the eighteenth century.¹⁹

First, we should note that this challenge has civil and military implications. We are exposed every day to new technologies that are more capable of amplifying the risks and accelerating the effects of disinformation, disorientation, and cognitive distortion than at any previous point in history. When it comes to the effects of these technologies, there is no convenient dividing line between the military and the rest

of society. Everyone is equally susceptible. The problems are only exacerbated by the dual-use, dual-nature characteristics of AI and related technologies. In theory, humans today are not necessarily more susceptible to misinformation or cognitive disorientation. And arguably, we should be less so after more than a decade of massive exposure to and continual public dialogue about the problem. Yet when combined with our congenital cognitive limitations and AI-enabled precision targeting of human perception and cognition, the three factors noted above—pace of change, breadth and depth of diffusion, and rate of adoption—make the associated dangers higher than at any other time. These factors have clear and troublesome implications for US military personnel in peacetime, crisis, and conflict.

Second, technology development has been outracing our ability to digest and process vast amounts of information via our *real* biological human neural networks, not the deep learning, digitally coded facsimiles based on logistic regression. By extension, this factor has a pernicious effect on our ability to gain rich contextual understanding of national and global challenges or to carefully reason our way through complex problems.²⁰ Since humans are already predisposed to take intellectual shortcuts and seek information that reinforces rather than challenges existing biases, it is becoming far too easy for those with malicious intent to use technology to warp individual and collective perceptions and affect cognitive processing. Since the orientation phase of the OODA loop is the most critical stage of any decision cycle, we need to better understand the dangers inherent in new technologies particularly effective at disrupting the ability to orient mentally to one's surroundings. They threaten to distort our internal representation of the world around us in new and unexpected ways. We are now firmly entrenched in a world in which neither seeing nor hearing is necessarily believing. Things will get worse before they get better. I expect that within a few years, we will look back on the early models of generative AI, such as ChatGPT, as primitive versions of what soon followed.

Third, the interaction of technologies and minds will affect perception in US military operations because, despite AI's seductive allure, the fog and friction of crisis and conflict will not miraculously dissipate. War will forever be characterized by uncertainty, ambiguity, complexity, and chaos.²¹ As James Johnson asks in his excellent article on the limitations of AI in command-and-control decision-making, "Will AI alleviate or exacerbate war's 'fog' and 'friction'?"²² He is not entirely sanguine when answering his own question, arguing that AI "cannot effectively or

reliably complement (let alone replace) the role of humans in understanding and apprehending the strategic environment to make predictions and judgments that inform strategic decisions.”²³

I offer three reasons why the United States must rise to this challenge. First, AI-enabled platforms, sensors, and analytic tools will be critical to future military operations, from peacetime through warfighting and post-conflict recovery, from undersea to outer space, in cyberspace, and everything else in between. Indeed, new technologies such as AI/machine learning (AI/ML) offer enormous potential to help sort through overwhelming amounts of information, find signals in noise, recognize patterns, detect anomalies and warn of threats, enable data fusion from disparate information streams, and draw useful connections or find important correlations across all domains that humans would otherwise miss. They can also accommodate the highly compressed decision cycles we expect in a future high-end conflict.

Another reason is that we already know China’s intent regarding the integration of AI into warfighting operations; it is part of their resolute march toward an integrated mechanized, informatized, and intelligentized force.²⁴ Whether or not China will succeed and to what extent are valid questions. Until we have a more definitive understanding of the rhetoric-reality mismatch, however, we must assume that the People’s Liberation Army (PLA) will continue to make steady progress.²⁵ As underscored by a 2022 *PLA Daily* article by Mao and Tan, “Narrative Contest: The Cognitive Battle in the ‘Post-Truth Era,’” the PLA is focusing more than ever on using new information-centric technologies. These include, but are not limited to, the use of AI/ML in “cognitive warfare” and the “cognitive domain.”²⁶ Similarly, Koichiro Takagi notes that cognitive warfare is one of four key features of China’s intelligentized warfare, along with increased information-processing capabilities, rapid decision-making, and the use of swarms. He discusses China’s use of public opinion warfare, psychological warfare, and legal warfare as three key “battles” in “cognitive warfare.” The PLA expects AI/ML to enhance the effectiveness of all three key battles. (In analyzing Russia’s war on Ukraine and potential lessons the PLA might draw from it, however, Takagi concludes with the important admonition that “cognitive warfare alone cannot win wars.”)²⁷

China’s path contributes to a third reason the United States must rise to the challenge: the accelerated securitization and militarization of AI. This concern arises because relative technological advantage is a critical element of peacetime deterrence and wartime success, which

in the case of emerging AI-enabled capabilities is buttressed by an unhealthy global hype about these technologies' effectiveness and an offense-dominant mindset. Moreover, when deliberating the integration of AI/ML into military operations, the fear of falling behind is causing the United States and China to seek first-mover advantage rather than rely on potential benefits from a fast-follower approach.

Several conditions combine to suggest that the United States military is facing a future characterized by not only great promise but also the potential for great peril. The putative promise of new technologies, uncertainty about their expected performance, and a lack of understanding of how to optimize human-machine teams are contributory factors. Another is an adversary's expected use of information and information-related capabilities to generate destructive self-reinforcing, tightly coupled feedback and feed-forward loops in US military decision cycles.²⁸

One Path We Can Choose

Neither humans nor machines are perfect. I am concerned about the considerable risks of automation bias in the AI-enabled battlespace of the future,²⁹ by which I mean placing excessive or unwarranted confidence in machines,³⁰ especially in time-compressed, high-uncertainty, stressful situations. Yet I am equally wary of human bias,³¹ manifested in the form of disregarding or dismissing the contributions of machines in favor of human "judgment," heuristics, or "gut instinct."³² We should never underestimate the risks and consequences of human fallibility, fear, ego, and hubris on the physical or virtual battlefield.

Both forms of biases are equally highly problematic. For this reason, I am an ardent advocate of optimizing human-machine teaming through human-system integration (HSI). Or more specifically, as described in the Special Competitive Studies Project (SCSP) 2022 report *Mid-Decade Challenges to National Competitiveness*, through the combination of human-machine cognitive collaboration (HMC) and human-machine combat teaming (HMT).³³ HSI or HMC/HMT rely on the fact that humans and machines each have unmistakable comparative advantages.³⁴ The relatively immature stage of AI-enabled military systems makes it difficult to predict whether these comparative advantages will swing in favor of humans or machines or by how much. Military operations will adopt AI advances and even newer types of related technologies, such as quantum and 5G, as they emerge.

Some human advantages—especially critical reasoning—will almost certainly remain immutable. Some machine advantages—for instance, the ability to process massive amounts of information faster than any human—will similarly prevail indefinitely. We should expect the balance sheet of human-versus-machine strengths and limitations to continue to fluctuate, perhaps rapidly and, at some point, even potentially radically, as more sophisticated new capabilities are integrated into military systems and as humans adjust over time to working with increasingly intelligent systems.

In examining the future role of human-machine teaming, scholar Paul Scharre asks, “Are we doomed, then, to choose between the brittleness of automation and human cognitive weaknesses?” He asserts that it is a false choice and that “the best systems will combine human and machine intelligence to create hybrid cognitive architectures that leverage the advantages of both.”³⁵ I go a step further in suggesting that the optimal answer in the future will not be permanent human-machine centaurs but more tailored context- and situation-dependent combinations of human-only, machine-only, and human-machine teams. That is a future not yet fully envisioned.³⁶

Six Considerations

(1) Emphasizing User Interface/User Experience

First is a renewed emphasis on user-centered User Interface/User Experience (UI/UX). *Optimizing the integration of humans and AI-enabled machines, which in turn depends on redesigning the interfaces between humans and machines and recalibrating human and machine roles and responsibilities, will be one of the most important and defining features of future military and intelligence operations in the digital age. The DOD will have to change how systems are designed and developed, how humans are trained to work with “smart” machines that are unlike any previous military systems, and how AI-enabled systems adapt to human interaction and intervention. The future environment will be characterized by AI-enabled systems whose maximum benefits can only be achieved through superior human-system integration.*

There is no comprehensive or universal understanding of exactly what this integration means. At least not yet. As a starting point, the Department of Defense will have to change how systems are designed

and developed, how humans are trained to work with “smart” machines that are unlike any previous military systems, and how AI-enabled systems adapt to human interaction and intervention.³⁷ The concept of world-class UI/UX, or human-centered design, is at the heart of every successful modern commercial software product. Far too often, however, user-focused, intuitive UI/UX has been given short shrift during the development of US military systems. This is not a trivial problem, especially for militaries beginning to shift from the industrial to the digital age, seeking to adapt to a rapidly evolving world of “software-defined warfare.”³⁸ Moreover, the failure to prioritize UI/UX in legacy military hardware and software, which in the past might have been considered an annoyance rather than a systemic shortcoming, will spiral into a debilitating condition in a future environment characterized by AI-enabled systems whose maximum benefits can only be achieved through dedication to the design of superior human-system integration (HMC/HMT).³⁹

(2) Training Smart Machines

Second, in an AI-enabled digital future, military users will have to train smart machines in such a way that systems adapt to an individual’s preferences, the pace of their cognitive development, and even their past behaviors.⁴⁰ *“Mass customization” is, on the surface, an oxymoron. Yet as technology continues to advance rapidly, the concept of highly tailored human-machine interaction and interdependence is an achievable goal.⁴¹ It demands an entirely new approach to training, however, one that will rely on more—and different kinds of—experimentation, simulations, exercises, and wargaming before AI-enabled systems are fielded operationally.*

These efforts will be vital in gaining a better understanding of human-machine team composition, the optimal assignment of human and machine roles and responsibilities, and an effective and efficient workflow integration. In addition, they should incorporate continuous assessments of human-machine team performance. Realistic experiments, exercises, and wargames will be instrumental in the development of new operating concepts, which at least for the foreseeable future will involve ways to bridge so-called legacy systems and new systems that integrate emerging technologies. At the same time, military developers and service system program offices should more thoroughly embrace the concept of fielding minimum viable products (MVP) to ensure end-user feedback is obtained as early

and as often as possible in the fielding and sustainment process for AI-enabled systems.⁴²

(3) Including “Red Teaming” Element

Third, if the real value of a smart assistant is to present information or options to users in ways that account for and counteract the human operator’s biases and innate cognitive limitations, the system must be trained to ensure it also always includes an element of “red teaming.”

In other words, the smart assistant would provide the human operator information and recommendations that reflect elements of devil’s advocacy; the user would not derive these on their own due to existing biases or blinders or limitations in their contextual understanding. Likewise, during training, experiments, exercises, and wargames, overall human-system team performance can be optimized through a continuous process of human feedback to the system as it returns its results.⁴³ Again, this process is similar to how most of us today “train” the applications we use in our personal lives to account for our individual preferences. Sean Guillory and John Carrola refer to the concept of “Cognitive Mission Support,” which they define as systems designed to help humans deal more effectively with the inevitability of information and cognitive overload.⁴⁴

(4) Accepting Data “As Is”

Fourth, human biases and other cognitive limitations require military end users to account for the possibility that future smart machines will frequently offer information and recommendations that should be accepted “as is,” resisting the temptation to dismiss machine-generated results out of hand.⁴⁵ Doing so is a very tall order unless humans and AI-enabled capabilities have established a long-term “partnership” through education, training, and use under operational conditions such that the operator has learned to have sufficiently high confidence in the system’s results.⁴⁶

(5) Engendering Unintended Strategic Consequences

Fifth, even organizational dynamics will be affected, from the tactical to the strategic level.⁴⁷ As James Johnson notes, “absent fundamental changes to our understanding of the impact (cognitive effects, organizational, and technical) of AI on the human-machine relation-

ship, we risk not only failing to harness AI's transformative potential but, more dangerously, misaligning AI capabilities with human values, ethics, and norms of warfare that spark unintended strategic consequences."⁴⁸ I could not agree more.

(6) Understanding Risks to AI-Enabled Military Systems

Sixth, the kind of digital future I describe above includes a variety of substantial risks that must be accounted for. At the more basic level, these include adversarial attacks, which can range from cyberattack against networks to deception, data poisoning, and brute force attacks against fielded models. All are designed to limit the performance of an AI-enabled system and to induce destructive feedback/feed-forward closed loops within the observation stage of the OODA loop.

Given the paucity of fielded AI-enabled military systems, other risks are not yet well understood. For instance, there is the likelihood that an individual's "smart machine assistant," if trained in the way described above, will use algorithms to prioritize how it displays results or even course of action recommendations to a commander, operator, or analyst. This is, in fact, exactly how we expect typical AI-enabled systems to perform today, as, for example, social media platforms present information tailored to individual users. In military operations, however, this reward-optimization function could well introduce significant cognitive risks. It could reinforce instead of neutralize individual human biases and blind spots or fail to present seemingly minor pieces of information about an adversary's plans or actions that if revealed could be critical to mission outcomes.⁴⁹ Apart from the self-learning nature of AI systems—which involves risks that still remain poorly understood since all AI-enabled systems fielded today are based on very narrow AI—another potentially dangerous risk needs to be addressed: the cumulative risks of connecting many different AI-enabled technologies in system-of-systems network architectures.

In short, the future of human-system integration and HMC/HMT calls for an updated systems theory-based approach to risk comprehension, risk acceptance, and risk management.

Conclusion

War has always been viewed as some mystical combination of art and science that is exceedingly challenging to manage. The horizontal

and vertical scale of conflict and speed with which events take place and change continuously, often chaotically, can make it seem nearly impossible to master either the art *or* the science. In the future, we should anticipate that warfighting, especially between peer adversaries, will only become more complex and chaotic, characterized by an even higher operating tempo.

The art side of the art-science equation remains as essential as ever. However, with the proliferation of new technologies and a shift to a data-centric environment, the science part of the equation is becoming increasingly consequential. In future crises and conflicts, the side that adapts faster and demonstrates the greatest agility—to include rapidly updating fielded software and AI models—may well gain a significant tactical and operational advantage. As stated in the SCSP report, “a military’s ability to deploy, employ, and update software, including AI models, faster than its adversaries is likely to become one of the greatest determining factors in relative military strength.”⁵⁰

One of the worst alternative futures is one in which the US military continues to “bolt on” AI capabilities to its platforms, sensors, and workplace tools versus “baking in” such capabilities during the design and development process for all new systems. Moreover, absent a reconceptualization and redesign of UI/UX for military systems and renewed emphasis on systems theory-oriented HSI/HMC/HMT, the combination of “Frankenstein systems” and poor design principles will have serious outcomes. An adversary can more easily distort the orientation stage of the decision cycle, and there is a much higher probability of *self-induced* destructive, closed feedback/feed-forward perception and cognition loops. In other words, these effects would achieve the adversary’s desired effects without any intervention on its part!

The US military’s AI-enabled future offers more promise than peril. That view, however, should be infused with a considerable dose of caution. Apart from the modernization steps mentioned above, along with career-long education and training for all personnel on emerging technologies and their role in military operations, the military should dedicate even more time to the study of the human condition, war and warfare, and culture. Even in a future dominated by AI-enabled capabilities and autonomous systems, war remains the ultimate human endeavor.⁵¹ While I do not expect that AI will change the nature of war—if *nature* is defined as the reasons some humans decide to fight other humans, which always come down to varying combinations of fear, honor, interest, and culture—it will,

when combined with other capabilities such as quantum, 5G, smart manufacturing, and other technologies not yet imagined, unquestionably change the character of warfare.

As someone who spent a long career in uniform, experienced firsthand the strengths, limitations, promises, and pitfalls of new technologies, and continues to study the science and art of conflict, I remain a guarded optimist. I am hardly a technology Pollyanna, but even accounting for the validity of the precautionary principle, I find that AI doomsaying is now as prevalent as AI hype, especially in the United States.⁵² The reality lies somewhere in the middle. My optimism is balanced by a degree of pessimism that derives as much as or more from our own considerable cognitive shortcomings as humans as it does from the undeniable limitations and risks of new technologies. Success in the military's digital future will demand attention to all the factors noted above along with a commensurate emphasis on responsible AI (RAI) and AI assurance.⁵³ Human agency will always matter, indeed, perhaps even more so in the age of AI-enabled machines. During future military operations, the key to success will depend on humans finding and sustaining the right balance between humans, machines, and a new kind of human-machine centaur.

Notes

1. This chapter is adapted from my remarks at the August 10, 2022, Strategic Multilayer Assessment (SMA) Mind-Tech Nexus Speaker Session with Dr. David Kilcullen and Dr. Nicholas Wright, <https://nsiteam.com/>.

2. The OODA loop is almost universally oversimplified, frequently associated with its tactical fighter aviation origin. It is typically depicted as a basic circle with four head-to-tail connected arrows depicting each of the four stages: Observe, Orient, Decide, Act. For a much more robust treatment of the OODA loop as originally envisioned by John Boyd, especially the critical roles of both positive and negative effects of feed-forward and feedback loops throughout all the stages of the decision cycle, see Spinney beginning at 1:21:30. Chuck Spinney, "Evolutionary Epistemology: A Personal View of John Boyd's 'Destruction and Creation' . . . and Its Centrality to the . . . OODA Loop," *52 Living Ideas*, YouTube (2:32:24), February 21, 2021, <https://www.youtube.com/>.

3. History shows that no single technology is by itself ever truly transformative. Rather, what matters most is how a technology is integrated across society and matched with legacy and innovative technologies and new employment concepts to drive local, national, and even global disruption.

4. I deliberately eschew the term "fourth industrial revolution" in favor of "digital revolution," which is designed to represent the third such major global transformation for humans after the agrarian and industrial revolutions. Many writers separate the industrial revolution into four different phases, typically parsed as follows: the age of steam (first industrial revolution), the age of electricity (the second), and the age of

information (the third). Using this taxonomy, AI and related emerging technologies are now fueling the fourth industrial revolution. In the interests of parsimony, I do not find this more detailed categorization to be particularly illuminating for the purposes of this chapter. I contend that the digital era represents a marked difference from the industrial age. While I do not offer a precise definition of digital revolution here—largely because I suggest the form it will take is still unknowable and unpredictable—it will manifest itself as a merger of humans, machines, and data in ways that go even deeper than human-machine symbiosis.

5. In general, “dual use” implies that the AI technology can be used to equal effect in commercial and military applications. Audrey Kurth Cronin advocates for the term “multi-use” rather than dual-use technologies because of the much broader range of people involved today in innovation. I use “dual nature” to indicate that AI technologies are, in isolation, neither inherently stabilizing nor destabilizing. It also connotes the limited ability to differentiate between the use of AI for offensive or defensive purposes once embedded into a military weapon system. Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists* (Oxford University Press, 2020), 13.

6. There is not widespread agreement on the meaning of technological determinism. For this chapter, I use the term explicitly to refer to the common practice by commercial companies over the past twenty years of fielding new disruptive technologies without a comprehensive understanding or appreciation of the impact those technologies would have on society (along with pronouncements made with a level of confidence, often bordering on hubris, that such technologies would dramatically improve society, with little to no downside). Such practices are accompanied by the persistent failure of political and policy leaders to implement laws, regulations, or policies or recommend best practices in ways that reflected a basic understanding of any given technology's benefits, risks, strengths, and limitations (what can be described as a mostly “hands-off” approach to technology policy). For an explication of technological determinism, see Allan Dafoe, “On Technological Determinism: A Typology, Scope Conditions, and a Mechanism,” *Science, Technology, & Human Values* 40, no. 6 (November 2015): 1047–76, <https://www.jstor.org/stable/43671266>.

7. I realize this invites unflattering comparisons to the facile slogan “Guns don't keep people, people kill people.” Yet clichés aside, in both cases the societal-wide impact of a technology depends to a large degree on how policies governing the use of those capabilities are implemented and how the citizenry views them.

8. Cronin notes that “sometimes technology causes social change first, and then affects military-technical innovation; sometimes the process works the other way around” (*Power to the People*, 33). Dafoe emphasizes the role of military-economic competition in governing the rate, breadth, and depth of technology diffusion (“On Technological Determinism,” 1047–76).

9. It is becoming increasingly difficult to comprehend the rate of change occurring in the AI field. In a Darwinian sense, humans are genetically programmed to be linear thinkers. It is hard to fathom the implications and ramifications of exponential rates of change. What separates AI from any other technology in history is that such exponential rates of change, when combined with systems that are beginning to learn on their own (that is, without being explicitly programmed to do so) and learning how to maximize reward functions in unexpected ways, could eventually alter society and conflict in ways we cannot yet begin to divine.

10. As noted by one of the participants during the SMA virtual session discussion period, the digital revolution is still mostly a “first-world” phenomenon. Some of the most noteworthy advancements generated by AI/ML-enabled technologies have not

diffused to many parts of the world, especially to areas lacking anything beyond a rudimentary digital infrastructure. Shanahan, SMA Mind-Tech Nexus Speaker Session.

11. See for example, Henry Farrell et al., “Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous,” *Foreign Policy*, September/October 2022, <https://www.foreignaffairs.com/>. They state, “The most urgent question is not whether the United States or China will win or lose in the race for AI dominance. It is how AI will change the different feedback loops that democracies and autocracies rely on to govern their societies” (Farrell et al., 9).

12. Rand Waltzman paints a somewhat grim picture of what is yet to come without even referring explicitly to new generative AI models such as ChatGPT: “At the heart of all deception is emotional manipulation. Virtual reality environments, such as Facebook’s (now Meta’s) metaverse, will enable psychological and emotional manipulation of its users at a level unimaginable in today’s media.” Waltzman, “Facebook Misinformation Is Bad Enough. The Metaverse Will Be Worse,” *Washington Post*, August 22, 2022, 1, <https://wapo.st/48cR8Oo>.

13. Sean A. Guillory and John T. Carrola expand this list further, using the term “Online-Offline (O-O) Convergence” to describe a future characterized by the widespread use of “Metaverse/Web3, synthetic training environments, Integrated Visual Augmentation Systems, digital twins, brain-machine interfaces and other biodigital convergences.” They adopted the term *O-O Convergence* to “describe when a person can’t differentiate between the information environment dimensions and sees it as one ‘reality.’” Guillory and Carrola, “What Online-Offline (O-O) Convergence Means for the Future of Conflict,” Information Professionals Association, July 25, 2022, 3, <https://information-professionals.org/>.

14. This aspect of AI differentiates it from any previous technology in history: Its “knowledge” is not programmed by humans. Instead, it is learned from data. AI systems “learn” by consuming data and drawing observations and conclusions based on the data versus acting in accordance with explicit preprogrammed rules.

15. See, for example, Azeem Azhar, *The Exponential Age: How Accelerating Technology Is Transforming Business, Politics, and Society* (Diversions Books, 2021).

16. David Pappalardo defines *cognitive warfare* as “a multidisciplinary approach combining social sciences and new technologies to directly alter the mechanisms of understanding and decision-making in order to destabilize or paralyze an adversary.” This view is similar to Boyd’s emphasis on using the feedback and feed-forward loops of the OODA loop to disorient an adversary and paralyze their decision-making ability. David Pappalardo, “‘Win the War Before the War?’: A French Perspective on Cognitive Warfare,” *War on the Rocks*, August 1, 2022, 2, <https://warontherocks.com/>.

17. Realistic video and audio deepfakes are already prevalent today and will only increase in sophistication over the next few years with generative AI models of ever-expanding multimodal capabilities. See, for example, Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide* (Carnegie Endowment for International Peace, 2024), <https://carnegieendowment.org/>; and Benjamin Wofford, “Meet the Lobbyist Next Door,” *Wired*, July 14, 2022, <https://www.wired.com/>. As Jack Clark of Anthropic notes, “All these generative models point to the same big thing that’s about to alter culture; everyone’s going to be able to generate their own custom and subjective aesthetic realities across text, video, music (and all three). . . . Society is moving from having a centralized sense of itself to instead highly individualized choose-your-own adventure islands, all facilitated by AI. The implications of this are vast and unknowable.” Clark, “Import AI 304: Reality Collapses Thanks to Facebook; Open Source Speech Rec; AI Culture Wars,” *Import AI*, October 3, 2022, 1, <https://jack-clark.net/>.

18. Nicholas (Nick) Wright uses slightly different terminology to describe the same process: detect and characterize, defend, and democratic compatibility. “A Conversation with Nicholas Wright on Cognitive Defense, the Joint Force in a Digitizing World,” *Clear and Present Podcast*, episode 1, transcript, Institute for Biodefense Research, April 22, 2022, <https://biodefenseresearch.org/>.

19. I chose the eighteenth century since it is generally accepted as the height of the Age of Reason or the Enlightenment (admittedly a term that derives from an overly Western-centric orientation). It was sparked, to a considerable degree, by one of the most important emerging technologies in human history (the printing press) along with the steady increase in global exchanges. Globalization is hardly a new phenomenon despite frequent claims to the contrary; the primary difference has been in the speed and scope of exchange, from the speed of humans walking to the transmission of digits at the speed of light.

20. In his piece on the threats posed by AI to human reasoning, Henry Kissinger described the effects of overreliance on the internet: “[They] emphasize retrieving and manipulating information over contextualizing or conceptualizing its meaning. . . . Information threatens to overwhelm wisdom.” Kissinger, “How the Enlightenment Ends,” *The Atlantic*, June 2018, 3–4, <https://www.indexinvestor.com/>.

21. The central point of Boyd’s OODA loop, one that is often neglected or misunderstood due to oversimplification, is that full awareness of the potential effects of positive and negative feedback and feed-forward closed loops would provide options for a military force to generate disorientation, disorder, chaos, and mental paralysis in adversary forces while simultaneously protecting friendly forces from those same debilitating effects. For an excellent, detailed examination of the OODA loop as it pertains to AI-enabled command and control, see James Johnson, “Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age,” *Defence Studies* 23, no. 1 (July 22, 2022): 43–67, <https://doi.org/10.1080/14702436.2022.2102486>.

22. Johnson, 45.

23. Johnson, 43.

24. While most writers refer to China’s ongoing shift as moving from an informatized to an intelligentized force, Tai Ming Cheung suggests instead that China’s military modernization objectives include “accelerating the *integration* of mechanization, informatization, and intelligentization” [emphasis added]. Cheung, *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Cornell University Press, 2022), 308.

25. See also, for example, Cheung; Ryan Fedasiuk and Emily Weinstein, “AI in the Chinese Military,” in *Chinese Power and Artificial Intelligence*, ed. William C. Hannas and Huey-Meei Chang (Routledge, 2023), 175–88; and Jinghan Zeng, *Artificial Intelligence with Chinese Characteristics: National Strategy, Security and Authoritarian Governance* (Palgrave Macmillan, 2022).

26. W. Mao and D. Tan, “Narrative Contest: The Cognitive Battle in the ‘Post-Truth Era,’” *PLA Daily*, July 5, 2022. See also L. Yang, who states, “Cognitive warfare should exploit information from all domains. In doing so, cognitive operations can be used to amplify the effects of political disintegration, economic sanctions, diplomatic offensives, and military operations in order to ‘exert full-dimensional pressure on target audiences and achieve the goal of defeating the enemy without fighting.’” L. Yang, “Aiming at the Future Battle and Fighting the Cognitive ‘Five Battles,’” *PLA Daily*, August 23, 2022, 3.

27. Koichiro Takagi, “The Future of China’s Cognitive Warfare: Lessons from the War in Ukraine,” *War on the Rocks*, July 22, 2022, 2–4, <https://warontherocks.com/>.

28. In referring to cognitive warfare, Zac Rogers states that “the adversary, in the age of hyper-connectivity, need only show up, inject, nudge, exploit, and disappear.” Rogers, “In the Cognitive War – the Weapon Is You!,” *Mad Scientist Laboratory* (blog), July 1, 2019, <https://madsicblog.tradoc.army.mil/>.

29. Automation bias, or the well-documented human propensity to favor outputs from machines over humans, is one of the more salient dangers of an AI-enabled future. Zac Rogers provides detailed critiques of overreliance on technology, especially AI-enabled capabilities, at the expense of human cognition. See Rogers, “In the Cognitive War”; Zac Rogers, “Goodhart’s Law: Why the Future of Conflict Will Not Be Data-Driven,” *Grounded Curiosity* (blog), February 14, 2021, <https://groundedcuriosity.com/>; and Zac Rogers, “Assessing the Cognitive Threat Posed by Technology Discourses Intended to Address Grey Zone Activities,” *Divergent Options*, January 17, 2022, <https://divergentoptions.org/>.

30. Analyses of the US military’s performance from the American Revolution to today are replete with detailed critiques of what is perceived to be an overreliance on technological solutions to human problems. Such critiques typically also fault excessively optimistic views of technology by military and industry leaders. While in general I sympathize with such critiques, at times the criticisms have been overstated. I am confident that US military personnel will adapt quite well to an AI-enabled future as long as they play a role in shaping that future.

31. I mostly agree with James Johnson’s critique of AI’s likely limitations in command-and-control decision-making, but I contend that humans are even more fallible than he suggests, especially in the crucible of combat. Johnson, “Automating the OODA Loop.”

32. In his 2021 congressional testimony, Herb Lin states that people generally do not process information rationally, thoughtfully, or deliberately, the result of three factors in particular: cognitive economy, dual-system cognition, and social identity. Herb Lin, *Hearing on Technology and Information Warfare: The Competition for Influence and the Department of Defense Before the House Armed Services Subcommittee on Cyber, Innovative Technology, and Information Systems*, 117th Cong., 2021, 3–5, <https://docs.house.gov/>.

33. I serve as an advisor to the SCSP Defense Panel. The SCSP report argues that HMC, focused primarily on cognitive tasks, “will be critical to optimizing decision making,” while HMT “will be essential for more effective execution of complex tasks, especially higher-risk missions, or in confronting an adversary with sophisticated autonomous systems.” Special Competitive Studies Project (SCSP), *Mid-Decades Challenges to National Competitiveness*, September 2022, 136–37, <https://www.scsp.ai/>.

34. The 2022 SCSP report states that “humans outperform machines on many sensory tasks, certain types of communications, high-context tasks requiring intuition [though as I argue elsewhere in this chapter, we often give too much credit to human intuition], and various types of creative exploration.” Machines, on the other hand, “often outperform humans at tasks that require processing extremely large volumes of data, a high degree of precision, memory, and constant repetition.” SCSP, 137.

35. Paul Scharre, “Centaur Warfighting: The False Choice of Humans vs. Automation,” *Temple International and Comparative Law Journal* 30, no. 1 (2016): 152, <https://sites.temple.edu/>.

36. Gilman Louie, a renowned technologist and cofounder of In-Q-Tel who was one of the commissioners on the US National Security Commission on Artificial Intelligence (NSCAI), characterized the risks inherent in suboptimal human-machine teams:

Human-machine teaming can often lead to inferior decision making [compared to] using either a pure human or pure machine approach. For

example, if a human can't keep up with the machine, the human could slow the process down . . . enough to take the team outside of the response window. On the other hand, a computer algorithm could fight against human input to create a dangerous oscillation where neither machine nor human is in full control. . . . While I support human machine teaming, I believe (but can't prove) that it is *important to understand when and under what condition the human or the machine should have principal decision making. Get that wrong, and the system will fail* [emphasis added].

He pointed to the Boeing 737 MAX accidents as an example of what happens when insufficient attention is given to human-system integration. “The National Security Commission on Artificial Intelligence Final Report (version 1 draft),” December 7, 2020, author's notes.

37. As described in “International Competition over Artificial Intelligence,” “Figuring out how (and whether) to incorporate AI into such high-stakes [military] settings will need to draw on decades of existing wisdom from fields such as human-machine interaction, safety-critical engineering, and software assurance to determine how to allocate responsibilities, train operators and design interfaces. These considerations do not generally carry the same glamour as demonstrating new AI capabilities and therefore tend to be neglected, especially in public discussion. *But they will be crucial in determining which actors can benefit most from AI progress*” (emphasis added). “International Competition over Artificial Intelligence,” *Strategic Comments* 28, no. 3 (June 2022): viii, <https://doi.org/10.1080/13567888.2022.2091878>. See also Patricia McDermott et al., *Human-Machine Team Systems Engineering Guide* (MITRE, December 13, 2018), <https://www.mitre.org/>.

38. For example, see Nand Mulchandani and John N. T. “Jack” Shanahan, *Software-Defined Warfare: Architecting the DOD's Transition to the Digital Age* (Center for Strategic and International Studies, September 2022), <https://csis-website-prod.s3.amazonaws.com/>.

39. This emphasis should include human readiness levels (HRL). See, for example, the Human Factors and Ergonomics Society, which notes that “many system development programs have been deficient in applying established and scientifically-based human systems integration (HSI) processes, tools, guidance, and standards, resulting in suboptimal systems that degrade mission performance.” “Human Readiness Scale in the System Development Process,” Human Factors and Ergonomics Society (draft), 2021, 1, <https://www.hfes.org/>. The consideration of HRL, while always important, becomes critical for AI-enabled systems that depend on substantial human interaction (as opposed to those that primarily merely report results for human consideration). Substantial human intervention has compensated for poor HRLs in earlier and current fielded military systems. In future AI-enabled systems, HSI must accord equal consideration to HRL and technology readiness level (TRL). Otherwise, we can expect suboptimal results from humans and machines.

40. In an insightful paper on the importance of “teaming intelligence” (human-machine interdependence) in an AI-enabled world, Matt Johnson and Alonso Vera make the case that “no AI is an island” and that “the growth of sophistication in machine capabilities must go hand in hand with the growth of sophistication in human-machine interaction capabilities.” Moreover, they make the critical point that “more intelligent capabilities inevitably require correlated teaming capability enhancements.” Matt Johnson and Alonso Vera, “No AI Is an Island: The Case for Teaming Intelligence,” *AI Magazine* 40, no. 1 (Spring 2019): 17–28, <https://doi.org/10.1609/aimag.v40i1.2842>.

41. I thank Nand Mulchandani, the JAIC's former chief technology officer (CTO) and current CIA CTO, for this insight.

42. We took this approach in both Project Maven and at the JAIC. During our first deliveries of AI-enabled capabilities to units deployed in combat, one of our most important early lessons learned in Project Maven was that it was counterproductive to field new capabilities midway through a unit's deployment. Instead, intelligence analysts needed to become familiar with the MVP capabilities during their pre-deployment training cycle.

43. Similar to my earlier MVP point, the first two years of Project Maven consisted of soliciting user feedback on UI/UX, including how individuals wanted to see AI/ML results displayed.

44. Guillory and Carrola, "What Online-Offline (O-O) Convergence Means." In an enlightening article on the risks of autonomous vehicles, Liza Dixon makes an important point along similar lines, arguing that "automated systems must not only be functional, reliable, and trustworthy; *they must be mindfully introduced to the humans they support*" [emphasis added]. She uses the term "autonowashing" to refer to the gap between how automation capabilities are described to users and a system's actual technical capabilities. Liza Dixon, "Autonowashing: The Greenwashing of Vehicle Automation," *Transportation Research Interdisciplinary Perspectives* 5 (May 8, 2020), 2, <https://www.sciencedirect.com/>.

45. One illustrative example happened in the famous Go match between AlphaGo and the human Go grand master Lee Sedol. As Gilman Louie describes it,

AlphaGo, on its 37th move in the second game, played a move that every Go expert felt was a mistake (even the programmers thought it was a mistake). In fact, no knowledgeable human Go player would have ever made that move. This 37th move redefined our understanding of AI by devastating the grand master. If human-machine teaming were allowed, that 37th move would never have been made. Again, in game 4, the grand master made a move that no machine would ever expect to make leading to the grand master's only victory (he lost 4-1 to AlphaGo) of that historical tournament. It is ironic that it was this match that many consider China's Sputnik moment. Kasparov has been a strong advocate of human-machine teaming, but I am not sure if this will always be true, even in a game like chess (see Stockfish vs. AlphaZero).

"The National Security Commission on Artificial Intelligence Final Report (version 1 draft)," December 7, 2020, author's notes.

46. Rather than referring to a human-machine relationship established upon "trust," which until recently has been the preferred term, the AI community is increasingly using the terms *justified confidence* and *AI assurance*. As described in the NSCAI 2021 final report, "having justified confidence in AI systems requires assurances that they will perform as intended when interacting with humans and other systems." AI assurance comprises RAI and comprehensive AI test, evaluation, verification, and validation. *National Security Commission on Artificial Intelligence Final Report* (National Security Commission on Artificial Intelligence, March 2021), 137, <https://www.nsc.ai.gov/>. See also David M. Tate, *Trust, Trustworthiness, and Assurance of AI and Autonomy* (Institute for Defense Analyses, April 2021), <https://apps.dtic.mil/sti/pdfs/AD1150274.pdf>; and Feras A. Batarseh et al., "A Survey on Artificial Intelligence Assurance," *Journal of Big Data* 8, no. 60 (2021), <https://doi.org/10.1186/s40537-021-00445-7>.

47. In a pathfinder paper examining the potential impact of disruptive technologies on society, Mats Lewan investigates the future of the nation-state in the context of change induced by the internet and digitalization. Lewan, "The Future of the Nation-State: How the Nation-State Can Find a Way Through Digitalization," in *Digital*

Transformation and Public Services: Societal Impacts in Sweden and Beyond, ed. Anthony Larsson and Robin Teigland (Routledge [Taylor and Francis Group], 2020), 293–317. His analysis of societal structure in an AI-enabled future is equally applicable to understanding how future military organizational design must adapt to thrive in a digital future. The magnitude of the changes that will take place over the next few decades will demand an “adapt or die” evolutionary mindset. James Johnson cautions about the dangers of the likely future organizational collision of the “strategic corporal” and “tactical general” in the AI-enabled battlespace. Johnson, “Automating the OODA Loop.”

48. Johnson, 17.

49. See, for example, James Davitch for an analysis of the effects of cognitive biases on military strategists’ decision-making processes (confirmation bias, fundamental attribution error, anchoring bias, and representative bias). Davitch, “Do Not Trust Your Gut: How to Improve Strategists’ Decision Making,” *Strategy Bridge*, August 31, 2022, <https://thestategybridge.org/>.

50. *Mid-Decades Challenges to National Competitiveness* (Special Competitive Studies Project, September 2022), 139, <https://www.scscsp.ai/>.

51. For this reason, while I agree with the urgent calls to graduate more STEM majors in the US to meet the exploding needs of the digital revolution, we need more tech-savvy liberal arts graduates as well. Technical degrees in the US should include the requirement for social science courses that address the challenges of managing the societal effects of disruptive technologies; at the same time, undergraduate liberal arts degree programs should introduce the basic technical aspects of AI and associated new technologies.

52. I agree with Richard Danzig’s warning in his 2018 monograph, *Technology Roulette*, on the risks of a race toward technological supremacy. He offers a compelling caution that “experience with nuclear weapons, aviation, and digital information systems should inform discussion about current efforts to control artificial intelligence (AI), synthetic biology, and autonomous systems. In this light, the most reasonable expectation is that the introduction of complex, opaque, novel, and interactive technologies will produce accidents, emergent effects, and sabotage. In sum, on a number of occasions and in a number of ways, the American national security establishment will lose control of what it creates,” and “twenty-first technologies are global not just in their distribution, but also in their consequences.” Danzig, *Technology Roulette: Managing Loss of Control as Many Militaries Pursue Technological Superiority* (Center for a New American Security, June 2018), 2, <https://www.cnas.org/>.

53. The US Department of Defense defines *RAI* as “a dynamic approach to the design, development, deployment, and use of AI capabilities that implements DoD AI Ethical Principles to advance the trustworthiness of AI capabilities.” United States Department of Defense, *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway* (DOD, June 2022), 6, <https://media.defense.gov/>. I assert that there is a healthy and entirely manageable tension between the safe, lawful, and ethical use of AI in the US military and the imperative to build AI-enabled systems under operationally relevant timelines.

Part 3

PERFORMANCE ENHANCEMENT

Chapter 8

Enhancing the Humans in the Mind-Tech Nexus

*Nicholas Wright, Georgetown University, University College
London, Center for Strategic and International Studies*

Abstract

How can advances in the Mind-Tech Nexus—such as from generative artificial intelligence (GenAI), brain-computer interfaces, drugs, genetics, and physiological monitoring—enhance warfighter performance? The Mind-Tech Nexus arises from how human factors and technology interface and converge. This chapter first explores the ways that Mind-Tech advances affect how humans interface with technology to enhance performance: through nonverbal, verbal, and direct brain-computer interfaces. Secondly, we explore how mind and tech converge in the process of innovation to enhance performance, and we examine two particular examples: humanoid robots and weightless AI cyber agents. Third, we ask how humans themselves can be changed through physical enhancement (e.g., an “exo-suit”), mental enhancement (e.g., tactical or expert AI advisors), and by directly altering the body (e.g., drugs or genetics). For this third area in particular the ethical judgments will be paramount and must be based on who we are as free, democratic and ethical societies—as well as an understanding of what can be done because not all societies across the globe will maintain our ethical standards.

Introduction

This chapter asks how advances in the Mind-Tech Nexus can enhance warfighter performance. The Mind-Tech Nexus raises a bewildering profusion of applications and implications—which this chapter breaks down into three more manageable bites. As shown in figure 8.1, I explore three aspects of the Mind-Tech Nexus:

- (1) How humans and technology *interface*. By interfaces, here we mean where separate systems—such as a human and a machine—interact with each other but don’t meaningfully change how the other is constituted. For example, a human driver switches on a

car's indicator lights, or the car's fuel gauge transmits information to the human. Interfaces can be nonverbal, verbal, or even direct with the brain.

- (2) How humans and technology *converge*. When separate systems interact, they can do more than just interface. They can also change each other cumulatively over time so that they better complement each other and *converge* toward becoming a more unified entity. Humans shape technologies, and technologies shape humans. Fundamental changes in the systems happen at many timescales. Across evolution, for example, the human brain itself has codeveloped with our tool use so that we became ever smarter in our use of tools and ever more dependent on using them. Innovation to develop effective new weapons, such as tanks in World War Two, often involves an iterative process. New ways of humans working codevelop with new versions of the technology to achieve more than could have been designed on a blank sheet of paper.
- (3) How *humans* are affected by the Mind-Tech Nexus. How can they be enhanced in terms of their bodies and brains?

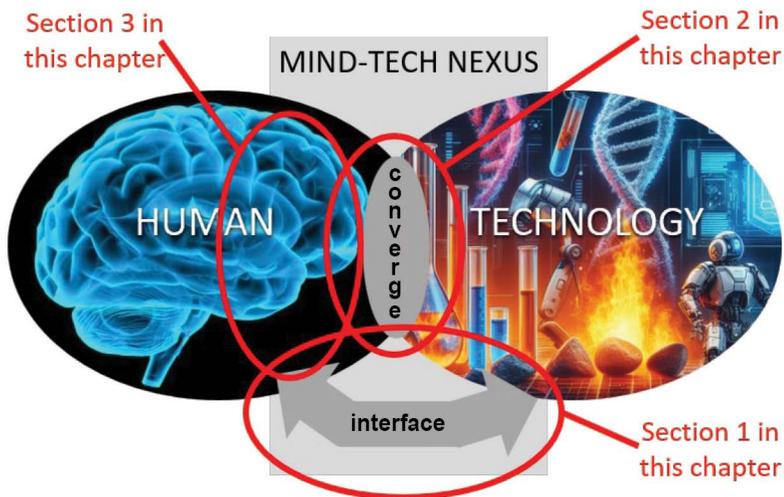


Figure 8.1. The Mind-Tech Nexus overview. The Mind-Tech Nexus is defined as how human factors and technology will interface and converge to shape the character and outcomes of competition. This chapter looks at enhancing (1) how they interface, (2) how they converge, and (3) the effects on humans.

I deliberately avoid looking at technology separately because of the bias toward focusing on technology in many Western discussions about the future or war. Technology is discussed throughout as it matters alongside humans. Moreover, borderline cases inevitably blur distinctions between any categories we might use. But in this field with its blizzard of advances, exploring these three aspects of the Mind-Tech Nexus will enable us to capture enough of what matters, for us to see where we are going.

(1) Interface

Humans and their technologies *interface*, which is where these separate systems interact. A human might turn a steering wheel or read a computer screen. Or a human pilot might flip the switch in an aircraft cockpit, as often happened in the B-17 Flying Fortress that was a workhorse US bomber during World War II.¹ Sadly, many B-17s were lost just as they were landing back at base—and during the war, these losses were attributed to many alternative explanations, such as pilot error, poor maintenance, or runway quality. But research after the war found the real reason: On the B-17 cockpit instrument panel, the switch that engaged the landing gear was next to the switch that operated the flaps. Many brave crews died because of a terribly dangerous interface.

But good interfaces have made trillions of dollars in the business world—like Microsoft Windows in the 1980s or the iPhone in the 2000s—and head-up displays (HUD) have given pilots a lethal edge since developed by the British in World War Two. We need to try to get interfaces right.

In this section, we describe a spectrum of entities that humans work with (i.e., tools, animals, AI-enabled entities, or human colleagues) and how humans can interface (i.e., nonverbally, with language, and via brain-computer) with these entities to work together.

(1.1) Human Interfaces Along the Spectrum: Hammers, Horses, and Humans

Workplaces across industry, defense, or the intelligence community will increasingly require collaboration with machines. Many children are already using GenAI, such as ChatGPT, to “help” with homework. Human-machine teams are not options that we are choosing to have

or not have. The question is not to use or not use them but how effectively we will use them. AI will sometimes replace humans and will often change the character of work.²

We humans work with a spectrum of aids, which can be distinguished by their capacity to process information. At one end of the spectrum are inert tools like hammers. At the other end are fellow humans, such as colleagues or a partner in doubles tennis. In between are entities like a horse or domesticated dog (e.g., to herd sheep, guide the blind, or pull a sled). Now, AI can enhance tools that lie in the middle of that spectrum, such as the widely used AI assistants that help computer programmers write code or students research and write essays. Newer AI-enabled tools will keep moving further along this spectrum.

Interfaces between the human and the tech are where these separate systems interact, and interfaces matter along the tool-human spectrum. The simplest inert tool, like a hammer or knife, benefits from an appropriate handle for a human hand. We have typically “communicated” with machines like cars, tanks, or aircraft using interfaces like steering wheels, levers, buttons, or switches like on the B-17 above. At the other end of the spectrum with a human colleague, we can interface through verbal and nonverbal routes. We communicate very differently with domesticated animals. How might we interface with the new AI-enabled tools between the two extremes of inert tools and human colleagues? Figure 8.2 illustrates some of these interactions.

Communication is wide and deep in the middle of the spectrum, with dogs or horses becoming part of a relationship. We move toward the mix of verbal and subtle nonverbal communication that we have with other humans. Increasingly, AI-enabled tools will interpret our facial expressions, tone of voice, and other cues to gauge and anticipate our confidence, emotions, and intentions (e.g., see the next two chapters by Bill Casebeer and David Huberdeau). Cavalry and other mounted warriors—“human-horse teams”—played a central role in warfare from ancient times to the late nineteenth century wherein humans communicated remarkably well with their non-human “teammates.”

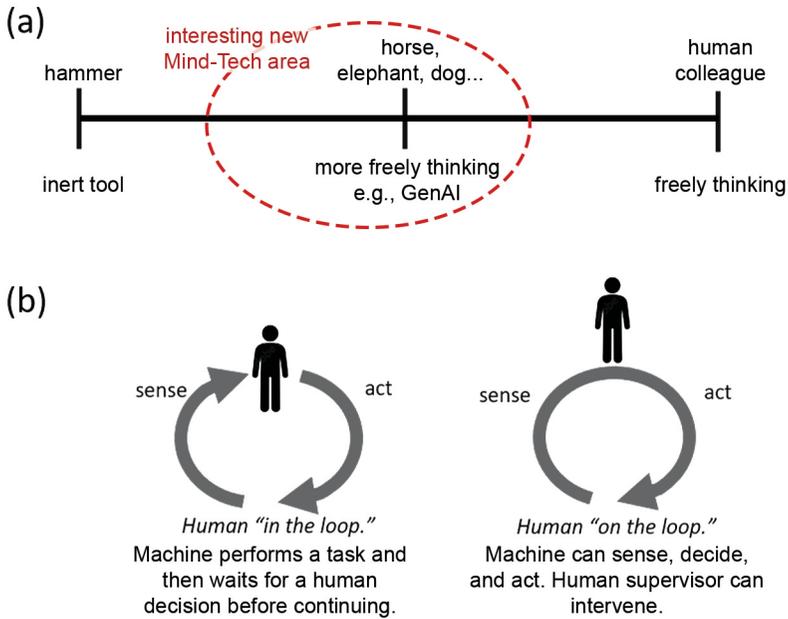


Figure 8.2. Tool-human spectrum, autonomy, and human control. Panel (a) How freely thinking is our “teammate”? The spectrum goes from an inert tool like a hammer to the freely thinking agent that is a human colleague. In the middle are agents who have complex and at least partially hidden processes by which they execute your commands (Box 8.1, below). When you give an instruction to a dog or to ChatGPT, how it chooses to execute that command is often a complex, messy business. An agent’s degree of free thinking is only partly related to its degree of autonomy: a landmine, for example, is autonomous because no human is involved in its decisions once set. An agent’s degree of free thinking can also be distinguished from where human supervisors are involved in control, for example, “in the loop,” or “on the loop,” as shown in Panel (b).

The number of entities toward the middle of the spectrum is growing due to digitization, AI, and now GenAI. With new GenAI, humans will increasingly be able to expand their communicative relationship with machines using complex language: humans giving prompts to machines and humans receiving written or spoken responses back from the machines. The rest of this subsection examines types of communication interfaces: first, between humans and nonhumans, then, interfaces through language, and finally, direct brain-computer interfaces.

Box 8.1. What Is Generative AI?

Artificial intelligence is giving computers behaviors that would be thought intelligent in human beings. A leap in the capability of AI, particularly for perception, occurred around 2012 and relied on “deep learning.”³ Deep learning is one of many approaches to enable machines to learn from data without being explicitly programmed. Deep learning was inspired by the brain, particularly the interconnections of many neurons (brain cells). The key idea in deep learning is that the neural networks have at least one “hidden layer” in the middle between inputs and outputs whose “neurons” can take on different weights while learning about the task. Big models can have many nodes in such hidden layers—and interpreting what all those nodes’ weights mean in terms comprehensible to humans makes it difficult to explain or predict why big, deep learning models make their decisions. They are not like a pocket calculator that always adds $2 + 2$ to give the same result. These big, deep learning models are more freely “thinking.”

Generative AI are models that can produce new instances of data by learning from other data. By seeing many pictures of dogs and cats, for example, the AI learns what dogs and cats look like. Then it can generate new pictures of dogs and cats and even of “dog-cats” that don’t actually exist. Generative AI had a major technical advance in 2017,⁴ and then ChatGPT (Chat Generative Pre-trained Transformer) burst into the public consciousness in 2022. The big, new GenAI models like ChatGPT learned from vast amounts of text and are large language models (LLM), see below. I can now read and successfully answer exam questions for parts of a Wharton MBA and do many other remarkable feats—as demonstrated at the end of this book, which includes work by GenAI. GenAI can now create new pictures and videos—and is the technology underpinning deepfakes (see chap. 15 on performance degradation). These models are improving their ability to plan and conduct multistep reasoning⁵: if dogs and horses can “think,” that is where these models are now going. But the models remain limited, and currently for many tasks the GenAI models are more like having unlimited interns than a crack team of experts.

(1.2) Communication Interfaces Between Humans and Non-humans

Wolves, ants, orca whales, dolphins, meerkats, and chimps can all communicate in enormously sophisticated ways.⁶ Chimps, orcas, and dolphins can communicate to collaborate in sophisticated, ingenious plans. Chimps form complex alliances, deter each other, and communicate in other ways that can mean the difference between life and death. Communication is the transfer of information from one individual (or group) to another individual or group. It involves both sending and receiving. Many communication methods exist, including visual, sound, smell, and touch. Many types of life-and-death information can be communicated, from the basic (e.g., “Watch out, I am dangerous!” or “I want to mate!”) to the more sophisticated, such as confidence, pride, shame, or status.

Humans extensively use nonverbal communication with other humans, perhaps communicating even more than via words.⁷ Charles Darwin studied how we communicate emotions to others using facial expressions. Our postures can convey messages. Congenitally blind athletes across cultures show body poses similar to non-blind athletes after winning (e.g., arms thrown up and chest out) and losing in Olympic judo competitions—something they won’t have learned by observing others.⁸ Laughter conveys a lot. We humans even use nonverbal cues in digital zoom meetings.⁹

Humans communicate with animals.¹⁰ Human riders communicate with horses to perform remarkably controlled actions like show jumping. Much of our interface with dogs is nonverbal. Dogs get valuable information from where we humans are looking or pointing, such as the location of prey or danger. Dogs understand that what we are communicating is informative and cooperative. If that sounds trivial, it isn’t: chimpanzees are undoubtedly clever, but dogs outperform chimps on such tasks. Dogs can recognize some human words for objects, such as ball or stick, and, remarkably, pet dogs have different patterns of brain activity when they are shown an object that doesn’t match the word they hear.¹¹

Tech can also receive information from humans via such nonverbal communication—as described by Bill Casebeer and David Huberdeau in the next two chapters. Warriors are increasingly monitored for measures like heart rate (which can increase with emotional arousal), where their eyes are looking, pupil size, and so on. AI can

monitor facial expressions, and although complicated (e.g., a smile may not indicate happiness or a scowl indicate anger), they convey a range of information important for social communication.¹² We should not expect tech to interpret human mental states or intentions with anything like certainty from such measures—I am a human and I cannot work out others’ mental states purely from nonverbal indicators such as their facial expressions. Instead, I use facial expressions as one indicator among many. We should anticipate that tech will increasingly be able to combine multiple nonverbal sources of information about us (e.g., body, face, tone of voice) and combine those with context and our words.

(1.3) Interface Through Language

Language is a means of communication consisting of words (or other symbols) used in a structured and conventional way. Human language abilities are far beyond those of any other animal.¹³ Human language is unique among animals and provides a unique interface.

Language is amazing for increasing the bandwidth of information communicated. The word “iron,” for example, conveys a vast store of information about what the metal is, its key properties (like rusting), and its uses. As you will know if you have played the game charades, for instance, if you must communicate a book’s title just using nonverbal communication, it is remarkable how much information even a single word can contain. Written words in objects like books can encapsulate vast stores of information.

Language is particularly relevant now because suddenly GenAI has enabled machines to communicate with us humans using a remarkable new human-tech interface. GenAI can send information to us via amazingly good text, and it can receive information from us via “prompts” written in human language (fig. 8.3).

So what? This new way of giving commands to machines using language (“prompts”) and receiving information back from the machine as language is likely to reflect a fundamentally new interface between humans and computers. In computing, this interaction can be called a user interface or UI.

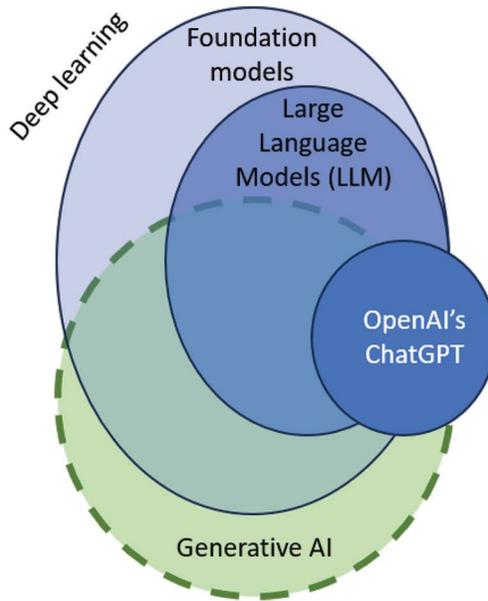


Figure 8.3. Language and large language models. GenAI can create new instances of data. The most powerful new GenAI models are “foundation models” that are deep learning models trained on large volumes of unlabeled data using self-supervised learning. The best of these are LLMs that are a subcategory of foundation models for text and computer code, such as OpenAI’s GPT. ChatGPT is an application built on a LLM created by the company OpenAI, and it has been optimized for dialogue. (Source: Figure is based on a presentation at System Applications and Products in Data Processing [SAP], Germany, June 2023.)

When computers emerged in World War Two, the interface was “batch processing” in which users specified a complete workflow of everything they wanted the computer to do.¹⁴ Then, from around 1964, multiple users could share a single mainframe computer through connected terminals, enabling “command-based interaction” in which the user and the computer took turns one command at a time. This type of interface has dominated computing ever since, including command lines (e.g., DOS or disk operating system) and graphical user interfaces (e.g., Macintosh, Windows, and all current smartphone platforms). Now, with GenAI and LLMS, instead of telling the computer what to do, users tell the computer what outcome they want; that is, users establish *intent*.

For instance, I asked an image generator to make a picture for my son's birthday card: "A red, bearded dragon and a tortoise holding a birthday cake with eight candles. On a light background." It generated four options, and I chose the image that most closely matched my intent (amusingly, it kept showing the wrong number of candles, and in another instruction to include text, it spelled the text incorrectly despite my having provided the text).

New ways to communicate using language can be a source of military advantage. It was crucial to Germany's World War Two blitzkrieg in which commanders gave their intent (or prompts) that subordinates were to carry out—the *Auftragstaktik* copied by the British and Americans as mission command ever since. David Vernal's chapter 17 gives some examples, and he then creates some GenAI analyses in chapter 18.

Intelligence analysis is another likely application.¹⁵ LLMs are good at generating written summaries of large amounts of information—as we do at the end of this book. As we describe later in this chapter, GenAI may also generate new ideas and so act as a commander's aide.

Given that much cutting-edge research is now happening in the commercial sector, it is also helpful to ask, What real-world applications of LLMs are we seeing outside the military?

In the commercial world, the two big 2023 use-cases for GenAI seem to have been computer coding and marketing. For computer coding, Microsoft's GenAI Copilot uses GenAI to suggest large chunks of code when someone starts typing: it now has 1.3 million paid Copilot accounts, with over 50,000 companies using the software.¹⁶

In marketing, one of the world's largest marketing companies, WPP, recently demonstrated its internal AI workspace, which gives employees managed access to a range of GenAI models across text and imaging.¹⁷ WPP also discussed training models on particular brands' tone or voice, or target demographics—and it already has almost 30,000 users and millions of prompts (the command the user inputs into the GenAI). Meanwhile, Coca-Cola talked about using GenAI to create thousands of marketing assets automatically.

Medicine is a much larger segment of the economy than defense (e.g., 18 percent of US GDP versus about 3–4 percent in 2023). AI took a big leap in 2012, but AI only recently began to enter real-world practice in hospitals, in limited ways.¹⁸ If recent advances in GenAI take a similar amount of time to mature, then given its breakthrough in 2017, we should expect to still be in the early stages now—and that is the case. A GenAI Google chatbot recently diagnosed heart and lung

conditions more accurately than doctors in online healthcare and was ranked higher on empathy—but this scenario was not with real patients but with actors playing patients, as I faced when I was a medical student.¹⁹ Ethical and practical issues are legion, but GenAI will probably begin applications over the next decade.²⁰

Some key challenges to real-world use have emerged from these commercial applications. For instance, the AI can “hallucinate” (i.e., confidently make untrue statements), and it is often unclear where the liability for mistakes lies within the human-machine teams. Another challenge is that GenAI may try to tell us what we want to hear or sounds plausible, hide parts of their reasoning, or even pick up on our deceptive behavior.²¹ We need ways to improve this language interface to better convey computer confidence and reasoning.

Moreover, at this stage in the application of GenAI, nobody really knows what the best types of UI will look like.²² In the same way that the hugely successful Google search interface or the iPhone did not immediately emerge, we may be waiting for some brilliant new interface that works wonderfully with us human users.

Could we instead bypass nonverbal and language and go straight to the brain itself?

(1.4) Brain-Computer Interfaces

A brain-computer interface (BCI) is a direct communication pathway between a brain and an external device.²³ Like other forms of interface, this communication can involve reading from the brain (e.g., for a paralyzed person to control a robotic hand) and/or writing to the brain (e.g., providing sensory information from the robotic hand’s “skin”).²⁴

BCIs could prove life-changing to restore function in people with disabilities. But it remains an open question as to how useful BCIs will be to enhance function in healthy individuals. It is possible that they can help improve the speed or bandwidth of communication between humans or between humans and machines—and we will only know about such potential benefits by testing the technologies.

Benefits must also be traded against risks, for example, as in neurosurgery to implant a device. Thus, whether the benefits outweigh potential risks will crucially depend on whether the BCI is implanted in the brain or is non-implantable.

Non-implantable BCIs can read from the brain from outside, for example, by reading changes in the electrical (EEG) or magnetic (MEG)

fields or blood flow (e.g., fMRI). Under controlled lab conditions, these can be highly precise and useful, but there are challenges to applications in war. For example, the level of precision needed when conducting EEGs requires a “Faraday cage” to remove unwanted electrical interference, and MRI scanners are currently bulky. Much simpler devices have been reportedly used in less controlled settings, for example, in truck drivers to detect drowsiness.²⁵ However, these cases are much simpler, and non-implantable BCIs remain of limited use in many real-world settings. That said, if these practical limitations could be overcome by a new advance (such as new types of skull contacts for EEG), these could be powerful. In human-machine teams, for example, researchers have recently used the noninvasive EEG measurement of brain signals to correct the mistakes of a robot.²⁶

Implantable BCI devices have advanced rapidly over the past three decades. In 2000 a team recorded signals from the brains of monkeys as those monkeys performed reaching tasks, and these brain signals could be used to control a robot arm in real time.²⁷ By 2006 a boy with severe epilepsy could control the video game *Space Invaders*, and by 2015 an effort backed by the Defense Advanced Research Projects Agency (DARPA) enabled a tetraplegic woman to control robotic arms and fly an F-35 simulator.²⁸ The most well-known BCI program is Elon Musk’s Neuralink. Although it has no particular advanced tech that others don’t have, it aims to bring together cutting-edge tech, backed by plentiful funding and a “can do” attitude. In 2024 Neuralink livestreamed the first human patient implanted with its first product, which showed him moving a cursor around a screen to play chess using only neural signals—with a device far smaller and less obtrusive than those pioneered only a few years before. Newer devices are also increasing the bandwidth of data acquired from the brain. There are many rivals to Neuralink, such as the Jeff Bezos and Bill Gates-backed startup Synchron in New York that has implanted its device in ten people.²⁹ China has also demonstrated this capability.³⁰

The limitations of these implantable devices currently constrain their use, but overcoming the limitations could lead to a sudden leap in their use for enhancing healthy humans. The main limitations include the following four considerations. First, brain surgery carries nontrivial risks. Second, there is “scarring” (gliosis) around the devices after only a few years (or sooner) that severely limit how long the devices can last (altering the risk-benefit analysis for young, healthy warfighters). Overcoming the problem of scarring is largely a materials science challenge,

analogous to the developments of new coatings and materials successfully developed for the stents put into coronary arteries after heart attacks. A third consideration is how to turn the vast amounts of brain data from these new BCIs into useful information that decodes the intentions of the user—the communication that is the purpose of an interface.³¹ Finally, the fourth limitation is how to update the devices if the company goes bankrupt or if security patches are needed and to do these updates securely, analogous to Vice President Dick Cheney’s need for a specially adapted cardiac pacemaker that did not connect to the outside world in a standard way.³²

Interfaces are where separate systems—such as a human and a machine—interact with each other. In this section, we have seen examples of interfaces, including nonverbal, language, and direct brain-computer interfaces. But when separate systems interact, they can do more than just communicate. They can also change each other cumulatively over time so that they better complement each other and *converge* toward becoming a more unified entity.

(2) Converge

Humans and their technologies *converge*, changing together toward some point of unity. Humans shape technologies, and technologies shape humans. The systems don’t just interface; the systems themselves fundamentally change—and that can happen at many timescales.

Human evolution was shaped by our technologies. Technology is the application of knowledge for practical purposes, and humans have made tools like the hand ax from about 2 million years ago and have controlled fire for around 400,000 years—before anatomically modern humans appeared around 300,000 years ago and cognitively modern humans around 30,000 years ago. These technologies changed our bodies as we came to rely more on our bigger and smarter brains, which enabled us to use ever more powerful technologies. Adult humans are physically puny compared to even a juvenile chimpanzee, but humans have spears and axes.³³ During an individual’s lifetime, our use of technologies changes the structure and functioning of our brain, as seen in many brain imaging studies involving typists, jugglers, musicians, golfers, and others.³⁴

Our remarkable human brains are the origin of these technologies—and so shape these technologies too. Humans originated in hot cli-

mates but constantly developed technologies like clothing over generations so they could thrive in cold climates all the way up to the permanent snow of the Arctic. Humans constantly imagine, adapt, and refine technologies—so that technologies evolve too.

In warfare, convergence changed the humans and the technology, again over many timescales. Over centuries, horse-human teams converged. Horses changed in size, shape and behavior; so did equipment to include the stirrup, bits, and saddles; and so too did the training and techniques of human riders as mounted archers, light cavalry, and heavy cavalry. Over lifetimes, the English longbowmen who won famous victories at Crécy in 1346 and Agincourt in 1415 changed themselves by developing expertise over many years.

Technologies and human operators also converge over the course of wars, as in World War Two. Germany's Heinz Guderian is famous for helping design tanks and crew training to improve performance. A less well-known story concerns what is often called World War Two's greatest tank: Russia's T-34.

The T-34 certainly was certainly a remarkable machine by early 1944, but as Yale historian Paul Kennedy describes in his book *Engineers of Victory*, making it work better with its crews required a long process of iteration.³⁵ In 1942–43 major problems included no means of communication between the crew (apart from the commander tapping his foot on the driver's shoulder). Further, the “poor commander's compartment was itself a horror, for he had far too many jobs to accomplish when a battle erupted, in a cockpit that was too cramped.”³⁶ These flaws also show the trade-offs that need to be made in innovation and production: Russia desperately needed to produce tanks at scale, and design improvements could only be made when the spring and autumn muds reduced the level of fighting. Like the famous P-51 Mustang, the T-34 was improved by iterative, incremental change, which could only happen when circumstances allowed it and after the experience fighting.

How can we better harness convergence today at different timeframes both before and during war?

(2.1) Convergence and the Process of Innovation Now

To create innovative capabilities in the Mind-Tech Nexus, we must understand the process of innovation today in a country like the United States. The process of innovation is shown in figure 8.4. This process typically proceeds from (1) *basic research* that seeks the laws of nature

(e.g., at universities), through (2) “*deep tech*” that is close to the edge of unanswered scientific questions and also has potential usefulness over a long time horizon (e.g., at DARPA),³⁷ through (3) *proprietary research* in which patents can exclude commercial competitors (e.g., Apple’s iPhone or big defense “primes”), and on to (4) *scale for value* to create large mass (e.g., Apple through suppliers in China). At all stages in this process, (5) *tech infrastructure* is vital for areas like measurement, testing, and standards (e.g., the National Institute of Standards and Technology).

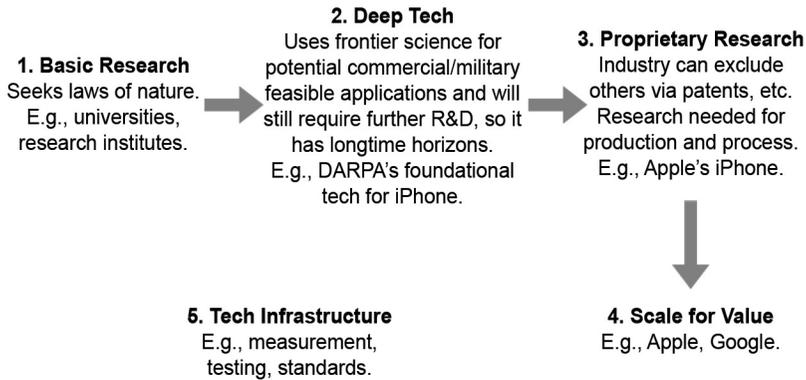


Figure 8.4. The process of innovation. (Adapted from Nicholas D. Wright, “DARPA’s Magic Ingredient—Speed—Can Help Build a Fleet of Allied ‘DARPAs,’” Commentary [Center for Strategic and International Studies, January 2022], <https://csis-website-prod.s3.amazonaws.com/>, which draws on David Sainsbury, *Windows of Opportunity: How Nations Create Wealth* [Profile Books, 2020] 201–4.)

Every stage in the innovation process can provide an edge: consider the iPhone that is the twenty-first century’s most successful tech gadget. Universities made key discoveries on which organizations like DARPA built crucial “deep tech” such as miniature GPS. Apple packed the technology in innovative ways, creating a brilliantly easy design that was then built on a huge scale. The iPhone has since been made ever more useful, and users have become expert in its operation through numerous iterations. The iPhone is also a good example because in our time, unlike in the Cold War, as described in this book’s introduction, much of this innovation is now done in the commercial rather than defense sector.

Applying this to innovation in the Mind-Tech Nexus for security, we can consider each step in the process of innovation. First, how are basic science researchers incentivized to work not purely on technology or

cognitive science but at the nexus where they meet? Second, at the level of deep tech, are organizations like DARPA considering areas at the intersection of mind and tech—and more broadly are there sandboxes where researchers and potential users can come together to potentially identify new avenues for development? At the deep tech stage, government support is vital because commercial returns can be a decade or more in the future, and commercial competitors may not be prevented from benefitting from the research.³⁸ Third, at the stage of proprietary research, sandboxes and exercises will be vital for Mind-Tech capabilities that really work—iterating as the Germans and Russians did before and during World War Two with their tanks. Fourth, scaling up without relying on the world’s manufacturing superpower—China—will be difficult, but the democracies must once again build their capabilities at this stage too. China is now very good at innovative manufacturing at scale: it can build electric cars far more cheaply than the US, Europe, or Japan, partly through subsidies but mainly through constant iterative, innovative manufacturing at scale.³⁹

Focusing on the Mind-Tech Nexus across the process of innovation—versus on pure technology with the human side largely an afterthought—is to harness the old adage that “what gets measured gets done.” In chapter 7, Jack Shanahan, founding leader of the Joint AI Center, discusses creating metrics for developing technologies that capture not just the readiness of the technology but also its readiness to operate with humans. Technology Readiness Levels (TRL) are a well-known measurement system to assess the maturity level of a particular technology.⁴⁰ It goes from TRL-1 in which scientific research is beginning to TRL-9 in which the technology is “flight proven.” Alongside the TRL, a Human Readiness Level (HRL) from HRL-1 to HRL-9 can similarly provide a simple number indicating the state of integration within the system with respect to humans and technology.⁴¹ It can go from HRL-1 involving basic research on human characteristics and performance to HRL-9, where the system is successfully used in operations across the operational envelope with the systematic monitoring of human-system performance.

What types of physical forms will these innovative new technologies take? In the next two subsections, we examine two cases in the middle tool-colleague spectrum that will increasingly involve GenAI: humanoid robots and weightless AI cyber agents.

(2.2) The “Humanoid Form Factor” and Moravec’s Paradox

One of the most striking ways that humans and technology will likely converge is to build robots with the form of humans. While this likelihood seems like science fiction, it isn’t. In early 2024 the CEO of leading AI chip company NVIDIA, currently neck and neck with Apple as the world’s biggest listed company, announced at its annual conference that humanoid robots powered by GenAI were a major new aim. He further revealed a new foundation model—the underlying model on which specific-use cases can be built—developed for controlling humanoid robots.⁴² To be sure, robots can take any physical form (such as robot arms in factories, tracked tanks, bomb disposal robots, or self-driving cars), and we can even build agents that are weightless in cyberspace (described below)—so why will one important form likely be a convergence toward humanoid robots?⁴³

Firstly, robots shaped like humans can *act within our human world as it already exists* with its vast array of environments and tools already designed for human use—stairs, tables, screwdrivers, spanners, saws, rifles, medical kits, grenades, keys, spades, garden rakes, secateurs, blowtorches, and so on. To make a robot useful around my house—a Victorian house in suburban London—it would help enormously if it could move around and use all the objects I already have to achieve tasks like cleaning, cooking, or looking after a sick person. In our public spaces, think about how many years and how much money it has taken to make many aspects of our built environment accessible to wheelchair users—and despite those efforts, many physical spaces remain poorly accessible. In my house, I have various sets of tools for cooking, gardening, carpentry, bicycle maintenance, and the like—all designed for human hands like mine.

Giving robots humanoid form (or at least aspects of it) will open up vastly more possibilities for those robots to act usefully in the human world. Not all robots will be humanoid, but it is a hugely versatile form because we humans have already spent millennia and trillions upon trillions of dollars making tools and worlds for humanoids like us. On the battlefield, humans and robots can converge as elements of interdependent collaborative units that include multiple humans, multiple robots, and the tools they use.

A second big advantage is that *building humanoid robots could help those robots learn*—and so help improve their AI “brains.” GenAI models such as OpenAI’s are running up against the problem that

much of their success rested on learning from vast amounts of data that includes much of the internet and many of the world's books, so where can they go next for useful data? Mammal infants are physically embodied agents who watch vast amounts of physical interactions in the world and can provide another source of data for training. These findings have been described recently by leading AI researchers at Meta⁴⁴ and in other research with AI learning language using footage from cameras placed on human infants.⁴⁵ Perhaps learning by watching billions of hours of videos is a proxy for physical embodiment and experience of the world, just as reading text written by humans at massive scale helped models like ChatGPT.

Human infants also learn by interacting with the world—and robotic interactions with the physical world could improve the AI models through an “embodied intelligence” strategy, which is key to Nvidia’s plan to develop AI in its Project GR00T.⁴⁶ Nvidia refers to the new platform as “a general-purpose foundation model for humanoid robots,” which could be an AI platform for many other humanoid robot companies.⁴⁷ Humanoid robots have begun operating in Amazon warehouses and factories for Mercedes-Benz and BMW.⁴⁸

Moreover, human infants and children learn from adults and peers—getting thousands of hours of useful data observing how others do things and receiving specific training. That is why, for example, Nvidia’s Project GR00T aims to develop AI models that help humanoid robots learn better by using linguistic instructions from adults, observing human demonstrations, and having human teleoperators help them practice actions.⁴⁹

Such help to learn is vital because of Moravec’s paradox: tasks thought difficult for humans are often easy for AI to accomplish (e.g., chess), but tasks thought easy for us humans (e.g., moving arms) can be hard for AI to accomplish. Learning to act in the physical world is incredibly difficult—far more so than most people realize. Even though they are improving rapidly, today’s best humanoid robots are far from as good as a human adult when assessed across a wide range of activities in real-world environments and have much to learn from humans.⁵⁰

These two advantages of the humanoid form factor will shape AI: better convergence with our existing human world and better learning of how things work in our existing human world. As AI becomes more powerful, it will also shape our world. And so the spiral of convergence goes.

We are already building humanoid robots that may be useful in simple environments like factories. We are moving toward having

useful humanoid robots that can receive verbal commands and be controlled as fleets or swarms of humanoid robots. We are also building non-humanoid robots like self-driving cars that are now racking up huge amounts of driving time that can act as data—and interestingly, it looks like China is equal to America in the competition of having large amounts of driverless car data.⁵¹ Who will build the humanoid robots at scale that will provide the data to improve the AI, that can in turn improve the humanoid robots, that in turn provide more useful data . . . ?

Physical forms like humanoid robots and self-driving cars will not, however, be the only form that AI agents can take—consider AI agents with almost no weight at all.

(2.3) Converging with Weightless Agents

Versatile AI agents, such as humanoid robots, will increasingly need to look ahead and plan how to use various tools to achieve tasks. In fact, any type of versatile AI agent will need this capability, which has become a focus in GenAI research. To see how general this is, consider that billions are being spent developing such capabilities for virtual AI assistants that can chain together sequences of actions, some of which involve tools like specific engines. A prompt might be, for example, “Get me from London to Milwaukee on these dates,” which could involve searching maps or booking trains, flights, and hotels.⁵²

“Agentic workflows” require the type of planning that is becoming a focus of intense competition between cutting-edge GenAI in big tech.⁵³ OpenAI’s Sam Altman believes helpful agents may be the “killer function” that makes GenAI truly indispensable in everyday life.⁵⁴ That potential applies to weightless agents in civilian cyberspace that might organize a trip and also to cyber agents in cybersecurity.

Autonomous or semiautonomous agents in civilian cyberspace already exist with considerable responsibility. Outside security, examples include algorithmic trading programs in Wall Street or the City of London that control hundreds of billions of dollars. When they go right, such algorithmic traders can make billions over years, and they have the advantage of operating at millisecond timescales. But when they go wrong, they can lose hundreds of millions of dollars in a few minutes⁵⁵—and GenAI may make this problem worse in new ways. GenAI is great for creating fake news, as I discuss in chapter 15, and the humans controlling trading algorithms are worried that the trading algorithms may be unable

to tell fake from real news, which may wrongly trigger forced selling of assets.⁵⁶ Using GenAI models for algorithmic trading brings new vulnerabilities, such as from hallucinations or new hacking techniques like “model inversion attacks” in which specific questions are asked of the model that trick it into revealing its secrets.⁵⁷

Autonomy in cyberspace already matters for security too. The most renowned cyber weapon yet used, Stuxnet, was deployed in 2010 against Iran’s nuclear program. This malware hid itself from antivirus software, then spreading to every machine in the network looking for a particular type of software (Siemens Step 7) that operated a specific type of controller for centrifuge speeds.⁵⁸ Stuxnet copies that found no target went dead, but those finding the target then deployed two “war-heads”: one to make the centrifuge controller go wrong, the other to deceive the human centrifuge users into believing that the controller was operating normally. Stuxnet had considerable autonomy once introduced into a system.

Defenders can also work with AI to help them operate in cyberspace at the speed and scale needed. DARPA ran a 2016 Cyber Grand Challenge in which over a hundred teams competed to build a fully autonomous Cyber Reasoning System to defend a network.⁵⁹ The process involved several steps: finding vulnerabilities, making a “patch,” knowing when and how to use the patches, and so on. With fifteen billion devices connected to the “Internet of Things” in 2023⁶⁰—a figure forecast to rise massively—humans will require the help of machine teams to help them go through the myriad multistep processes required for defense.

Weightless AI-enabled agents will be the dogs, horses, tanks, and machine guns we humans will use in cyberspace. These weightless agents will be able to use cyber tools originally designed for humans (e.g., mapping software or search engines). We humans will converge with these agents to become more effective units that can achieve our missions. If this sounds like science fiction, remember that so much of our human mental life already happens apart from our bodies in shared mental worlds: when we watch a film we can be so totally engrossed that we are “in the film.” We have had shared mental lives as humans since prehistoric times through religious ideas, then on to stories like Homer’s *Odyssey*, engrossing books, plays, and so on. How will humans operate in the geography of cyberspace? They will do so with “red” servers, defending forwards, and all the rest. We will require AI agents to help us react at the speed and scale needed to compete, just as drones or humanoid robots in the physical world use tools and

respond to our language commands. Over time, we humans will converge with these technologies, the humans and the tech enhancing each other to execute tasks more effectively.

As well as humans interfacing and converging with tech, Mind-Tech advances can also be aimed at more directly enhancing our human abilities.

(3) The Human

As I type this sentence, I am wearing spectacles to *correct* my eyesight. As I look out of my office window at night, if I desired, I could use a pair of night vision goggles to *enhance* my vision beyond the limits of human biological potential. The correction of reduced performance, and the enhancement of performance beyond human physical potential, both have enormous uses far beyond the military—which is why many powerful, dual-use Mind-Tech advances are being developed by civilian organizations in areas like medicine and big tech. We have considered how humans and technology interface in the Mind-Tech Nexus and then how they converge. In this final section, we consider this nexus from the perspective of the human.

Humans will be central to warfare for the foreseeable future. We must remember that humans are actually very good at many things: their “frail bodies” have climbed Mount Everest and their “limited” brains have invented the technologies to put humans on the moon. Humans are good at things in war too, which is why they will not be replaced for many warfighting tasks. Indeed, even if machines outperform humans for various tasks, humans will not be immediately abandoned. Humans are versatile. Humans are also often cheaper than technology. Recent research from MIT, for example, showed that even in the quite well-established field of AI vision, it is only economically viable to replace humans in about a quarter of currently feasible cases.⁶¹ Indeed, militaries always use a mix of old and new means of doing things, which is why Germany’s 1941 blitzkrieg into Russia used cutting-edge technologies—and also took in 600,000 horses.⁶²

But humans are not perfect and will often be the target of more direct enhancement. In this final section, we explore three areas: physical enhancement (e.g., an “exosuit”), mental enhancement (e.g., tactical or expert AI advisors), and directly altering our cell biology (e.g., genetics).

(3.1) Physical Enhancement

Human bodies can be enhanced to be mechanically stronger. Exoskeletons are external, removable structures that can support the human musculoskeletal system. Powered exoskeletons have been under development for decades but are currently limited mainly by battery life, financial cost, and constraints on speed and range of movement.⁶³

Drugs can enhance aspects of physical strength and endurance—such as “EPO” to increase red blood cell production or anabolic steroids to increase muscle—although these drugs can also have negative side effects such as strokes, increased predisposition to injuries, or long-term decreased fertility.⁶⁴ Such drugs are banned in elite sports because of their side effects, but athletes in elite sports like cycling often use such drugs “off-label,” in doses not adequately studied by scientists, to gain an edge over non-drug users.⁶⁵ During selection for military fields like special forces, the candidates as a whole would be better off medically if none took the drugs, and only robust drug-testing regimes can prevent drug-using candidates from creating an unlevel playing field.⁶⁶ If during future warfare these powerful drugs *may* play roles, employing them in ways that truly contribute to outperforming adversaries will involve complicated, ethically challenging questions. These questions are best answered by ethically sound and clever scientific study rather than by random amateur, anecdotal trial and error.

We can also extend our sensory performance. Sensory extenders include passive devices like telescopes and active devices like night vision goggles or the helmet of an F35 pilot that can “see” using multiple types of cameras. Such sensory extenders can be mixed with “Augmented Reality” to layer on additional information—as you look at foreign language scripts, for example, Meta’s AI-enabled Ray-Bans can translate the script in almost real time.⁶⁷ Augmented Reality may use AI to identify objects we might need to pay attention to, which was the basis of the Pentagon’s Project Maven led by Jack Shanahan (author of chap. 7). However, there is no free lunch, and if poorly used, these extenders can be detrimental. Passive extenders like telescopes enable you to see more of less, for example, by magnifying and reducing the visual field. Active extenders like Augmented Reality goggles can get in the way of our excellent human perceptual systems—as Ben Connable describes in chapter 13 for a recent high-profile US DOD program. Such technologies must be developed so they converge with the human’s needs.

(3.2) Mental Enhancement

Many aspects of brain function can be augmented. This includes vital lower-level brain processes, such as coping with sleep deprivation. Drugs like modafinil (tradename Provigil) can help humans cope with sleep deprivation, for example, and caffeine can help with alertness.⁶⁸ Once again, as drugs like amphetamines illustrate, potential side effects mean that such drugs should be used carefully and under supervision.

Higher-level brain functions can also be enhanced,⁶⁹ and to see some examples we can consider the process by which humans make more sophisticated decisions (fig. 8.5). We can break the decision-making process into a chain from *data* as a “raw material” processed into *information*, then *knowledge* (ordered sets of justified enough beliefs), and finally, *wisdom* (broader context for more holistic judgments). Advances in AI around 2012 enabled it to greatly enhance the ability to turn data into information, as seen in programs like Project Maven. But that was only the start.

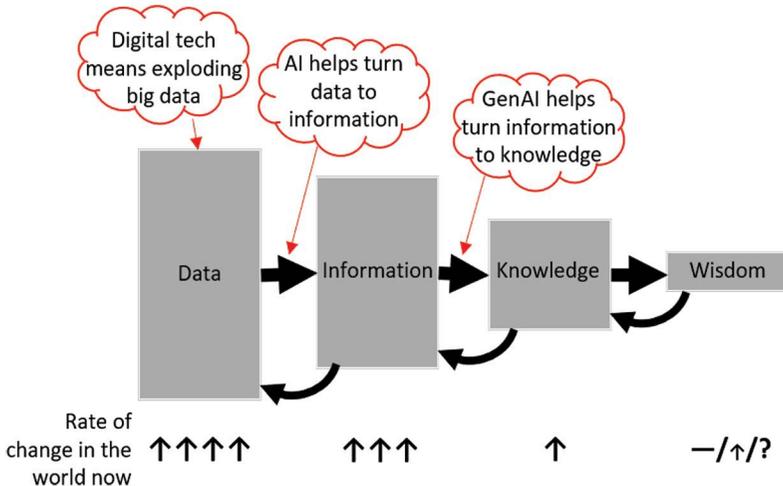


Figure 8.5. Data, information, knowledge, and wisdom. See the introduction to this book for further discussion.

GenAI advances since 2022 have moved higher up the decision-making process to enable enhanced knowledge.⁷⁰ ChatGPT is a generic LLM trained on the internet in general, but it already has the knowledge to pass some exams at places like Wharton.⁷¹ New LLMs are being built with more specific focus, such as “ScienceGPT,” a massive new science research

model on a US government supercomputer at Argonne National Laboratory.⁷² LLMs may even increasingly devise new tactics: Google's TacticAI is an assistant for soccer tactics, such as corner kicks, and outplayed human suggestions 90 percent of the time.⁷³ However, even the best GenAI is still not reliable enough to provide solutions like medical advice,⁷⁴ so its role will be helping human experts, at least for the near future.

Such advice will likely affect the humans receiving it in multiple ways. One effect will be to make humans follow the new incentives these AIs create, as shown recently by an analysis of referees in professional tennis. Tennis has used AI to assist referee decisions for the past few years, and it changed the decision-making of human referees by minimizing their chances of publicly making the wrong judgments.⁷⁵ Other effects have been shown to have mixed results in previous research: Humans sometimes overrely on AI ("automation bias," for example), but when the stakes rise, they may become more cautious about relying on algorithms. We need further research on what factors make the humans *rely appropriately* on AI expert knowledge.⁷⁶ Moreover, expert knowledge alone is not enough.

Wisdom involves broader context for more holistic judgments and remains much more human. However, wiser choices can be operationalized via systematic approaches like jointness and net assessment and aided by technology. AI aids might help by adding an outside perspective and critiquing our thinking, which can help fix blind spots and correct biases.⁷⁷ They can enable us humans to improve our "metacognition" or "thinking about thinking."

(3.3) Changing the Cell

A final way that technology can change humans is by acting at the cellular level. Genetic engineering can alter human DNA either by modifying our reproductive cells ("germline modification," which is passed on to the next generation) or by modifying cells in the grown organism ("somatic modification," which affects only target cells and those cells descended from them in the individual's body). CRISPR technology emerged around 2012 and provided a technological leap in our ability to edit genes, which can be applied to both germlines and somatic cells.

Recent work on *germline modification* in the US has created hundreds of CRISPR-edited pigs in four elite pig breeding lines, which are immune to a disease estimated to cost farmers \$2.7 billion a year globally.⁷⁸ These

pigs are likely to become the first genetically modified farm animals to be used for large-scale meat production. A Chinese researcher shocked the world in 2019 by announcing the birth of two human babies whose genomes had been CRISPR-edited to prevent HIV infection—for which he was sent to prison. Germline editing raises profound ethical issues and is not currently recommended anywhere in the world.⁷⁹

Somatic modification in humans, on the other hand, has now been done in many studies. In a world first, in 2023 a medical protocol to use CRISPR gene editing was approved by the UK Medicines Regulators—in order to treat people aged twelve and over who have the serious, genetically caused blood diseases sickle cell disease and transfusion-dependent beta-thalassemia.⁸⁰ However, correcting such relatively simple and well-understood genetic diseases is vastly simpler than enhancing the complicated genetic control of physical or cognitive traits; thus, genetic science remains far from knowing how to enhance performance. We need a far better understanding of basic genetic science controlling such traits before we can enhance performance.

Besides the genetic engineering of humans themselves, another way cellular technology can affect humans is by modifying bacterial cells or viruses to create *biological weapons*. In the near future, it may even be possible to make new cells synthetically. Such technologies intersect with AI because although using LLMs to create biological weapons will be difficult,⁸¹ more broadly it is estimated that commercial AI software will design perhaps 30 percent of medicines over the next five years—helping to make biowarfare more accessible and affordable.⁸² These technologies raise potential ways to attack humans, and they will also be needed for defense, such as using new mRNA vaccines that can enhance our human immune systems.⁸³

Conclusions

The Mind-Tech Nexus arises from how human factors interface and converge with technology, and Mind-Tech advances have enhanced warfighter performance for millennia. To better anticipate the character of the Mind-Tech advances in our time, this chapter explored three areas. First, it discussed ways that Mind-Tech advances affect how humans *interface* with technology to enhance performance: non-verbally, verbally, and direct brain-computer interfaces. Second, it described how mind and tech *converge* in the process of innovation to

enhance performance, and we examined two particular examples: humanoid robots and weightless AI cyber agents. Third, we asked how *humans* themselves can be changed through physical enhancement (e.g., an “exosuit”), mental enhancement (e.g., tactical or expert AI advisors), and by directly altering the body.

We must harness these Mind-Tech advances to compete in our era—and we must harness them in ways consistent with who *we* are as free, democratic, and ethical societies.

Notes

1. Ian Levy, “So Long and Thanks for All the Bits,” blog post, National Cybre Security Centre, October 27, 2022, <https://www.ncsc.gov.uk/>.

2. Matthew Johnson and Alonso H. Vera, “No AI Is an Island: The Case for Teaming Intelligence,” *AI Magazine* 40, no. 1 (2019): 16–28, <https://doi.org/10.1609/aimag.v40i1.2842>; and Carl Benedikt Frey, *The Technology Trap: Capital, Labor, and Power in the Age of Automation*, illus. ed. (Princeton University Press, 2019).

3. Nicholas D. Wright, ed., *Artificial Intelligence, China, Russia, and the Global Order* (Air University Press, 2019), <https://www.airuniversity.af.edu/>. See, for example, chap. 1.

4. Visual Storytelling Team and Madhumita Murgia, “Generative AI Exists Because of the Transformer,” *Financial Times*, September 12, 2023, <https://ig.ft.com/generative-ai/>.

5. Madhumita Murgia and Cristina Criddle, “OpenAI and Meta Ready New AI Models Capable of ‘Reasoning,’” *Financial Times*, April 9, 2024, sec. Artificial intelligence, <https://www.ft.com/>.

6. See BBC nature documentaries with David Attenborough for vivid examples, e.g., chimpanzees in *Dynasties*, series 1, episode 2, *Chimpanzee*, aired November 2018 on BBC One; or dolphins in *Mammals*, series 1, episode 3, aired April 2024 on BBC One.

7. Judith Holler and Stephen C. Levinson, “Multimodal Language Processing in Human Communication,” *Trends in Cognitive Sciences* 23, no. 8 (August 1, 2019): 639–52, <https://doi.org/10.1016/j.tics.2019.05.006>.

8. Jessica L. Tracy and David Matsumoto, “The Spontaneous Expression of Pride and Shame: Evidence for Biologically Innate Nonverbal Displays,” *Proceedings of the National Academy of Sciences* 105, no. 33 (August 19, 2008): 11655–60, <https://doi.org/10.1073/pnas.0802686105>.

9. Joanna York, “How ‘Non-Verbal Communication’ Is Going Digital,” BBC, November 8, 2022, <https://www.bbc.com/>.

10. Don Kulick, “Human-Animal Communication,” *Annual Review of Anthropology* 46 (October 2017): 357–78, <https://doi.org/10.1146/annurev-anthro-102116-041723>.

11. For dogs versus chimps see Nichola Raihani, *The Social Instinct: How Cooperation Shaped the World* (Jonathan Cape, 2021), 197–98. For dogs and words, see James Woodford, “Dogs Really Do Understand That Words Stand for Objects,” *New Scientist*, March 22, 2024, <https://www.newscientist.com/>.

12. Lisa Feldman Barrett et al., “Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements,” *Psychological Science in the Public Interest* 20, no. 1 (July 2019): 1–68, <https://doi.org/10.1177/1529100619832930>.

13. Simone Pika et al., “Taking Turns: Bridging the Gap Between Human and Animal Communication,” *Proceedings of the Royal Society B* 285, no. 1880 (2018), <https://doi.org/10.1098/rspb.2018.0598>.

14. This paragraph on user interface paradigms draws on Jakob Nielsen, “AI: First New UI Paradigm in 60 Years,” blog, Nielsen Norman Group, June 18, 2023, <https://www.nngroup.com/>.

15. William Usher et al., *Intelligence Innovation: Repositioning for Future Technology Competition* (Special Competitive Studies Project, April 2024), <https://www.scsp.ai/>.

16. Will Knight, “AI Is Rewiring Coders’ Brains. Yours May Be Next,” *Wired*, February 8, 2024, <https://www.wired.com/story/>.

17. Benedict Evans newsletter no. 528, Tuesday, February 20, 2024, list@ben-evans.com.

18. Madhumita Murgia, “Healthcare Turns to AI for Medical Note-Taking ‘Scribes,’” *Financial Times*, January 5, 2025, sec. Artificial intelligence, <https://www.ft.com/>; Sarah Neville, “The Doctors Pioneering the Use of AI to Improve Outcomes for Patients,” *Financial Times*, November 6, 2024, sec. Artificial intelligence, <https://www.ft.com/>; Sarah Ferry and Chibuchi Amadi-Livingstone, “AI in Healthcare: Navigating the Noise,” NHS Confederation, September 20, 2024, <https://www.nhsconfed.org/>; and “Artificial Intelligence Has Long Been Improving Diagnoses,” *The Economist*, March 27, 2024, <https://www.economist.com/>.

19. Mariana Lenharo, “Google AI Has Better Bedside Manner than Human Doctors—and Makes Better Diagnoses,” *Nature* 625, no. 7996 (January 12, 2024): 643–44, <https://doi.org/10.1038/d41586-024-00099-4>.

20. Mariana Lenharo, “AIs Will Make Health Care Safer and Better,” *The Economist*, March 27, 2024, <https://www.economist.com/>.

21. Evan Hubinger et al., “ Sleeper Agents: Training Deceptive LLMs That Persist Through Safety Training,” arXiv, January 17, 2024, <https://doi.org/10.48550/arXiv.2401.05566>; and Ben Dickson, “Language Models Can Use Steganography to Hide Their Reasoning, Study Finds,” VentureBeat (blog), November 9, 2023, <https://venturebeat.com/>.

22. Luke Wroblewski, “AI Models in Software UI,” LukeW Ideation and Design, November 20, 2023, <https://www.lukew.com/>.

23. Anika Binnendijk et al., *Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment* (RAND Corporation, August 27, 2020), <https://www.rand.org/>; and Benjamin Blankertz et al., “The Berlin Brain-Computer Interface: Progress Beyond Communication and Control,” *Frontiers in Neuroscience* 10 (November 2016), <https://doi.org/10.3389/fnins.2016.00530>.

24. Sharlene N. Flesher et al., “A Brain-Computer Interface That Evokes Tactile Sensations Improves Robotic Arm Control,” *Science* 372, no. 6544 (2021): 831–36, <https://doi.org/10.1126/science.abd0380>.

25. Nita A. Farahany, “Neurotech at Work,” *Harvard Business Review*, March–April 2023, <https://hbr.org/>.

26. Andres F. Salazar-Gomez et al., “Correcting Robot Mistakes in Real Time Using EEG Signals,” in *2017 IEEE International Conference on Robotics and Automation (ICRA)* (IEEE, 2017), 6570–77, <https://doi.org/10.1109/ICRA.2017.7989777>.

27. Johan Wessberg et al., “Real-Time Prediction of Hand Trajectory by Ensembles of Cortical Neurons in Primates,” *Nature* 408, no. 6810 (November 2000): 361–65, <https://doi.org/10.1038/35042582>.

28. Nick Stockton, “Woman Controls a Fighter Jet Sim Using Only Her Mind,” *Wired*, March 5, 2015, <https://www.wired.com/>.

29. William Gavin, “Elon Musk’s Neuralink Showed Off Its First Human Patient. Here Are 6 Brain Chip Rivals,” Quartz, March 26, 2024, <https://qz.com/>; and Cassandra Wilyard, “Beyond Neuralink: Meet the Other Companies Developing Brain-Computer

Interfaces,” *MIT Technology Review*, April 19, 2024, <https://www.technologyreview.com/>.

30. William Hannas et al., “Bibliometric Analysis of China’s Non-Therapeutic Brain-Computer Interface Research” (Center for Security and Emerging Technology, March 2024), <https://cset.georgetown.edu/>.

31. Doing so is a challenge for noninvasive and invasive BCI. Advances for non-invasive BCI include methods that can decode narratives from trained human participants using fMRI and GenAI. Karen O’Leary, “MRI Decoders Translate Thoughts into Words,” *Nature Medicine*, May 16, 2023, <https://doi.org/10.1038/d41591-023-00044-4>.

32. Mary Lee et al., *The Internet of Bodies: Opportunities, Risks, and Governance* (RAND Corporation, October 29, 2020), https://www.rand.org/pubs/research_reports/RR3226.html.

33. Joseph Henrich, *The Secret of Our Success: How Culture Is Driving Human Evolution, Domesticating Our Species, and Making Us Smarter* (Princeton University Press, 2015), 69–70.

34. Cassandra Sampaio-Baptista et al. “Structural Plasticity in Adulthood with Motor Learning and Stroke Rehabilitation,” *Annual Review of Neuroscience* 41, no. 1 (2018): 25–40, <https://doi.org/10.1146/annurev-neuro-080317-062015>.

35. Paul Kennedy, *Engineers of Victory: The Problem Solvers Who Turned the Tide in the Second World War*, repr. ed. (Allen Lane, 2013), chap. 3.

36. Kennedy, chap. 3.

37. DARPA operates at a crucial stage in the process of innovation—and to collaborate requires a common name for this stage. “Deep tech” is simple—gaining private and public sector traction—and it is not defense specific. Alternative terms for this concept include “generic research,” “frontier tech,” or types of applied research.

38. For example, deep tech startups are reported to need 35 percent more time and 48 percent more money than usual startups to make over \$5 million in revenue. See *The European Deep Tech Report: 2023 Edition* (Lakestar, Catalyst, and Dealroom, November 30, 2023), <https://dealroom.co/>.

39. Robinson Meyer, “Opinion: China’s Electric Vehicles Are Going to Hit Detroit Like a Wrecking Ball,” *The New York Times*, February 27, 2024, sec. Opinion, <https://www.nytimes.com/>; and Keith Bradsher, “How China Built BYD, Its Tesla Killer,” *The New York Times*, February 12, 2024, sec. Business, <https://www.nytimes.com/>.

40. Catherine Manning, “Technology Readiness Levels,” NASA, September 27, 2023, <https://www.nasa.gov/>.

41. George Salazar et al., “Understanding Human Readiness Levels,” in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 64, no. 1: 1765–69 (SAGE Publications, December 2020), <https://doi.org/10.1177/1071181320641427>. See also <https://www.osti.gov/biblio/1807329>.

42. Alex Hern, “Nvidia: What’s So Good About the Tech Firm’s New AI Superchip?,” *The Guardian*, March 19, 2024, sec. Business, <https://www.theguardian.com/>.

43. *Form factor* can be defined as “the physical characteristics of a device or object including its size, shape, packaging, handling, and weight.” National Institute of Standards and Technology (NIST), Glossary: “Form Factor,” accessed April 26, 2024, <https://csrc.nist.gov/>.

44. “V-JEPA: The Next Step Toward Advanced Machine Intelligence,” Meta AI, February 15, 2024, <https://ai.meta.com/>.

45. Wai Keen Vong et al., “Grounded Language Acquisition Through the Eyes and Ears of a Single Child,” *Science* 383, no. 6682 (2024): 504–11, <https://doi.org/10.1126/science.adi1374>.

46. Jeremy Hsu, "Why Giving AI a Robot Body Could Make Its 'Brain' More Human-Like," *New Scientist*, March 21, 2024, <https://www.newscientist.com/>.
47. Brian Heater, "Nvidia Enlists Humanoid Robotics' Biggest Names for New AI Platform, GR00T," TechCrunch (blog), March 18, 2024, <https://techcrunch.com/>.
48. Jeremy Hsu, "Humanoid Robots Will March into Factories and Homes in 2025," *New Scientist*, December 23, 2024, <https://www.newscientist.com/>.
49. Hsu, "Giving AI a Robot Body."
50. "The Quest to Build Robots That Look and Behave like Humans," *The Economist*, June 5, 2024, <https://www.economist.com/>.
51. Ryan McMorro and Edward White, "China Challenges the West for Driverless Car Supremacy," *Financial Times*, January 31, 2024, sec. Driverless vehicles, <https://www.ft.com/>.
52. Stephanie Palazzolo and Amir Efrati, "OpenAI Shifts AI Battleground to Software That Operates Devices, Automates Tasks," *The Information*, accessed January 21, 2025, <https://www.theinformation.com/>.
53. Murgia and Criddle, "OpenAI and Meta Ready New AI Models."
54. James O'Donnell, "Sam Altman Says Helpful Agents Are Poised to Become AI's Killer Function," *MIT Technology Review*, May 1, 2024, <https://www.technologyreview.com/>.
55. Nicholas Megaw, "Algorithms Prop Up the Market as Fretful Humans Sit Out the Uncertainty," *Financial Times*, May 14, 2023, sec. US equities, <https://www.ft.com/>; and Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (W. W. Norton, 2018), 213–15.
56. George Steer and Laurence Fletcher, "Computer-Driven Trading Firms Fret over Risks AI Poses to Their Profits," *Financial Times*, June 15, 2023, sec. Artificial intelligence, <https://www.ft.com/content/>.
57. Jonty Bloom, "Could AI 'Trading Bots' Transform the World of Investing?," BBC News, January 31, 2024, sec. Business, <https://www.bbc.com/>.
58. Scharre, *Army of None*, 213–15.
59. Scharre, *Army of None*, 216–22.
60. Lionel Sujay Vailshery, "Number of Internet of Things (IoT) Connections Worldwide from 2022 to 2023, with Forecasts from 2024 to 2033," Statista, September 11, 2024, <https://www.statista.com/>.
61. Maja Svanberg et al., "Beyond AI Exposure: Which Tasks Are Cost-Effective to Automate with Computer Vision?," SSRN Scholarly Paper January 19, 2024, <https://doi.org/10.2139/ssrn.4700751>.
62. Antony Beevor, *The Second World War* (Weidenfeld & Nicolson, 2012), 237.
63. "Human Augmentation – The Dawn of a New Paradigm," A Strategic Implications Project (UK Ministry of Defence, 2021), 34–35, <https://www.gov.uk/>.
64. "Performance-Enhancing Drugs: Know the Risks," Mayo Clinic, accessed January 21, 2025, <https://www.mayoclinic.org/>; and "Effects of Performance-Enhancing Drugs," US Anti-Doping Agency (USADA), accessed January 21, 2025, <https://www.usada.org/>.
65. James Witts, "Doping in Cycling: Everything You Need to Know," Cyclist (blog), February 9, 2023, <https://www.cyclist.co.uk/>.
66. Dave Philipps, "Navy Will Start Testing SEALs for Illicit Drug Use," *The New York Times*, September 29, 2023, sec. U.S., <https://www.nytimes.com/>.
67. Victoria Song, "The Ray-Ban Meta Smart Glasses Have Multimodal AI Now," The Verge, April 23, 2024, <https://www.theverge.com/>.

68. Cameron H. Good et al., “Sleep in the United States Military,” *Neuropsychopharmacology* 45, no. 1 (January 2020): 176–91, <https://doi.org/10.1038/s41386-019-0431-7>.
69. As we’ve seen earlier in this chapter, GenAI can also enhance communication.
70. In what senses LLMs have “knowledge” is an active point of research. For example, see Ilker Yildirim and L. A. Paul, “From Task Structures to World Models: What Do LLMs Know?,” *Trends in Cognitive Sciences* 28, no. 5 (May 1, 2024): 404–15, <https://doi.org/10.1016/j.tics.2024.02.008>.
71. Christian Terwiesch, “Would Chat GPT3 Get a Wharton MBA? A Prediction Based on Its Performance in the Operations Management Course,” Mack Institute for Innovation Management at the Wharton School, University of Pennsylvania, 2023, <https://mackinstitute.wharton.upenn.edu/>.
72. Keumars Afifi-Sabet, “The GPT to Rule Them All: Training for One Trillion Parameter Model Backed by Intel and US Government Has Just Begun,” TechRadar, November 20, 2023, <https://www.techradar.com/>.
73. “AI Models Can Improve Corner-Kick Tactics,” *The Economist*, March 19, 2024, <https://www.economist.com/>.
74. Dev Dash et al., “How Well Do Large Language Models Support Clinician Information Needs?,” HAI, Stanford University Human-Centered Artificial Intelligence, March 31, 2023, <https://hai.stanford.edu/>.
75. “What Tennis Reveals about AI’s Impact on Human Behaviour,” *The Economist*, February 15, 2024, <https://www.economist.com/>.
76. Michael C. Horowitz and Lauren Kahn, “Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts” (arXiv, June 28, 2023), <https://doi.org/10.48550/arXiv.2306.16507>.
77. For an application to USSTRATCOM, see, for example, Nicholas D. Wright, *Who Will We—and They—Be on Day 30 or Day 1000 in Deterrence?*, Intelligent Biology (forthcoming), <https://www.intelligentbiology.co.uk/publications>.
78. Michael Le Page, “First Gene-Edited Meat Will Come from Disease-Proof CRISPR Pigs,” *New Scientist*, February 23, 2024, <https://www.newscientist.com/>.
79. Smriti Mallapaty, “Disgraced CRISPR-Baby Scientist’s ‘Publicity Stunt’ Frustrates Researchers,” *Nature* 614, no. 7949 (February 2023): 599–600, <https://doi.org/10.1038/d41586-023-00382-w>.
80. “MHRA Authorises World-First Gene Therapy That Aims to Cure Sickle-Cell Disease and Transfusion-Dependent β -Thalassemia,” GOV.UK, November 16, 2023, <https://www.gov.uk/>.
81. Tejal Patwardhan et al., “Building an Early Warning System for LLM-Aided Biological Threat Creation,” OpenAI, January 31, 2024, <https://openai.com/>.
82. “Executive Summary,” The Future War Strategy and Technology Conference, Wilton Park, West Sussex, October 9–11, 2023, <https://www.wiltonpark.org.uk/>.
83. Joseph Clark, “DOD Chemical, Biological Defense Program Adapts to Emerging Threats as It Marks 30-Year Anniversary,” DOD News, November 30, 2023, <https://www.defense.gov/>.

Chapter 9

Physiologic Intelligence (PHYSIOINT) **A Framework for Assessing Warfighter Sustainment and** **Performance Improvement Using Physiological and** **Neurobiological Signals**

William D. Casebeer, HRL Laboratories

Abstract

Widespread collection using wearable sensors and a growing body of experimental data demonstrate the promise of being able to assess and forecast performance for warfighters on important tasks. These results highlight the promise of physiologic intelligence, or PHYSIOINT: harvesting and analyzing physiological and neurobiological data for the purpose of drawing assessments or conclusions about Soldiers, Marines, Sailors, Airmen, and Guardians. For blue forces, PHYSIOINT can be used to assess readiness, improve sleep and nutrition regimens, identify the efficacy of training and operations, and perhaps even “close the loop” in real time to improve training or performance outcomes using this data on the fly. For red forces, physiologic intelligence can be used to assess readiness and provide more detailed psychological and combat assessment useful for everything ranging from order of battle and status of forces to key leader engagements. While we must exercise caution when drawing conclusions from physiologic data (due primarily to task-induced and individual variability in the relationship between sensed data and hidden states or performance outcomes), PHYSIOINT nonetheless promises innovative insights and findings for improving performance among allied service members and better characterizing the strengths and vulnerabilities of adversary forces. Keeping the ethical, legal, and social implications (ELSI) of PHYSIOINT at the fore will allow us to develop praiseworthy uses of these technologies to deter aggression and keep the peace.

Since the discovery of Fitts' Law by Paul Fitts in 1954, human factors engineers and allied professionals such as psychologists and cognitive scientists have sought to correlate warfighter behavior with variables

that can be monitored and tracked over time.¹ Fitts showed that we can design better displays for Soldier tools if we understand how long it takes a person to reach a button or knob; his work correlated predictions of human movement with observable variables such as the width of and distance to a target. For Fitts, the things we can sense today routinely or with relatively low-cost equipment and methods would have been incredible. Wearable sensors that many of us have on our wrists can more reliably track heart rate, heart rate variability, blood oxygenation levels, and accelerometer and gyrometer-measured movement patterns than sophisticated lab equipment from Fitts' time.

In much the same way that Fitts' work has been useful in helping us design effective interfaces for soldiers interacting with computers and robots, contemporary scientists have discovered relationships between observable and sensible variables and performance-relevant outcomes, such as ability to fly an airplane well or stay awake while on swing shift accomplishing military intelligence analysis. In this chapter, I discuss the concept of physiologic intelligence, highlight some of its uses, and discuss notes, warnings, and cautions we must observe if we are to reliably use this data to improve the performance of our own and allied forces and understand the hidden weaknesses of adversary forces.

What Makes an “INT”?

Intelligence analysts often use technical means of collection to gather the information they will fuse to make judgments about everything ranging from an adversary's strategic intention to the disposition of their order of battle. These categories of intelligence data are classically grouped into “INTs,” according to the unique methods used to collect the data, the novel methods used to analyze it, and the specific insights or assessments that can be gained by doing so. For example, “SIGINT” stands for SIGnals INTelligence and highlights that we will use novel sensors (such as radio frequency detectors) and unique analytic methods (such as Fourier decomposition to break down a radio frequency signal into component parts) to draw novel conclusions (such as saying that a radio frequency signal corresponds to an emergency beacon emitted by a downed adversary aircraft). While discussion of SIGINT, communications intelligence (COMINT), human intelligence (HUMINT), and the other forms of intelligence collection and analysis is beyond the scope of this chapter, I offer this example to make a homely point: The sensors

used to collect physiologic data—data about the operation and activity of the brain and body—and the methods used to analyze the data and mine it for insight likely qualify it for inclusion in the pantheon of INTs.²

PHYSIOINT leverages data that is often otherwise neglected, applies traditional signal processing techniques and purpose-built and unique methods to that data to make sense of it, and allows analysts or engineers to draw conclusions we could not otherwise reach. It qualifies as a unique intelligence method, hence the PHYSIOINT moniker.

PHYSIOINT Reaching a Tipping Point

While PHYSIOINT has demonstrated promise for multiple decades, we are only now reaching a break point where the data has become easier to collect, our analytic methods are maturing, and it is possible to apply PHYSIOINT to militarily relevant operational performance and assessment problems.

On the sensor side, some types of physiologic collection instruments are almost ubiquitous. For instance, since their introduction in 2015, about 230 million Apple watches have been sold as of mid-2023.³ Other devices such as Fitbits and Oura rings that collect similar data (heart rate, heart rate variability, blood oxygenation levels, some types of movement data, etc.) are similarly growing in usage. Worldwide shipments of wearable devices reached at least 504 million units in 2023, showing steady growth.

In laboratory settings, there has been an explosion of lower-cost sensors and methods to enable us to ascertain the impact of the state of the body and the brain on military performance. These include developments in lower-cost electroencephalogram (EEG) technology (to sense electrical activity noninvasively on the scalp, which correlates with brain states), eye tracking systems, pupillometry systems to measure pupil dilation, galvanic skin response systems to measure sweat conductance, higher-quality heart rate and blood pressure monitors, and the like.

So, physiology sensors are prolific; likewise, growing experimental evidence confirms at least some correlation between these measurable variables and military-performance-related cognitive and body states, such as arousal, fatigue, cognitive burden, and situational awareness. In some cases, these results have been usefully applied by academic and industry research labs to improve warfighter training and readiness. Finally, the insights offered by these data collection and analytic

techniques are unique. They can allow us access to otherwise hidden variables such as cognitive burden that until now have been assessed after the fact (“post hoc”) or with imperfect tools linked to self-report (imperfect because our ability to report on the internal states of our brains and bodies—called “interoception”—varies and in some cases is simply not reliable).

Arguably, these developments since Fitts have enabled us to reach a PHYSIOINT tipping or break point. With the right investments in sensors, analytic methods, and assessment techniques, I believe we can harness PHYSIOINT to gain unique insights into training and performance improvements for our own forces and insight into the status of and how we might degrade the performance of adversary military units.

Summarizing the Literature

The literature in this area has grown enough that summarizing it in a single chapter is problematic. However, the following table outlines some sensors, assessment methods, and laboratory experiments that highlight the usefulness of these physiologic intelligence methods for the PHYSIOINT performance-characterization-and-improvement enterprise.

This table should make apparent the possibilities for PHYSIOINT. At the individual and team performance level, many pieces of data that we can collect with our physiological or closely related sensors can be analyzed to assess and forecast military training and performance-relevant states. Whether fatigue is causing a warfighter to lose situational awareness, an intelligence analyst is facing task demands causing them to burn through their cognitive reserve, or military team members are demonstrating the kinds of synchronicity among their heartbeats indicative of close attention to each other’s states and tasks are all, in principle, assessable.

Table 9.1. Military performance–relevant states—their raw data sources, analysis methods, and relevant previous work: a bastardized history

<i>Performance-Relevant State</i>	<i>Raw Signals to Compute State</i>	<i>Computation of State</i>	<i>Justification & Some Previous Work</i>
Individual cognitive reserve	Functional near-infrared spectroscopy (fNIRS), EEG, pupillometry	Existing models from multiple academic and industry labs	Cognitive reserve reflects an individual’s capacity to process information and perform work. ⁴

Table 9.1 (continued)

<i>Performance-Relevant State</i>	<i>Raw Signals to Compute State</i>	<i>Computation of State</i>	<i>Justification & Some Previous Work</i>
Cognitive workload	EEG, fNIRS, Galvanic Skin Response (GSR), pupillometry	Computation of power bands for Task Load Index ratio (EEG)	Signatures evaluated for performance in measuring cognitive load by industry labs such as Riverside Research, HRL Labs, and Charles River Analytics
Attention / Saliency	EEG, mouse scrolls and clicks, EEG P300s	P300 classification, computation of EEG power bands	In several projects, this signature was used to find moments of recognition (such as recognizing objects in intelligence imagery). ⁵
Aggregate cognitive reserve	fNIRS, EEG, pupillometry, GSR	Task-state weighted averages, graph analytics, and synchronicity model	Aggregate cognitive reserve sums across team members to identify potentiation and attenuation effects resulting from team dynamics ⁶
Situational awareness	Eye tracking	Gaze sample entropy, dwell time, and Markov entropy	Gaze sample entropy was used to measure expertise in software reverse engineering by HRL Labs.
Aggregate situational awareness	Eye tracking	Task-state weighted averages & graph analytics	Aggregate situational awareness indicates to the sum and interactions of awareness across team. ⁷
Mind wandering	Eye tracking, pupillometry	Gaze velocity computation, fixation computation	Used to track mind-wandering by labs such as HRL Labs, Riverside Research, and Lockheed Martin Advanced Technology Labs
Generalized task state	Verbal communications, computer inputs	State space reduction	Reduced task state space minimizes search space and ensures task-generalizability. ⁸
Aggregate EEG entropy	EEG	Neurophysiologic synchrony models	EEG-derived entropy measure predicts expert team performance. ⁹
Individual pro-sociality	Verbal communications	Fine-tuned large language model (LLM)	Determining if a person has good social cohesion within a group ¹⁰
Aggregate pro-sociality	Verbal communications	Fine-tuned LLM	Quantifies team cohesion, i.e., are the social interactions within the team overall positive or negative ¹¹

Table 9.1 (continued)

<i>Performance-Relevant State</i>	<i>Raw Signals to Compute State</i>	<i>Computation of State</i>	<i>Justification & Some Previous Work</i>
Vocal properties	Verbal communications	Model incorporating speech properties	Vocal properties furnish insight into individual and team cohesion and readiness. ¹²
Conversational repair attempts	Verbal communications	Fine-tuned LLM	Verbal phrases/statements to rebuild/repair trust in a conversation ¹³
Individual fatigue	Heart rate, heart rate variability (HRV)	Regression model	Measuring individual fatigue refines individual performance baseline. ¹⁴
Aggregate fatigue	Heart rate, HRV	Regression model	Measuring individual fatigue refines team performance baseline. ¹⁵
Team-agnostic physiology synchronicity	Heart rate, EEG	Shannon entropy	Determining whether characteristics independent of teammates are synchronized ¹⁶

Applying PHYSIOINT

The agile use of physiologic intelligence can help assess and improve the training and performance of US and allied forces. For example, the US Air Force Research Laboratory, serving the US Air Force and US Space Force, has used a long-standing “quantified warrior” framework to think about the relationship between what can be sensed, how that data can be assessed, and how that can in turn augment warfighter performance. For example, keeping in mind the previous table, we might be able to use electroencephalograms to sense brain wave patterns relatively easily. From those patterns, by focusing on the positive wave of electricity that courses over the scalp about 300 milliseconds after our bodies and brains recognized a novel object in a photograph, we might be able to assess when an analyst has seen—faster than they may be able to consciously report—something new in a photograph. We might then be able to augment the performance of an analyst by setting aside all those photos that show a P300 signal, so the analyst can spend their quality time and heartbeats with those photographs that likely contain something new (say, an enemy tank in synthetic aperture radar imagery).

In fact, what I have just described is an older experiment and proof of concept accomplished at DARPA in the Neurotechnology for Intelligence Analysts program that I managed while there. Numerous other

contemporary examples abound, such as Riverside Research, Lockheed Martin ATL, Advanced Brain Monitoring, Mind Research Network, QUASAR, Charles River Analytics, and other industry and academic labs (e.g., MIT, USC, Georgia Tech, etc.) too numerous to mention. From this body of work, we can draw some initial conclusions that physiologic intelligence can be useful for numerous applications. These include warfighter state assessment (Losing focus? Too tired? In need of an automation or autonomous algorithm “assist”?), performance improvement (dynamic adaptation to team or individual state, assistive algorithms to improve team performance, etc.), and adaptive warfighter training technology (e.g., by designing scenarios that stress-test the unique physiologic configurations of one team rather than mass-producing educational interventions).

Conversely, these same data, analytic methods, and performance-relevant assessments can be used to understand adversary or red forces and characterize what they are like under the hood. For instance, the mere presence of a platoon in a marshalling area does not necessarily indicate they are fit to fight; if we can, at a distance with sensors or by monitoring wearable technologies, determine that most of those soldiers are sleep-deprived, prone to react poorly to stress, or likely to defect from their unit, our operational posture toward that platoon would be very different.

PHYSIOINT complements the other forms of intelligence we use to assess order of battle, red force readiness, and actual or potential adversary strategic, operational, and tactical posture, or intent. For example, some pointed physiologic data collection may set the stage for success in key leader engagements. If I understand that someone will perceive me as a threat (and hence activate neurobiology and physiology linked to the flight or fight response), I can watch for signs of sympathetic nervous system activation and use those to consider a strategy for fruitful engagement and how to tactically adapt my interactions on the fly (as people who are good with influencing or persuading others already do naturally).

Limits of Physiological and Neurobiological Assessments

Like all forms of data collection, the inferences you can justifiably make from any given data to any given conclusion depend on other

factors or variables. For instance, while having a static beat-to-beat heart interval can indicate an inability to adapt to stress well, it could also be a function of excessive caffeine consumption. A higher heart rate could reflect cardiac exertion or a lower basal cardiac level of fitness.

In general, two major sources of variability that will constrain the inferences we can make from physiologic data are (1) individual variability and (2) task-related variability. While you and I are similar because we are both people, we are different in, for example, the finer details of the physiology of our stress response—that is individual variability. Task-induced variability highlights that our work environments interact with our brains and bodies in ways that make it hard to straightforwardly infer a complicated judgment about mental states, for instance, from a single piece of physiological data. My eyes might be dilated above some mean measurement, for example, because I find you a fascinating conversationalist or, instead, because I am in a low-light setting.

Fortunately, these sources of variability can be addressed with several techniques. First, we can acknowledge the limits of our models and use them only when valid (as we already do with other INTs). Second, we can use model libraries to put together predictive models that account for major sources of (say) individual variability. We can then choose from that model library according to a baselining session with the warfighter (“we chose this workload model from the library because our three-minute testing situation in virtual reality indicates it is a best fit for him”). Third, we can leverage machine learning techniques and large datasets to attempt to find novel relationships between variables that we might miss with traditional or first-order statistics or with small subject numbers (“small N’s”). It is highly likely that for some complexes of variables the relationships will not be linear or one-to-one; Fitts’ Law is an achievement, and we will likely discover some equivalents to it throughout PHYSIOINT, but not in many cases.

Keeping the Ethical, Legal, and Social Implications in Mind

PHYSIOINT presents unique ethical, legal, and social implications, as almost all breakthrough technologies do. In much the same way that some forms of intelligence collection challenge our notions of privacy, physiologic data collection and analysis can understandably generate concerns about cognitive privacy and liberty. While a com-

prehensive ethical, legal, and social implications analysis cannot be done in this chapter, the general framework we use to structure our thinking about the moral implications of military technology likely also applies to physiological and neurobiological intelligence. By keeping in mind the three primary impacts of our PHYSIOINT technology, we can push our technologies in directions that are morally praiseworthy or at least morally permissible. The first of these is character—what impact does this technology have on my flourishing, and does it help me develop good habits? The second is consent—does this technology respect me as a decision-maker by treating me as an end, not merely as a means, worthy of respect and dignity? The third is consequences—does this technology produce good outcomes and increase the net store of happiness when used?¹⁷

While these technologies will pose ethical questions and ask us to make value trade-offs, in general the questions they ask will be a lot like the ones we have asked as we have developed and deployed cars, vaccines, communications satellites, radar systems, and the like. We as people developed and fielded those technologies and need to analyze the difficult questions that arise when we do so, perhaps changing the design of a fielded system as a result.

Conclusion

We are entering a unique period in our history where more data is being collected about us in general and where analytic techniques are allowing us to make sense of that data and use it fruitfully. Widespread collection using wearable sensors and a growing body of experimental data demonstrate the promise of being able to assess and forecast performance for warfighters on significant tasks. These results highlight the promise of physiologic intelligence, harvesting and analyzing physiological and neurobiological data for the purpose of drawing assessments or conclusions about Soldiers, Marines, Sailors, Airmen, and Guardians. For us and our allies, we can use PHYSIOINT to keep our forces fitter and improve training and operational efficacy. For actual and potential adversaries, we can employ it to assess readiness and provide more detailed psychological and combat assessment useful for everything from order of battle and status of forces to key leader engagements. However, we must exercise caution when drawing conclusions from physiologic data, due primarily to task-induced and

individual variability in the relationship between sensed data and hidden states or performance outcomes.

But PHYSIOINT nonetheless promises innovative insights and findings for improving the performance of allied service members and better characterizing the strengths and vulnerabilities of adversary forces. We can use the right data analysis techniques, PHYSIOINT strategies, and machine learning to help us exercise due caution when incorporating physiology into training and operations. Ultimately, we must keep the ethical, legal, and social implications of PHYSIOINT foremost as we develop PHYSIOINT technology. Doing so will enable us to develop praiseworthy uses of these technologies to deter aggression and keep the peace and to take care of our warfighters when they return home and reintegrate into civilian society.¹⁸

Acknowledgments

My thanks to the Joint Staff J-39 Strategic Multilevel Analysis team for feedback. I am deeply indebted to my current lab members, such as Dr. David Huberdeau, Dr. Jeff Cody, Dr. Joey Salisbury, and Mr. Taylor Moss, for assembling the table of physiologic signals and keeping abreast of current work. Thanks also to collaborators in national-security-centered PHYSIOINT projects in the past, including the labs and teams mentioned in the text, and co-authors and collaborators, such as Dr. Bart Russell, Dr. Pat Churchland, and Dr. Matthias Ziegler.

Notes

1. For a discussion of Fitts' Law, see, for example, Stephan Guastello, *Human Factors Engineering and Ergonomics: A Systems Approach* (CRC Press, 2014), 158–60.

2. For a discussion of the traditional INTs, see Robert M. Clark, *Intelligence Collection: A Systems Approach* (CQ Press, 2013).

3. See, for instance, IDC's Worldwide Wearables Market forecast, accessed January 2024, <https://www.idc.com/>.

4. See Robert R. Whelan, "Neuroimaging of Cognitive Load in Instructional Multimedia," *Educational Research Review* 2, no. 1 (January 2007): 1–12, <https://doi.org/10.1016/j.edurev.2006.11.001>; Mathieu Figeys et al., "Transcranial Direct Current Stimulation over the Right Dorsolateral Prefrontal Cortex Increases Oxyhemoglobin Concentration and Cognitive Performance Dependent on Cognitive Load," *Behavioural Brain Research* 443 (April 2023): 114343, <https://doi.org/10.1016/j.bbr.2023.114343>; Moona Mazher et al., "An EEG-Based Cognitive Load Assessment in Multimedia Learning Using Feature Extraction and Partial Directed Coherence," *IEEE Access* 5 (2017): 14819–29, <https://doi.org/10.1109/ACCESS.2017.2731784>; Andrew T. Duchowski et al., "The Index of Pupillary Activity: Measuring Cognitive Load vis-à-vis Task Difficulty with Pupil Oscillation," in *CHI 18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery, April 2018),

Paper no. 282, 1–13, <https://doi.org/10.1145/3173574.3173856>; Matthias Scheutz et al., “Estimating Systemic Cognitive States from a Mixture of Physiological and Brain Signals,” *Topics in Cognitive Science* 16, no. 3 (2023): 485–526, <https://doi.org/10.1111/tops.12669>; and Ayca Aygun et al., “Investigating Methods for Cognitive Workload Estimation for Assistive Robots,” *Sensors* 22, no. 18 (January 2022): 6834, <https://doi.org/10.3390/s22186834>.

5. See Robbin Miranda et al., “DARPA-Funded Efforts in the Development of Novel Brain–Computer Interface Technologies,” *Journal of Neuroscience Methods* 244 (April 2015): 52–67, <https://doi.org/10.1016/j.jneumeth.2014.07.019>.

6. References here include Diego A. Reinerio et al., “Inter-Brain Synchrony in Teams Predicts Collective Performance,” *Social Cognitive and Affective Neuroscience* 16, no. 1–2 (January–February 2021): 43–57, <https://doi.org/10.1093/scan/nsaa135>; and Ronald H. Stevens et al., “Cognitive Neurophysiologic Synchronies: What Can They Contribute to the Study of Teamwork?,” *Human Factors* 54, no. 4 (August 2012): 489–502, <https://doi.org/10.1177/0018720811427296>.

7. See, for example, Eduardo Salas et al., “Situation Awareness in Team Performance: Implications for Measurement and Training,” in *Situational Awareness*, ed. Eduardo Salas (Routledge, 2017): 63–76, <https://doi.org/10.4324/9781315087924-5>.

8. Muhammad Zubair Rehman et al., “A Novel State Space Reduction Algorithm for Team Formation in Social Networks,” *PLOS ONE* 16, no. 12 (December 2021): e0259786, <https://doi.org/10.1371/journal.pone.0259786>.

9. Stevens et al., “Cognitive Neurophysiologic Synchronies.”

10. Benjamin E. Hilbig et al., “Personality and Prosocial Behavior: Linking Basic Traits and Social Value Orientations,” *Journal of Personality and Social Psychology* 107, no. 3 (2014): 529–39, <https://doi.org/10.1037/a0036074>.

11. See Gita Sukthankar and Katia Sycara, “Activity Recognition for Dynamic Multi-Agent Teams,” *ACM Transactions on Intelligent Systems and Technology* 3, no. 1 (2011): 18:1–18:24, <https://doi.org/10.1145/2036264.2036282>; Shengnan Hu and Gita Sukthankar, “Predicting Team Performance with Spatial Temporal Graph Convolutional Networks,” in *2022 26th International Conference on Pattern Recognition (ICPR)*, August 2022, 2342–48, <https://doi.org/10.1109/ICPR56361.2022.9956457>; Albert Chai et al., “Applying Graph Theory to Examine the Dynamics of Student Discussions in Small-Group Learning,” *CBE—Life Sciences Education* 18, no. 2 (2019): ar29, <https://doi.org/10.1187/cbe.18-11-0222>; and Ling Zhao et al., “T-GCN: A Temporal Graph Convolutional Network for Traffic Prediction,” in *IEEE Transactions on Intelligent Transportation Systems* 21, no. 9 (September 2020): 3848–58, <https://doi.org/10.1109/TITS.2019.2935152>.

12. Christine Nussbaum et al., “Contributions of Fundamental Frequency and Timbre to Vocal Emotion Perception and Their Electrophysiological Correlates,” *Social Cognitive and Affective Neuroscience* 17, no. 12 (2022): 1145–54, <https://doi.org/10.1093/scan/nsac033>.

13. Matthew Marge et al., “Spoken Language Interaction with Robots: Recommendations for Future Research,” *Computer Speech and Language* 71 (2022): 101255, <https://doi.org/10.1016/j.csl.2021.101255>.

14. Neusa R. Adão Martins et al., “Fatigue Monitoring Through Wearables: A State-of-the-Art Review,” *Frontiers in Physiology* 12 (2021), <https://doi.org/10.3389/fphys.2021.790292>.

15. Martins et al.

16. Roger D. Dias et al., “Physiological Synchronization and Entropy as Measures of Team Cognitive Load,” *Journal of Biomedical Informatics* 96 (August 2019): 103250, <https://doi.org/10.1016/j.jbi.2019.103250>.

17. See Myers et al., “The Core Values: Framing and Resolving Ethical Issues for the Air Force,” *Air and Space Power Journal* 11, no. 1 (Spring 1997): 38–53, <https://www.airuniversity.af.edu/>; William D. Casebeer, *Natural Ethical Facts: Evolution, Connectionism, and Moral Cognition* (MIT Press, 2003); Patricia S. Churchland, *Braintrust: What Neuroscience Tells Us About Morality* (Princeton University Press, 2011); and William D. Casebeer, “Building an Artificial Conscience: Prospects for Morally Autonomous Artificial Intelligence,” in *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations*, ed. Yvonne R. Masakowski (Emerald Publishing, 2020), 81–94, <https://typeset.io/>.

18. William D. Casebeer, “Ethics and the Biologized Battlefield: Moral Issues in 21st-Century Conflict,” in *Bio-Inspired Innovation and National Security*, ed. Robert E. Armstrong et al. (Published for the Center for Technology and National Security Policy by National Defense University Press, 2010), 293–304, <https://ndupress.ndu.edu/>. Thoughts in this article have been informed by DARPA programs and seedlings I was honored to be the program manager for, including Narrative Networks, Neurotechnology for Intelligence Analysts, Strategic Social Interaction Modules, Education Dominance, Accelerated Learning, Low-Cost EEG for Crowd-Sourced Neuroscience, Veteran’s Education with the Digital Tutor, the Young Faculty Award, Neuroadaptive Feedback for Stroke Rehabilitation, and Mirror-Imaging Detector for Analyzing Surprise.

Chapter 10

Making Sense of Wearable Sensing

A Principled Approach to Quantifying Human Physiological, Cognitive, and Behavioral Attributes

*David Huberdeau, Artificial Intelligence/Machine Learning
Engineer, Riverside Research Institute*

Abstract

Wearable technology and advanced analytics are transforming military operations through the precise quantification of human attributes. This topic is relevant for the defense and intelligence sectors, as it is critical to accurately assess warfighter readiness, health status, and performance capabilities. Unlike consumer markets where some level of measurement error might be tolerated, the military often demands exacting standards of accuracy, precision, and validation akin to those in the medical device industry. This necessity arises from the unique challenges of military applications, where even less directly observable attributes like cognitive readiness or psychological resilience—critical under operational stress and environmental factors—must be quantified reliably. Wearable technologies equipped with artificial intelligence and machine learning algorithms are introduced as possible breakthrough tools for achieving high reliability in measuring a wide spectrum of human attributes under stringent military standards. These advancements promise to enhance personalized training, rapid health diagnostics, and predictive analytics, presenting a new frontier in warfighter optimization.

Introduction

For decades, there has been growing interest in the measurement and quantification of human attributes, including health status, performance estimates, readiness levels, activity tracking, and more. Potential applications of human quantification are particularly relevant in the defense and intelligence communities, where insight into indi-

vidualized human attributes can have significant impacts on mission effectiveness, efficiency, and other factors critical to national security.

Adoption of techniques and technologies for individualized attribute quantification pose unique challenges in the defense and intelligence sectors as compared to other commercial markets. While human attribute quantification approaches for consumer recreational markets may tolerate a degree of measurement and estimation error,¹ public sector applications may require greater accuracy and precision if their data is to be used for tactical decision-making.

Furthermore, there is an expanding need for analyses and insights into human attributes that are typically not directly observable but that nevertheless can provide critical insights into the status and potential effectiveness of personnel, such as cognitive readiness.² Hidden attributes such as these, so called because they are generally not directly observable, are particularly pertinent for military applications. Operational stressors and environmental factors can have significant impacts on an individual's mindset,³ and thus insight into cognitive readiness could be invaluable in a military setting. However, estimating and quantifying such attributes can be ambiguous; they are generally context-dependent, making them particularly challenging to obtain.

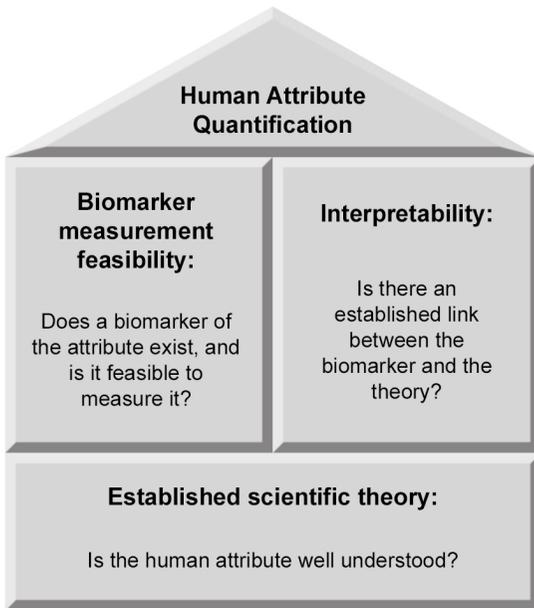
Advancements in wearable technology, combined with artificial intelligence (AI) and machine learning (ML) algorithms, are poised to offer significant breakthroughs in both the reliability of human attribute quantification and the variety of attributes available to measure under the exacting standards required of military and intelligence applications. These emerging technologies will enable the real-time monitoring and analysis of a wide range of physiological and environmental data, facilitating personalized training programs, rapid health diagnostics, and predictive analytics.

This chapter provides a framework for conceptualizing the challenges and emerging possibilities in the exciting field of human attribute quantification for military applications. Drawing on the more established area of medical applications illustrates the challenges inherent in seeking greater reliability and variety in this field and enables determining the implications for defense and intelligence.

Obtaining Useful Metrics of Human Attributes by Asking Better Questions

Typically, one seeks to quantify human attributes to answer a question about a person or group of people. What is my physical fitness level? What is my risk of cardiovascular disease? Is this combat team prepared to face the challenges of a new operational environment? With the right question in hand, it becomes possible to craft a strategy to obtain interpretable, useful metrics of individualized human attributes.

For any question that the quantification of human attributes might answer, it is critical that the attribute of interest be grounded in well-established scientific theory, that indicators of the desired attribute exist and are feasible to obtain, and that those indicators be interpretable within the established theory (fig. 10.1). In this regard, it is



useful to consider the endeavor of quantifying human attributes as akin to developing biomarkers for human health. Biomarkers in medicine serve as leading indicators of a typical or pathological process or as trackers of an intervention regarding a clinical outcome.⁴ As in biomarker development for health outcomes, quantification of human attributes for any other purpose requires scientific understanding, va-

Figure 10.1. Scientific theory, feasible biomarkers, and interpretability form the key building blocks supporting the ability to infer human attributes.

lidity of measurements, and interpretability of those measurements with respect to the established theory. Human attribute quantification

may be considered a generalization of medical biomarker development, and thus this chapter adopts that terminology to emphasize these important parallels.

To illustrate these principles, consider the individual assessment of coronary heart disease risk. Mechanisms of coronary heart disease are well understood.⁵ For instance, plaque accumulation in the coronary artery eventually leads to complete arterial blockage and myocardial infarction.⁶ As the arterial blockage progresses, physiological indicators emerge, such as chronic high blood pressure and elevated heart rate. Furthermore, risk factors preceding these signs that forecast plaque development include high cholesterol, body mass index in the overweight or higher range, and a chronic sedentary lifestyle.⁷ Measurable behavioral and physiological biomarkers exist that are interpretable with respect to this mechanistic understanding and these risk factors. Direct measurement of physical activity, heart rate, blood pressure, and other physiological and behavioral indicators can individually or together quantify cardiovascular disease risk.⁸ Critically, each of these quantities can be measured individually using existing commercially available products. This example highlights a case that fits the bill for individualized human attribute quantification—a well-established theory, measurable biomarkers, and a framework for interpreting the biomarkers within the theory.

The insistence that successfully quantifying human attributes require these criteria may at first appear needlessly conservative. For instance, if seeking to quantify steps taken in a day, it hardly seems necessary to consider the science of walking. Furthermore, the interpretation of individual steps to total daily step count appears trivial—just add them up. However, the central theme here is that even in cases where the linkage among these criteria appears trivial, the pattern still holds. For more complicated attributes or those that have eluded successful implementation to date, these criteria may serve as a guide for successful future developments. It is furthermore worth considering that there may not exist any attributes whose quantification is truly trivial. Even for step counting, important questions emerge. What exactly constitutes a step? Are all steps equal with respect to the purpose for measuring them in the first place? For instance, if the purpose for measuring step count is to obtain a proxy for passive daily activity⁹ and the sensor for measuring is a standard pedometer,¹⁰ the type of step and context in which someone took it may be practically irrelevant. On the other

hand, if the purpose for step counting is to evaluate recovery from a stroke,¹¹ the nature of each step may be critically important.

This landscape brings challenges. Significant hurdles exist when attempting to estimate attributes that are less well understood and for which suitable biomarkers have not yet been developed or discovered. Unfortunately, many attributes of interest for the Department of Defense and intelligence community fall in this category. Relevant attributes in these domains, such as appropriateness for mission roles, situational awareness,¹² or cognitive workload,¹³ lack clear and unambiguous biomarkers that link the attribute to an established theory. Another factor is that they might require measurements that are not always feasible in an operational setting, such as cumbersome assessments of brain activity.¹⁴

However, there are pathways to overcome these challenges, even for attributes that are currently out of reach. On the one hand, one could focus on attributes that already meet the criteria of being scientifically grounded, measurable, and interpretable. This approach leverages the existing technological and scientific landscape to its maximum potential. Alternatively, limiting the scope of inference can yield more targeted and interpretable insights from available measurements; that is, one could gain some insight into a desired attribute even if a full accounting is not currently feasible. Promisingly, new opportunities will emerge as technological advancements enhance our capability to measure human physiology and behavior, scientific knowledge deepens through the formulation of theories for relevant attributes, and mechanisms or biomarkers for key traits are discovered. Wearable devices paired with artificial intelligence algorithms that measure rich human experiences, behaviors, and situational contexts are promising capabilities on the horizon. The pairing of these highly specific measurements and inferences of context with physiological measurements is likely to be a key development toward achieving greater insight and unlocking long-desired inferential capabilities of human attributes.

This chapter surveys the successes, current challenges, and future trends of the pursuit to quantify human traits. The intention is to develop a perspective that gives the reader a framework to understand and assess the current state of the field and to interpret future developments, especially in the defense and intelligence communities. The chapter first discusses some success stories and examples of attributes well suited to quantification with current understanding and technology. It next

discusses attributes of potential interest that may have a ways to go before implementation. It concludes with a forecast and discussion of developments on the horizon and what capabilities these might unlock.

Quantifying Human Attributes Through Wearable Sensing Technology

Attributes currently suited to quantification have biomarkers that are interpretable within established scientific theory. Some human attributes that are relevant and significant to the defense and intelligence community are well suited to quantification through wearable sensing technology. These attributes are scientifically well understood and have known biomarkers that are readily interpretable. Daily physical activity and sleep quality are two excellent examples of human attributes that are well suited to quantification, have enjoyed measures of success through widespread application in extant consumer technologies, and are mission-relevant.

Daily Physical Activity

Higher levels of daily physical activity are correlated with a reduced risk for a host of conditions, including cardiovascular disease, stroke, and diabetes.¹⁵ Furthermore, daily physical activity predicts physical fitness levels,¹⁶ which in turn can relate to mission readiness and combat effectiveness. Mechanisms accounting for the relationship between daily physical activity and physical fitness include vasodilation and the promotion of new vasculature,¹⁷ adaptive heart hypertrophy,¹⁸ and cardiac mitochondrial biogenesis.¹⁹ Measuring and tracking individual daily physical activity can therefore be beneficial for gaining insight into one's general physical fitness and combat readiness.

Furthermore, recording daily physical activity and making this data individually available has been found to increase individual physical activity.²⁰ The science behind physical activity and its relation to physical fitness is thus well established, and the types of measurements of daily physical activity and how those measurements can be interpreted with respect to the science is clear. This attribute is thus suitable as a candidate for meaningful and useful individualized quantification.

Unsurprisingly, modern wearables like fitness trackers and smart-watches are adept at measuring physical activity. They can track the type of activity, amount of time engaged in the activity or distance travelled,

heart rate during the activity, and estimates of calories expended. These quantities are further directly interpretable with respect to the question of physical fitness. More physical activity correlates with greater fitness levels. The measurements are clear and interpretable, and the insights are directly actionable.

Sleep Quality and Quantity

Obtaining consistent, high-quality sleep is critical not only for the mission but also for long-term health and quality of life factors.²¹ Sleeping during consistent hours from day to day, sleeping a sufficient number of hours consistently, and practicing good sleep hygiene—to include avoiding sleep-impairing substances like caffeine and light exposure prior to sleep—have been shown to improve sleep quality.²² However, it can be difficult for individuals to accurately judge their own sleep patterns.²³ It can thus be beneficial for mission readiness and individual health to track one's sleep with respect to duration, quality, and stages to gain insight into one's sleep patterns. Doing so can motivate behavioral changes to improve sleep hygiene.²⁴

Wearable devices can monitor sleep patterns, including the duration of sleep and the time spent in different sleep stages.²⁵ Some devices also provide insights into sleep trends and offer suggestions for improving sleep hygiene. For sleep health, the purpose or question is clear—ascertaining whether an individual obtains sufficient sleep—the science is well understood, the measurements are available, and the interpretation of those measurements is defined. Quantifying sleep duration and quality is thus a suitable attribute for successful quantification, and it is unsurprising that modern wearables have focused on this attribute with success.

Physical activity and sleep are just two attributes well suited to quantification. In each case the question and purpose is clear. Quantifying physical activity or sleep can directly inform one's status with respect to meaningful attributes of interest and with relevance to health and wellness. The attributes are also well understood scientifically. Physical activity and sleep quality are each strongly related to numerous health and wellness outcomes. Both are readily measurable through existing technology, and those measurements are readily interpretable with respect to the science and the motivating question.

Measuring and Interpreting Human Attributes Through Wearable Sensing Technology

Not all human attributes are currently well suited for measurement and quantification due to the challenges of interpretability or scientific understanding. Attributes for which there are sound needs, such as measuring cognitive status or an individual's situational awareness, are desirable, but current technology and methods do not always meet the bar for their effective measurement. For instance, one might ask, "Can this person accomplish this task at this time?" Some possible ways to approach this question are to further ask whether the individual is mentally prepared for the task. Are they engaged in another activity now, and do they have the necessary information, instructions, or experience and training to handle the task? Such questions may emerge in many situations, such as a pilot navigating in a storm while also trying to track a target.

There may be several ways to gain insight into an individual's instantaneous level of preparedness for a cognitive challenge, but two promising concepts are cognitive workload and situational awareness. These are human attributes for which the scientific frameworks are mature,²⁶ checking at least one of the criteria outlined here as necessary. Yet, they suffer some weaknesses that make their operationalization challenging at present. It is not currently clear that there are accessible and appropriate measurements that are unambiguously interpretable to estimate these attributes with existing technology.

Cognitive Workload

Cognitive workload describes the mental processing involved in executing a cognitive task.²⁷ Much effort has gone into accurately measuring instantaneous cognitive workload. However, its subtlety and complexity make it difficult to quantify unambiguously. Current methods, such as measuring features of the electroencephalogram (EEG) or pupillometry, have had some success,²⁸ but they are limited in their ability to measure cognitive workload unambiguously and with high sensitivity and specificity across contexts and situations. Furthermore, these states are highly individualized and influenced by internal and external factors that make standardizing the measurement challenging. Thus, obtaining reliable measurements that are interpretable with respect to theory and to the original question is not typically achievable.

The cognitive workload an individual experiences is context-dependent. Extant measurement modalities such as the EEG and pupillometry are only valid with the knowledge that the individual is engaged in a task for which it is sensible to measure cognitive workload. A general-purpose sensor would thus require context information. Without such context, biometric measures like pupillometry are not fully interpretable.

Situational Awareness

Situational awareness is the concept of having knowledge of and the ability and propensity to appropriately act on relevant information in one's environment and in a way that is consistent with one's goals.²⁹ Much like cognitive workload, situational awareness has been studied extensively.³⁰ Furthermore, mature scientific frameworks exist against which to rationalize potential measurements and observations. For instance, one can infer an individual's level of situational awareness by staging a test within the context of a task that requires them to notice, acknowledge, and act appropriately and promptly in response to new information. However, individual situational awareness is difficult to practically measure in a way that makes interpretation unambiguous.

There have been efforts to discover signatures of an individual's level of situational awareness without considering context (i.e., their situation),³¹ but they have not yet managed to produce unambiguous biomarkers of an individual's situational awareness for general scenarios. Presently, one reliable way to identify someone's level of situational awareness is for a trained observer to witness them receiving potentially relevant information and then determine whether they acted on that information appropriately and at the appropriate time; another is to quiz them on their level of awareness of the information with a questionnaire. For example, if a weather alert is delivered to an airplane's cockpit, one could ascertain the situational awareness of the navigator with respect to the weather alert by observing the route they plan.

While it may be possible to obtain an interpretable measurement that would signify situational awareness within a specific, narrowly scoped application, it is uncertain how one would measure this with a general-purpose sensor using today's standard commercially available technology. How would a system measuring an individual's actions in response to new information know what reaction is expected and when without knowing the individual's goals in the situation they are facing? How would a system know what information is relevant to the individual? A

general-purpose system would need the capacity to reason about the appropriate situational awareness itself. This capability is not yet feasible for a general-purpose biomarker of situational awareness.

Horizons of Technology for Quantifying Human Traits

Emerging technologies and methodologies to quantify human traits using wearable technology are poised to advance the depth and scope of what can be measured and interpreted.

One promising emerging technology in this area is augmented reality (AR), including, for the purposes of simplicity, any wearable remote sensing device that measures a user's environment in real time. AR technology facilitates a deeper connection with one's environment. It typically senses the user's environment to integrate virtual elements such as visual overlays or virtual objects and senses the user's behaviors within the environment. These capabilities not only facilitate novel interactions but also offer the possibility of building a representation of the user's context and situation, which could reduce or eliminate the ambiguity in measuring attributes like cognitive workload and situational awareness. Automatically detecting the user's type of task or scenario may thus be possible, providing the context information critical for interpreting measures within the appropriate scientific framework.

The fusion of context-inferring technology, such as wearable remote sensing devices embedded within AR platforms, with physiological measurements like eye tracking and heart rate monitoring may introduce exciting new possibilities for attribute quantification (fig. 10.2). Having context information significantly enhances the interpretability of biosignatures for many possible attributes. For instance, understanding the environmental context in which a heightened heart rate occurs (e.g., during physical exertion vs. concerted concentration) can lead to more accurate attribute assessments.

Specialized sensors facilitating appropriate data to infer context are only the first step to fully disambiguating user context. Artificial intelligence will also be critical for the detection and interpretation of context. Novel algorithms that detect context, including objects in a user's environment, behaviors a user performs, or activities they are engaged in, will be integral to effectively identifying context and

disambiguating the meaning of other biomarkers like heart rate, EEG, or pupillometry signals.

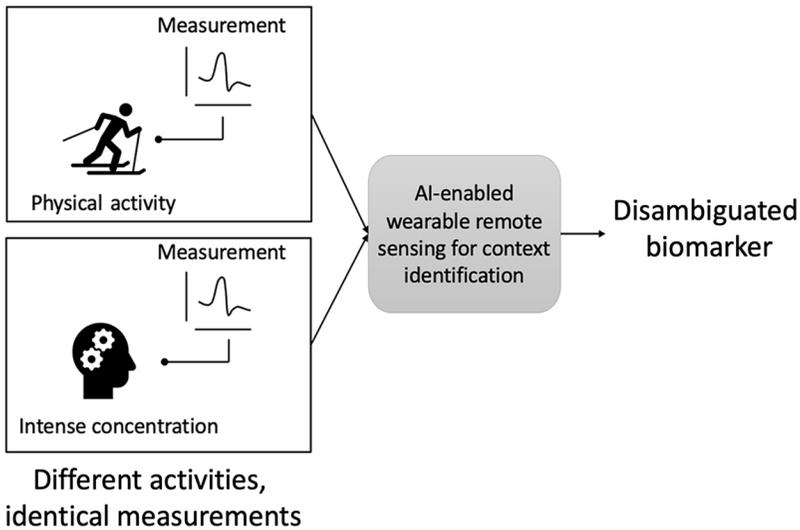


Figure 10.2. AI-enabled wearable remote sensing technology may facilitate disambiguation of otherwise identical measurements by detecting context.

Longitudinal data collection is another promising emerging capability. Gathering data from the same individuals over extended periods of time and across varied contexts and scenarios may enable researchers and developers to gain insights into long-term trends and changes in individual attributes. Longitudinal data collection will enable characterization of sources of variability in potential biomarkers over time and across individuals. This information is critical, as most individualized attributes have intrinsic ambiguity regarding the sources of variability. This longitudinal approach enables a more accurate and comprehensive accounting of those sources of variability and the factors that may help account for them in operational environments.

Longitudinal data collection may also allow for developing predictive models that can forecast future changes in individualized attributes or behavioral patterns. Integrating predictive modeling in wearable technology may facilitate the ability to intervene to change the course of an attribute, exploit a beneficial situation, or prevent negative consequences. For example, if a predictive model foresees a period of heightened awareness or availability of cognitive workload, the individual could

be alerted and advised to tackle a more challenging task given their predicted heightened ability. Alternatively, a system that detects exhaustion or other lack of readiness could alert the individual to rest or avoid taking on high-stakes activities.

Combining advanced wearable technologies with AI and longitudinal data collection will likely open new frontiers in understanding human behavior and physiology. The potential applications are vast, ranging from enhancing athletic performance to detecting diseases early and improving mental health or cognitive performance.

Conclusions

Effectively quantifying human traits is not straightforward. It requires sound theory about the attributes in question, the feasibility to measure relevant and established biomarkers, and a means to meaningfully interpret those biomarkers with respect to the scientific theory. While quantifying visible states like physical fitness has progressed remarkably, the journey toward accurately measuring and interpreting hidden cognitive states is still evolving. The future of quantifying human attributes through wearables holds immense promise. By leveraging emerging technologies and methodologies, better detection of context may become possible, thereby enabling the proper interpretation of signatures within established theory. Furthermore, longitudinal measurements may increase the accuracy of attribute quantification, and the development of predictive models may facilitate exciting new possibilities for intervention or human performance optimization. Regardless, the successful quantification of human attributes requires that the scientific understanding of the attribute be well established, that measurement of biomarkers is possible, and that the biomarkers be interpretable within the established scientific framework.

The path forward in the military application of human quantification and wearable sensors is illuminated by the promise of integrating advanced computational methods with wearable technologies. Artificial intelligence and machine learning algorithms, in particular, stand to revolutionize the interpretation of complex, multidimensional data collected from wearables, enabling developing predictive models that can anticipate health issues, physical overstrain, or cognitive overload before they become critical. This proactive approach to managing warfighter health and performance could dramatically enhance mission

readiness and effectiveness. These advancements underscore the value of continued investment in research and development to refine the accuracy, reliability, and applicability of wearable sensors and AI-driven analysis in military settings.

As we look to the future, the integration of wearable technologies in military operations is poised to enter a new era of sophistication and effectiveness. The challenge lies not just in the technical realm but also in ensuring that these technologies are deployed ethically and responsibly, with due consideration for the privacy and well-being of the individuals they are designed to support. The promise of these technologies to enhance military readiness and safeguard the health of service members is immense, contingent upon a collaborative effort between scientists, engineers, military strategists, and policymakers to advance our scientific understanding and technological capabilities. By adhering to rigorous scientific principles and prioritizing the development of interpretable and reliable biomarkers within this framework, the military can harness the full potential of human attribute quantification to achieve unprecedented levels of operational efficiency and strategic advantage.

Notes

1. Federico Germini et al., “Accuracy and Acceptability of Wrist-Wearable Activity-Tracking Devices: Systematic Review of the Literature,” *Journal of Medical Internet Research* 24, no. 1 (January 21, 2022): e30791, <https://doi.org/10.2196/30791/>.

2. Luke Cramer et al., “A Review of Individual Operational Cognitive Readiness: Theory Development and Future Directions,” *Human Factors* 63, no. 1 (2021): 66–87, <https://doi.org/10.1177/0018720819868409/>.

3. Andrew Flood and Richard J. Keegan, “Cognitive Resilience to Psychological Stress in Military Personnel,” *Frontiers in Psychology* 13 (March 16, 2022), <https://doi.org/10.3389/fpsyg.2022.809003/>.

4. FDA-NIH Biomarker Working Group, BEST (Biomarkers, EndpointS, and Other Tools) Resource (Food and Drug Administration (US), 2016), <http://www.ncbi.nlm.nih.gov/>; and Robert M. Califf, “Biomarker Definitions and Their Applications,” *Experimental Biology and Medicine* 243, no. 3 (February 2018): 213–21, <https://doi.org/10.1177/1535370217750088/>.

5. Brian J. North and David A. Sinclair, “The Intersection Between Aging and Cardiovascular Disease,” *Circulation Research* 110, no. 8 (April 13, 2012): 1097–1108, <https://doi.org/10.1161/CIRCRESAHA.111.246876/>; Elsayed Z. Soliman et al., “Atrial Fibrillation and the Risk of Myocardial Infarction,” *JAMA Internal Medicine* 174, no. 1 (January 2014): 107–14, <https://doi.org/10.1001/jamainternmed.2013.11912/>; Francesco Violi et al., “Atrial Fibrillation and Myocardial Infarction: A Systematic Review and Appraisal of Pathophysiologic Mechanisms,” *Journal of the American Heart Association* 5, no. 5 (May 20, 2016): e003347, <https://doi.org/10.1161/JAHA.116.003347/>; and Miho Iida et al., “Application of Metabolomics to Epidemiological Studies of Atherosclerosis

and Cardiovascular Disease,” *Journal of Atherosclerosis and Thrombosis* 26, no. 9 (September 1, 2019): 747–57, <https://doi.org/10.5551/jat.RV17036/>.

6. Kristian Thygesen et al., “Fourth Universal Definition of Myocardial Infarction (2018),” *Journal of the American College of Cardiology* 72, no. 18 (October 30, 2018): 2231–64, <https://doi.org/10.1016/j.jacc.2018.08.1038/>; and Violi et al., “Atrial Fibrillation and Myocardial Infarction.”

7. Carmen Fiuza-Luces et al., “Exercise Benefits in Cardiovascular Disease: Beyond Attenuation of Traditional Risk Factors,” *Nature Reviews Cardiology* 15, no. 12 (December 2018): 731–43, <https://doi.org/10.1038/s41569-018-0065-1/>; and Marie-Eve Piché et al., “Overview of Epidemiology and Contribution of Obesity and Body Fat Distribution to Cardiovascular Disease: An Update,” *Progress in Cardiovascular Diseases* 61, no. 2 (2018): 103–13, <https://doi.org/10.1016/j.pcad.2018.06.004/>.

8. Pedro L. Valenzuela et al., “Exercise Benefits in Cardiovascular Diseases: From Mechanisms to Clinical Implementation,” *European Heart Journal* 44, no. 21 (June 1, 2023): 1874–89, <https://doi.org/10.1093/eurheartj/ehad170/>; and Danyang Tian and Jinqi Meng, “Exercise for Prevention and Relief of Cardiovascular Disease: Prognoses, Mechanisms, and Approaches,” *Oxidative Medicine and Cellular Longevity* (2019): 3756750, <https://doi.org/10.1155/2019/3756750/>.

9. Nancy F. Butte et al., “Assessing Physical Activity Using Wearable Monitors: Measures of Physical Activity,” *Medicine and Science in Sports and Exercise* 44, no. 1, Suppl. 1 (January 1, 2012): S5–S12, <https://doi.org/10.1249/MSS.0b013e3182399c0e/>; and Louisa G. Sylvia et al., “A Practical Guide to Measuring Physical Activity,” *Journal of the Academy of Nutrition and Dietetics* 114, no. 2 (February 2014): 199–208, <https://doi.org/10.1016/j.jand.2013.09.018/>.

10. Scott E. Crouter et al., “Validity of 10 Electronic Pedometers for Measuring Steps, Distance, and Energy Cost,” *Medicine and Science in Sports and Exercise* 35, no. 8 (August 2003): 1455–60, <https://doi.org/10.1249/01.MSS.0000078932.61440.A2/>.

11. Jane E. Sullivan et al., “Feasibility and Outcomes of a Community-Based, Pedometer-Monitored Walking Program in Chronic Stroke: A Pilot Study,” *Topics in Stroke Rehabilitation* 21, no. 2 (2014): 101–10, <https://doi.org/10.1310/tsr2102-101/>; and Tara D. Klassen et al., “Consumer-Based Physical Activity Monitor as a Practical Way to Measure Walking Intensity During Inpatient Stroke Rehabilitation,” *Stroke* 48, no. 9 (September 2017): 2614–17, <https://doi.org/10.1161/STROKEAHA.117.018175/>.

12. Saeed Afshar et al., “Event-Based Object Detection and Tracking for Space Situational Awareness,” *IEEE Sensors Journal* 20, no. 24 (December 2020): 15117–32, <https://doi.org/10.1109/JSEN.2020.3009687/>; and Mica R. Endsley et al., “A Comparative Analysis of Sagat and Sart for Evaluations of Situation Awareness,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 42, no. 1 (October 1, 1998): 82–86,

13. John Sweller, “Cognitive Load Theory,” chap. 2 in *Psychology of Learning and Motivation*, vol. 55, *Cognition in Motivation*, ed. Jose P. Mestre and Brian H. Ross (Academic Press, 2011), <https://doi.org/10.1016/B978-0-12-387691-1.00002-8/>.

14. Essam Debie et al., “Multimodal Fusion for Objective Assessment of Cognitive Workload: A Review,” *IEEE Transactions on Cybernetics* (September 23, 2019): 1–14, <https://doi.org/10.1109/TCYB.2019.2939399/>; and Matthias Scheutz et al., “Estimating Systemic Cognitive States from a Mixture of Physiological and Brain Signals,” *Topics in Cognitive Science* 16, no. 3 (2023): 485–526, <https://doi.org/10.1111/tops.12669/>.

15. Hmwe H. Kyu et al., “Physical Activity and Risk of Breast Cancer, Colon Cancer, Diabetes, Ischemic Heart Disease, and Ischemic Stroke Events: Systematic Review and Dose-Response Meta-Analysis for the Global Burden of Disease Study 2013,” *BMJ* 354 (Clinical Research ed.) (August 9, 2016): i3857, <https://doi.org/10.1136/bmj.i3857/>;

Connie W. Tsao et al., “Heart Disease and Stroke Statistics—2022 Update: A Report from the American Heart Association,” *Circulation* 145, no. 8 (February 22, 2022): e153–639, <https://doi.org/10.1161/CIR.0000000000001052/>; Marc Nocon et al., “Association of Physical Activity with All-Cause and Cardiovascular Mortality: A Systematic Review and Meta-Analysis,” *European Journal of Cardiovascular Prevention and Rehabilitation* 15, no. 3 (June 1, 2008): 239–46, <https://doi.org/10.1097/HJR.0b013e3282f55e09/>; and Emily M. Miele and Samuel A. E. Headley, “The Effects of Chronic Aerobic Exercise on Cardiovascular Risk Factors in Persons with Diabetes Mellitus,” *Current Diabetes Reports* 17, no. 10 (September 12, 2017): 97, <https://doi.org/10.1007/s11892-017-0927-7>.

16. C. K. Morris and V. F. Froelicher, “Cardiovascular Benefits of Physical Activity,” *Herz* 16, no. 4 (August 1991): 222–36. PMID: 1916618.

17. T. Dylan Olver et al., “Molecular Mechanisms for Exercise Training-Induced Changes in Vascular Structure and Function: Skeletal Muscle, Cardiac Muscle, and the Brain,” *Progress in Molecular Biology and Translational Science* 135 (2015): 227–57, <https://doi.org/10.1016/bs.pmbs.2015.07.017/>; and Kelsey Pinckard et al., “Effects of Exercise to Improve Cardiovascular Health,” *Frontiers in Cardiovascular Medicine* 6 (June 4, 2019): 69, <https://doi.org/10.3389/fcvm.2019.00069/>.

18. Rick B. Vega et al., “Molecular Mechanisms Underlying Cardiac Adaptation to Exercise,” *Cell Metabolism* 25, no. 5 (May 2, 2017): 1012–26, <https://doi.org/10.1016/j.cmet.2017.04.025/>.

19. Roberto Vettor et al., “Exercise Training Boosts eNOS-Dependent Mitochondrial Biogenesis in Mouse Heart: Role in Adaptation of Glucose Metabolism,” *American Journal of Physiology – Endocrinology and Metabolism* 306, no. 5 (March 1, 2014): E519–E528, <https://doi.org/10.1152/ajpendo.00617.2013/>.

20. Laura Gormley et al., “Interventions to Increase Physical Activity: An Analysis of Candidate Behavioural Mechanisms,” *Preventive Medicine Reports* 28 (August 2022): 101880, <https://doi.org/10.1016/j.pmedr.2022.101880/>; Shuang Wu et al., “The Effectiveness of Wearable Activity Trackers for Increasing Physical Activity and Reducing Sedentary Time in Older Adults: A Systematic Review and Meta-Analysis,” *Digital Health* 9 (May 22, 2023): 20552076231176705, <https://doi.org/10.1177/20552076231176705/>; and Caining Li et al., “Wearable Activity Trackers for Promoting Physical Activity: A Systematic Meta-Analytic Review,” *International Journal of Medical Informatics* 152 (August 1, 2021): 104487, <https://doi.org/10.1016/j.ijmedinf.2021.104487/>.

21. Navya Baranwal et al., “Sleep Physiology, Pathophysiology, and Sleep Hygiene,” *Progress in Cardiovascular Diseases* 77 (2023): 59–69, <https://doi.org/10.1016/j.pcad.2023.02.005/>; Laura Palagini et al., “Sleep, Insomnia and Mental Health,” *Journal of Sleep Research* 31, no. 4 (August 2022): e13628, <https://doi.org/10.1111/jsr.13628/>; and Maki Jike et al., “Long Sleep Duration and Health Outcomes: A Systematic Review, Meta-Analysis and Meta-Regression,” *Sleep Medicine Reviews* 39 (June 1, 2018): 25–36, <https://doi.org/10.1016/j.smrv.2017.06.011/>.

22. Baranwal et al., “Sleep Physiology,” 59–69.

23. Celyne H. Bastien et al., “Insomnia and Sleep Misperception,” *Pathologie Biologie* 62, no. 5 (October 2014): 241–51, <https://doi.org/10.1016/j.patbio.2014.07.003/>; and Yingjie Liang et al., “Sleep Misperception and Associated Factors in Patients With Anxiety-Related Disorders and Complaint of Insomnia: A Retrospective Study,” *Frontiers in Neurology* 13 (2022): 836949, <https://doi.org/10.3389/fneur.2022.836949/>.

24. Bastien et al., “Insomnia and Sleep Misperception,” 241–51; and Ruth Ravichandran et al., “Making Sense of Sleep Sensors: How Sleep Sensing Technologies Support and Undermine Sleep Health,” in CHI ’17: *Proceedings of the 2017 CHI Conference on Human*

Factors in Computing Systems (Association for Computing Machinery, 2017), 6864–75, <https://doi.org/10.1145/3025453.3025557/>.

25. Rebecca Robbins et al., “Sleep Tracking: A Systematic Review of the Research Using Commercially Available Technology,” *Current Sleep Medicine Reports* 5, no. 3 (2019): 156–63, <https://doi.org/10.1007/s40675-019-00150-1/>.

26. Endsley et al., “Comparative Analysis of Sagat,” 82–86.

27. Sweller, “Cognitive Load Theory,” chap. 2.

28. Pavlo Antonenko et al., “Using Electroencephalography to Measure Cognitive Load,” *Educational Psychology Review* 22, no. 4 (2010): 425–38, <https://doi.org/10.1007/s10648-010-9130-y/>; and Andrew T. Duchowski et al., “The Index of Pupillary Activity: Measuring Cognitive Load vis-à-vis Task Difficulty with Pupil Oscillation,” in CHI ’18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Association for Computing Machinery, 2018), 1–13, <https://doi.org/10.1145/3173574.3173856/>.

29. Patrick Van Horne and Jason A. Riley, *Left of Bang: How the Marine Corps’ Combat Hunter Program Can Save Your Life*, narrated by Danny Campbell (Tantor Audio, 2015).

30. Afshar et al., “Event-Based Object Detection,” 15117–32; and Sarang Thombre et al., “Sensors and AI Techniques for Situational Awareness in Autonomous Ships: A Review,” in *IEEE Transactions on Intelligent Transportation Systems* 23, no. 1 (January 2022): 64–83, <https://doi.org/10.1109/TITS.2020.3023957/>.

31. Ting Zhang et al., “Physiological Measurements of Situation Awareness: A Systematic Review,” *Human Factors* 65, no. 5 (2023): 737–58, <https://doi.org/10.1177/0018720820969071/>.

Part 4

CHINESE AND RUSSIAN MIND-TECH

Chapter 11

The Case of Russia

*Samuel Bendett, Adjunct Senior Fellow, Center for a New
American Security*

Abstract

This chapter explores Russian military attempts at enhancing human combatant capabilities with modern technologies. The Russian military, academia, and practitioners are deliberating current and future combat, where the human-machine nexus involves a synthesis of mission-driven types of automated, semiautomated, and robotic systems powered by artificial intelligence as a key decision-making, data analysis and C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) tool. While Russia's invasion of Ukraine has revealed significant issues with Russian military technology, concepts, and personnel utilization, Russian military institutions, academies, defense-industrial enterprises, and research and development centers charged with conceptualizing high-tech combat have maintained focus on the human-technology nexus, especially in light of the growing use of advanced robotics and autonomous technology by both belligerents. Overall, the Russian Ministry of Defense (MOD) man-machine concept revolves around replacing or removing combatant human operators and human soldiers by enabling greater autonomy for military systems. An overlapping and complementary set of developments includes enhancing Russian soldiers with advanced capabilities for more accurate and lethal human performance on the battlefield. Russia's ongoing war against Ukraine and the resulting rapid evolution of systems and technologies operated by humans are pushing technologists to develop systems and weapons that can operate and react faster than the adversary's. With the current wartime needs taking a heavy human toll on the Russian military force, designing and fielding systems that enhance human performance is a logical direction for the MOD and similar to the technology paths chosen by other military powers as well considering the ongoing Ukraine combat. For now, Russia's public discussion on the topic of mind-technology and man-machine nexus merits close attention.

The Russian military discussion about the role of machines in war goes back many decades, probably to the first remote-controlled aerial and ground vehicles of the 1930s–1940s. As the battlefield technology continued to evolve, and as Soviet and later Russian military thinking about war has attempted to adapt to modern conflicts and adversary developments, a Russian Ministry of Defense (MOD) assessment of human-machine collaboration resulted in the evaluation and development of concepts such as the role of military robotics, autonomy, and artificial intelligence in combat. This chapter is not specifically about how the Russian military thinks in such terms or about these specific technologies—rather, it is a brief exploration of its attempts to enhance human combatant capabilities with modern technologies.

Russian writings from the military, academic, and practitioner communities are deliberating current and future combat, where the human-machine nexus involves a synthesis of mission-driven automated, semiautomated, and robotic systems powered by artificial intelligence as a key decision-making and C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) tool. Despite a relatively public development and testing of such concepts prior to the invasion of Ukraine in February 2022,¹ many of these efforts likely have been reworked, updated, shelved, or changed altogether to reflect Russian military performance and challenges and Ukraine's development and fielding of such systems and weapons.²

While Russia's invasion of Ukraine has revealed significant issues with military technology, concepts, and personnel use, Russian military institutions, academies, defense-industrial enterprises, and research and development (R&D) centers charged with conceptualizing high-tech combat have maintained focus on the human-technology nexus. The Russian military is also focused on similar and parallel developments in the United States, NATO, China, Iran, Turkey, Israel, and other countries, monitoring their respective technological progress and application examples. Overall, the Russian MOD man-machine concept centers on replacing or removing combatant human operators and soldiers by enabling greater autonomy for military systems. An overlapping, complementary set of developments includes enhancing Russian soldiers with advanced capabilities for a more accurate and lethal human performance on the battlefield.

Man-Machine Nexus

Smart Helmets and Neural Links

Primary factors driving the Russian military's conceptualization and eventual development of enhanced human battlefield performance include a perceived vulnerability to a more technologically advanced US-NATO cooperation, the peer-mirroring of global technology R&D devoted to military systems, and even the country's worsening demographic situation. The effort to remove soldiers from dangerous missions and safeguard an ever-decreasing supply of young Russian men is reflected in statements from the larger R&D, military academic, and even volunteer communities that a large "army of men" may no longer be a feasible option in the future—rather, an "army of robots" should be "birthed" by the domestic military-industrial complex.³ Technology is providing a way for combatants to increase their precision, lethality, and performance. Several examples are worth considering as a reflection of the Russian MOD's vision of how this synergy might look.

One example includes a concept for a helmet to allegedly control aerial drones with the power of a soldier's thought.⁴ It consists of a neuro-headset that can be mounted inside an infantry helmet, tank helmet, or cap. According to the Russian *Izvestia* state media publication that broke the story in 2022, additional caps with electrodes are not required in this case to measure the brain's electrical signals. This "neuro-helmet," developed by the medical cybernetics laboratory at Voronezh State University, can be suitable for field and extreme conditions and allegedly allows for monitoring the operator's health and mood. Russian experts quoted in the *Izvestia* article consider this technology in demand by the military, a range of civilian professions such as geologists, and people with disabilities. The helmet works as follows: a dry electrode is mounted on a cap, and a specially developed application for a mobile device receives electrical signals from the brain, decodes them, and eventually interprets them into commands to control a drone or other uncrewed device (fig. 11.1).⁵



Figure 11.1. Neural helmet concept. (Source: Maria Nedyuk, «Мыслью по шлему: ученые создали нейрокаска для управления дронами» [Helmet thought: scientists have created a neurohelmet to control drones], Iz.ru, October 23, 2022, <https://iz.ru/>.)

According to the developers, the wearer can control not only a drone but also a vehicle, boat, light aircraft, underwater system, or even spacecraft. The device includes command not just by the power of thought but with a glance. For example, an operator blinks several times to issue a command for an aerial drone to land while issuing a mental command for a drone to fly forward. The developers also claimed in 2022 that at the current stage of this “neurohelmet’s” development, it can be used primarily to determine a person’s mental health—a key factor in a high-stress combat environment. On the other hand, Russian state media may exaggerate the technological developments it covers while providing few technical details for objective analysis. However, this particular publicized device is likely one of several similar projects also occurring in the MOD and civilian R&D ecosystem. At the same time, it has not shown up on the Ukraine battlefields to date.

Another military project that may be closer to reality is the soldier enhancement concept that is part of the Ratnik fighting system, comprising of kinetic, computational, and protective systems in a suit-like form. In an advanced Ratnik version called Sotnik, individual soldier's actions and operations are allegedly enabled by connecting a soldier to the commander and other troops with the assistance of artificial intelligence. The soldier also operates their own miniature UAVs and uncrewed ground vehicles for greater situational awareness and combat performance. Considering the amount of data each soldier would need to process, Ratnik is supposed to include a "smart helmet" with communication systems and a tactical computer built in and incoming information displayed directly on the visor. Combat information would be displayed in front of the soldier's eyes to enable quick absorption of the data, potentially reducing the time spent on making decisions.⁶ The Ratnik plans as of 2019—before Russia invaded Ukraine—included a communication, control, and "friend or foe" recognition system built into this helmet that would monitor the soldier's mental, psychological, and physical state in real time.⁷ As a result, each fighter should become a sensor, receiving information and target designation and transmitting data further to the higher command structures.⁸

While this development has been teased regularly for the past five years, there are as yet no working concepts or a detailed description of how such a suit is operating. The combat in Ukraine has pushed the requirements down to the most basic level, with many Russian soldiers having the minimal equipment and supplies even in the supposedly elite formations. At the same time, the MOD's Central Research Institute of Precision Engineering still announced that the next Ratnik iteration—the Legionnaire—was to be tested in 2023. Given the resource expenditures for the continued Ukraine invasion and the likely reprioritization of certain MOD projects, the latest Legionnaire news includes its test version appearing sometime in 2025, with mass delivery to the forces starting around 2035.⁹ Such lengthy R&D horizons are no doubt dictated by the Russian military's ground performance in Ukraine and the limits faced by the domestic defense industry's ability to develop such a sophisticated system, which so far evades even the most advanced and well-funded militaries around the world. The Legionnaire suit is also allegedly equipped with a smart helmet that enables a soldier to get UAV and drone-based data via augmented reality.¹⁰

The fielded smart helmet solutions could also come from Russia's private sector, with numerous high-tech and information technology

companies experimenting with different battlefield concepts and prototypes. For example, in November 2023, Russian scientists from the Neurobotics company used a neural interface to control a small UAV using brain impulses.¹¹ According to the company, simple commands to pilot a quadcopter can be allegedly learned in just ten minutes. Neurobotics planned to hold domestic racing competitions on such “neurocopters,” with the developers noting that controlling a drone using the power of thought can be a highly useful workout for the brain to improve concentration and to cope with stress and emotions.¹² The country’s military, eager to achieve an advantage over Ukrainian forces, may also seek to utilize civilian achievements like this Neurobotics effort.

Virtual, Augmented, and Mixed Reality

The Russian military’s experimentation with virtual, augmented, and mixed reality is not well documented in public sources, yet a few announcements point to the MOD’s general trends in step with key global developments. As described above, data analysis, remote control, and other functions are built into some of the technologies that are supposed to directly enhance Russian soldier performance. A sample development includes Rostec State Corporation’s working prototype of a next-generation mixed reality simulator to train military personnel by combining real and virtual objects in a single environment.¹³

In 2017, the Russian government discussed plans to implement virtual reality and augmented reality in combat training centers. The Russian government considered the reduced training time via such technologies key to lowering the overall costs by saving on fuel and ammunition expenditures.¹⁴ The 2017 plans also called for including augmented, mixed, and virtual reality technologies across the nation’s military-industrial complex to improve the efficiency of maintenance and production processes in the defense industry.¹⁵ It is unclear how far these plans were implemented since then, especially in light of resource allocation for the invasion of Ukraine. Also in 2017, the MOD discussed new training for the Airborne Forces (VDV) to practice parachuting in virtual reality.¹⁶ These and other plans may be ongoing, but the overall emphasis on ground-based warfare in Ukraine that uses a mix of decades-old infantry and artillery concepts backed by newer technologies like aerial drones and tactical electronic warfare will likely impact how the Russian military trains and fights going forward.

Robotics and Autonomy

Other Russian military examples of connecting humans and machines for combat include the developments at Android Technologies, one of Russia's flagship robotics and high-tech companies with direct links to the MOD. The company is in an official partnership with the Advanced Research Foundation (AFP), Russia's DARPA-like equivalent. Together, they developed the Marker combat uncrewed ground vehicle (UGV) platform for computer vision, natural language processing, navigation, autonomous movement, and group vehicle control. Tests publicized by Russian state media and conducted a few years before Russia's invasion of Ukraine allegedly had Marker follow soldier commands and prompts in a manned-unmanned teaming arrangement, essentially turning infantry into spotters for robots.¹⁷ The Russian press also gave ample coverage to the alleged Marker tests in eastern Ukraine starting in March 2023, though without any specific details or even visual evidence.¹⁸ While there is no follow-up information at this point in the Russian media about such tests or even Marker's actual combat use, the fact that these advanced R&D institutions were working on such concepts points to the potential—even if distant—use in combat by Russian forces. For now, many UGVs used at the front are remote-controlled vehicles for demining and light combat or small logistics and evacuation vehicles assembled by Russian soldiers at the front and by volunteer and start-ups efforts for moving supplies, ammunition, and wounded personnel.¹⁹

Robotic and autonomous projects are in various stages of development across the Russian MOD, many predating the invasion of Ukraine and just as many influenced by brutal combat, where reconnaissance and close-range combat drones are ubiquitous across the battlefield. The ongoing war is likely to reallocate key high-tech resources away from prospective and toward more conventional and pressing needs, with the potential to limit research into more advanced military features of Mind-Tech cooperation. Despite the massive resources this war demands of the Russian military, multiple advanced UAV and robotics development projects are underway, albeit somewhat behind their original schedules.²⁰ One such project is the Okhotnik heavy combat drone, which can potentially fly in a manned-unmanned teaming arrangement with crewed aircraft.

MOD Ecosystem for the Mind-Tech and Man-Machine Nexus

Studies relating to the mind-technology and human-technology connection are occurring across numerous MOD and government-affiliated and funded institutions. In Russia, most scientific and technological research is government-funded, with the state assisting and supporting R&D centers across academia, industrial corporations, and military institutions. In that sense, most of the conceptual and ready products and systems will belong to the state, even if the government bodies or military researchers did not initially participate in such work.

One of the newer centers working on cutting-edge R&D is ERA Technopolis, launched in 2018 as a R&D campus where military and nonmilitary or private sector high-tech projects can be fast-tracked for the needs of different branches of the country's armed forces. In 2021, ERA announced research on the new neuropsychological diagnostic methods for testing military personnel. The system allegedly records brain activity, facial expressions, eye movement, direction of gaze, gestures, breathing, and heartbeat to determine the objective predisposition of soldiers and officers to perform a certain type of professional activity.²¹ This system is also supposed to assess human stress resistance in critical and extreme conditions.

The aforementioned Android Technologies together with the Advanced Research Foundation were developing a robotic avatar for space-based work, with humanlike exoskeletons called Teledroid and Tester in development since the much-publicized 2019 launch of the Fedor robot to the International Space Station.²² Although initially more of a remote-controlled exoskeleton, future iterations of these systems do not exclude control via more advanced means such as virtual, augmented, and mixed realities. Earlier in 2015, AFP announced work on the brain-computer interface to control technology with the power of thought, with the initial developments allegedly ready for transfer to government agencies.²³ As with other similar announcements in Russian state media, there is little to no follow-up in public sources on the exact nature of this project.

Russian universities and research labs are also working on brain-computer interface technologies, and many of these institutions are connected directly or indirectly to the government and MOD. Medical research in the civilian space dealing with such issues is also of

interest to the military, such as work at the Samara State University's (SSU) on neurocomputer interfaces—tools for communication and interaction between the human brain and a computer. SSU's research is primarily directed at medical recovery following significant medical injury, with patients using the power of thought to move and enable systems designed to mimic normal human actions.²⁴ However, in 2015, AFP allegedly visited the SSU neurocomputer lab, possibly seeking to adapt and adopt available solutions for military applications.²⁵

In 2018, the Russian Academy of Sciences, a government body that oversees national scientific activity and research, established the Cyber-Physical Systems (CPS) Laboratory to combine the work of computers, networks, and physical processes.²⁶ CPS's research consists of elements and actuators in which computers monitor and control physical processes using feedback.²⁷ This lab was supposedly working on creating cyber-physical systems, along with the technologies and methods for controlling robotics and improving the quality of the human-machine interface in special conditions. This lab was also developing methods to pilot and control heterogenous robotic systems in different environments. Considering that this institution is government-funded, its research can potentially find its way to the military for follow-on work on controlling such heterogenous robotic agents with the power of thought, as outlined above.

Conclusion

Russia's ongoing war against Ukraine and the resulting rapid evolution of systems and technologies operated by humans are pushing technologists to build weapons that can operate and react faster than the adversary's. Russian developments in this space include systems meant to enhance human performance and mission effectiveness. Currently, many such developments are still in the testing and experimental stages, with more relevant work likely conducted in the classified environment. Nonetheless, public sources reveal trials and examples that point to Russia's general R&D direction. It is unclear to what extent some of the examples made public and cited in this chapter will see the light of day, given the massive resources Russia must devote to its current conventional requirements on the Ukraine battlefield. Ukraine's high-tech advancements will likely push Russia to invest in or accelerate new and existing projects. With the current

wartime needs taking a heavy human toll on the Russian military force, designing and fielding systems that enhance human performance is a logical direction for the MOD. Whether its defense-industrial complex can deliver on this technology remains to be seen—for now, Russia’s public discussion on mind-technology and the man-machine nexus merits close attention.

Notes

1. Jeffrey Edmonds et al., *Artificial Intelligence and Autonomy in Russia* (Center for Naval Analyses, 2021), <https://www.cna.org/>.

2. Samuel Bendett, “Bureaucrat’s Gambit: Why Is Dmitry Rogozin Sending Russian Uncrewed Ground Vehicles to Ukraine—And Does It Matter?,” Center for a New American Security, February 10, 2023, <https://www.cnas.org/>; and Sam Bendett, “Roles and Implications of AI in the Russian-Ukrainian Conflict,” *Russia Matters*, Belfer Center, July 20, 2023, <https://www.russiamatters.org/>.

3. Дронификация войны [Dronification of combat], Dronnitsa Telegram channel, August 25, 2023, <https://t.me/dronnitsa/257>.

4. Maria Nedyuk, « Мыслью по шлему: ученые создали нейрокаска для управления дронами » [Helmet thought: scientists have created a neurohelmet to control drones], *Iz.ru*, October 23, 2022, <https://iz.ru/>.

5. Nedyuk.

6. Yuferev Sergey, «Комплект экипировки «Ратник» получит экзоскелет и умный шлем» [The Ratnik equipment set will receive an exoskeleton and a smart helmet], *TopWar.ru*, February 20, 2019, <https://topwar.ru/>.

7. Sergey.

8. Sergey.

9. «Опытный образец экипировки «Легионер» создадут в 2025 году» [A prototype of the Legionnaire equipment will be created in 2025], *Ria.ru*, February 6, 2023, <https://ria.ru/>.

10. «Испытания экипировки «Легионер» начнутся после новогодних праздников» [Testing of the “Legionnaire” equipment will begin after the New Year holidays], *Ria.ru*, December 29, 2022, <https://ria.ru/>.

11. Nikita Laktyushin, «В России создали квадрокоптеры, которыми можно управлять силой мысли (видео)» [Quadcopters that can be controlled by the power of thought have been created in Russia], *Hi-Tech.mail.ru*, November 28, 2023, <https://1-hi-tech-mail-ru.translate.google/>.

12. Laktyushin.

13. «Виртуальная реальность в вооруженных силах России» [Virtual reality in the Russian armed forces], *TAdviser.ru*, March 19, 2020, <https://www.tadviser.ru/>.

14. «Власти России собрались внедрить виртуальную реальность в войска и медицину» [The Russian authorities are going to implement virtual reality in the troops and medicine], *CNews.ru*, December 20, 2017, <https://www.cnews.ru/>.

15. “Russian authorities.”

16. “Virtual reality in the Russian armed forces.”

17. Kelsey D. Atherton, “Russian System Uses Infantry to Spot for Robots,” *C4ISRNet.com*, March 3, 2019, <https://www.c4isrnet.com/>.

18. «Четыре боевых робота «Маркер» прибыли в Донбасс» [Four “Marker” combat robots arrived in Donbass], *Tass.ru*, February 2, 2023, <https://tass.ru/>.

19. Telegram Channel: UAV Developer, December 14, 2023, <https://t.me/UAVDEV/4932>; Telegram Channel: UAV Developer, December 8, 2023, <https://t.me/UAVDEV/4823>; and Telegram Channel: Pomosch Zemlyakam, December 2, 2023, <https://t.me/>.
20. «Источник: госиспытания тяжелого ударного БЛА «Охотник» планируют завершить до конца года» [Source: state tests of the heavy attack UAV “Okhotnik” are planned to be completed by the end of the year], Tass.ru, August 8, 2023, <https://tass.ru/>; and «Новый российский ударный дрон «Сириус» выполнит первый полет в этом году» [The new Russian attack drone “Sirius” will perform its first flight this year], Ria.ru, August 9, 2022, <https://ria.ru/>.
21. «В технополисе «Эра» разработают новые способы тестирования военных» [Technopolis “Era” will develop new ways to test the military], Mil.Press Boehhoe, February 2, 2021, <https://xn--b1aga5aadd.xn--p1ai/>.
22. Natalia Yachmennikova, «Зачем в космосе нужны роботы-аватары» [Why do we need robot avatars in space?], RG.ru, November 19, 2019, <https://rg.ru/>.
23. Maria Leyva, «В России создали интерфейс управления техникой силой мысли» [In Russia, an interface for controlling equipment with the power of thought has been created], RBC.ru, June 8, 2015, <https://www.rbc.ru/>.
24. Department of Information Policy of the Administration of the Governor of the Samara Region, «Самарские технологии нейрокомпьютерных интерфейсов высоко оценил Фонд перспективных исследований» [Samara technologies of brain-computer interfaces highly appreciated by the Advanced Research Foundation], PNP.ru, March 13, 2015, <https://www.pnp.ru/>.
25. Department of Information Policy.
26. V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, «Лаборатория № 80: Киберфизических систем» [Laboratory No 80: Cyber-Physical Systems], accessed July 2024, <https://www.ipu.ru/>.
27. V. A. Trapeznikov Institute.

Chapter 12

The People's Liberation Army at the Nexus of Mind and Technology to Shape the Cognitive Battlefield

*Josh Baughman, Analyst, China Aerospace Studies Institute,
Air University*

Abstract

The People's Liberation Army (PLA) of China underscores the paramount significance of the cognitive domain in achieving triumph in conflicts, particularly highlighting the integration of mental processes and technological interfaces. Embedded within their strategic framework of "system-of-systems warfare," the cognitive domain emerges as the pivotal battleground, influencing both strategic and operational decision-making. Recent publications from the PLA delve into prospective technologies capable of optimizing cognitive domain operations. While technological platforms play a pivotal role in executing cognitive attacks for "system destruction," the PLA places equal emphasis on "system survival." This involves bolstering the mental resilience of soldiers through a fusion of traditional and technological approaches. Additionally, the PLA prioritizes equipping commanders with tools that facilitate the seamless integration of human capabilities and machine intelligence, thereby fostering informed decision-making on the dynamic battlefield.

For the People's Liberation Army (PLA), the ultimate victory is to destroy an adversary's will to fight. PLA strategists believe that "military confrontation, on the surface, is a confrontation between the hard powers of the two sides, but at a deeper level, no matter what the nature of the war and the purpose, it is ultimately a contest of human will."¹ The ultimate high ground in which "human will" is fought is in the cognitive domain where the mind is the main battleground. While the cognitive domain has existed since the first conflicts of mankind, the PLA sees the power in the nexus of mind and technology to shape the cognitive battlefield. Particularly, social media, the metaverse, smartphone apps,

wearable technology, virtual reality (VR), artificial intelligence (especially generative AI), digital twins, and the future of brain-computer interface technology will all play a role in the success of the PLA in the cognitive domain. The importance of the cognitive domain follows the PLA's operational concept of "system-of-systems warfare." The mind is the key node in a system and, thus, the ultimate goal in both the "system destruction" of an adversary and the "system survival" of the PLA. The United States and its allies must understand how China will use technology in the cognitive domain, or any future wars could be lost before they begin.

Conceptual Overview

Understanding China's View of the Cognitive Domain

To understand the cognitive domain, grasping cognition itself is essential. According to the *PLA Daily* article "A Perspective on the Evolution Trend of Cognitive Warfare," *cognition* is delineated as "the process of acquiring, processing, and applying information and knowledge."² An adversary's manipulation of cognition can disrupt decision-making and overarching strategies aligning with the objectives of cognitive domain operations. The *PLA Daily* article "A Brief Analysis of the Basic Meaning of Cognitive Domain Operations" offers a definition of the term: "Cognitive domain operations take the human brain as the main combat space, and focus on striking, weakening, and dismantling the enemy's will to fight, using human psychological weaknesses such as fear, anxiety, and suspicion as a breakthrough point, focusing on soft-kill methods to create an atmosphere of insecurity, uncertainty, and mistrust within the enemy, and increasing their internal friction and decision-making doubts."³ Cognitive domain operations target individuals' will, beliefs, thoughts, and psychology directly, aiming to influence decision-making and behaviors by altering the opponent's cognition.

For the PLA, attacking an adversary's mind in the cognitive domain is essential, as is fortifying the minds of PLA soldiers. Mao Zedong is famously quoted on the key to winning the "war to resist U.S. aggression and aid Korea," stating, "The enemy has more *gang* [钢] and less *qi* [气], but we have less *gang* [钢] and more *qi* [气]."⁴ *Gang* can be directly translated as "steel," but the basic idea refers to physical weapon systems such as tanks and planes. *Qi*, which can be directly translated

as “air,” refers to the will to fight and the spirit of struggle at the foundation of ideals and beliefs. As Mao states, “Only a person with firm ideals and beliefs is not afraid of sacrifice and dares to fight.” While the ability to effectively attack an adversary in the cognitive domain is critical to PLA strategic thinking, having a strong mental state, or *qi*, is equally necessary for success on the battlefield.

The PLA understands that the minds of its soldiers are vulnerable not only to the hardships of warfare but also to potential external manipulation. In a *PLA Daily* article titled “Cognitive Domain Operations from the Perspective of Intelligence,” the author writes, “In future cognitive domain operations, the influence of rational factors such as science and logic on individual cognition is likely to be weakened, and cognitive confrontation may become a contest of emotions.”⁵ The emotions, overall mental state of PLA soldiers individually and collectively, and key nodes at the leadership level must be protected. The PLA has adopted the continuation of traditional political work alongside emerging technologies to protect and strengthen the *qi* of its soldiers.

System-of-Systems Warfare

Fundamental to the PLA’s understanding of the paramount importance of the cognitive domain is their concept of system-of-systems warfare, which views modern warfare as a clash between opposing operational systems rather than the traditional focus on units, arms, services, and platforms, as observed in earlier eras. The confrontation of systems extends beyond the conventional physical domains of land, sea, and air to include outer space, cyberspace, electromagnetic fields, and, critically, the cognitive domain. The cornerstone of the PLA’s current victory strategy involves effectively conducting “system destruction warfare,” aiming to incapacitate and potentially dismantle vital functions within an adversary’s operational systems. As per this theory, the adversary reaches a point of losing the will and ability to resist once its operational systems fail to function effectively. At the core of every system is the mind: the main target in cognitive domain operations. While aiming for “system destruction,” system warfare also views “system survival” as a main objective. For the cognitive domain, the PLA must fortify its soldiers’ minds to maintain their will to fight and optimal decision-making capabilities.

System Destruction

Social Media

The main battlefield identified in the cognitive domain is social media platforms.⁶ China, through extensive research and development of its own platforms, understands the power of social media to shape narratives and cognition over events and actions. In the *PLA Daily* article “Cognitive Confrontation on the Social Media Battlefield,” authors Duan Wenling and Liu Jiali break down four confrontational actions to ensure victory with social media: information disturbance, discourse competition, public opinion blackout, and information blockade (table 12.1). The goal is to achieve an “invisible manipulation” and “invisible embedding” of information production “to shape the target audience’s macro framework for recognizing, defining, and understanding events.”⁷ By shaping narratives on social media, China aims to create a more favorable environment for the Chinese Communist Party (CCP) at home and abroad.

Table 12.1. Confrontational actions to ensure victory with social media

<i>Confrontational Action</i>	<i>Description</i>
Information disturbance [信息扰动]	Use official media channels to push a targeted narrative.
Discourse competition [话语竞争]	Subtly and gradually shape cognition by targeting existing bias (cognitive cocoon).
Public opinion blackout [舆论遮蔽]	Flood social media with a specific narrative to influence the direction of public opinion.
Information blockade [信息封锁]	Technical attacks, blockades, and even physical destruction of the enemy’s information communication channels.

Source: Developed from Duan Wenling [段文灵] and Liu Jiali [刘甲立], “Cognitive Confrontation on the Social Media Battlefield” [社交媒体战场上的认知对抗], *PLA Daily*, February 2, 2023, <http://www.81.cn/>.

The first type of confrontational action is information disturbance; the authors describe this as “publishing specific information on social media to influence the target audience’s understanding of the real combat situation and then shape their positions and change their actions.”⁸ Here, the idea is to use official media channels like CGTN, *Global Times*, and Xinhua News to distribute specific messaging. The

real-world example given to explain this type of action is what was dubbed the “Twitter War” in 2014 between Israel and Palestine, where the Israeli Defense Force and the Qassam Brigade used Twitter to gain support. Information disturbance uses official social media accounts to help push and shape a narrative in specific ways. While the Chinese authors believe that certain aspects of Palestinian and Israeli social media activity were effective, they conclude that the Palestinians did better in achieving their goal to “win international support by portraying an image of being weak and the victim.”⁹ Although social media did not exist at the time of Deng Xiaoping’s strategy of *Tao Guang Yang Hui* (韬光养晦)—literally translated as “Hide brightness, nourish obscurity”—it is reminiscent of the idea of information disturbance. China created a specific message to target the United States (and the West more broadly) under the official messaging of the CCP, that China was a humble nation focused on economic development and friendly relationships with other countries. This narrative was powerful for decades in shaping US and other nations’ policies toward China.

The second type of confrontational action is discourse competition, which relies on a much more subtle and gradual approach to shape cognition. Within discourse competition, the authors describe what they dub “trolling strategy” [拖钓] as “spreading narratives through social media and online comments, gradually affecting public perception, and then helping achieve war or political goals.”¹⁰ The idea is to “fuel the flames” of existing biases and manipulate emotional psychology utilizing a comprehensive analysis and calculation of users’ personal identity, psychological characteristics, behavioral habits, interests, and preferences to influence and deepen a desired narrative. Algorithmic recommendations will push more and more information to target audiences with desired biases. Over time, the emotion and bias will grow, and the user will reject information that does not align with their perspective to create a “cognitive cocoon” [认知茧房].¹¹ The authors cite the influence that “invisible manipulation” and “invisible embedding” can have on social media platforms such as Facebook and Twitter (now X) in the context of international events.

The third type of confrontational action is public opinion blackout, with the goal of flooding social media with a specific narrative to influence the direction of public opinion. The main tool used to “black out” public opinion is bots that quickly spread the desired narrative. The authors reference studies that suggest a common and effective method

of exerting cognitive influence is to use machine learning to mine user emotions and prejudices to screen and target the most susceptible audiences, then quickly and intensively “shoot” customized “spiritual ammunition” to the target group.¹²

Finally, the fourth type of confrontational action, information blockade, focuses on “carrying out technical attacks, blockades, and even physical destruction of the enemy’s information communication channels.”¹³ The goal is to monopolize and control information flow by preventing an adversary from disseminating information effectively. Duan and Liu believe the United States has a huge advantage with blocking information. They cite that “in 2009, the U.S. government authorized Microsoft to cut off the Internet instant messaging ports of Syria, Iran, Cuba, and other countries, paralyzing their networks and trying to ‘erase’ them from the world Internet.” The authors also mention that in 2022, Facebook “publicly announced restrictions on some media in Russia, Iran, and other countries by deleting posts negative toward the United States to gain an advantage in cognitive confrontation.”¹⁴

However, as the authors note, it is difficult to completely block an opponent’s information in practice, and the social media battlefield will always have some level of varying and false information. With the rise in popularity of TikTok, China conceivably has the ability to shape narratives and block negative information. For example, in 2019, TikTok reportedly suspended the account of a 17-year-old user in New Jersey after she posted a viral video criticizing the Chinese government’s treatment of the Uyghur ethnic minority.¹⁵ In the future, as China attempts to be the first mover in shaping what will be known as the metaverse, it sees great potential to better control how the CCP’s story is told. It did not invent the Internet, but it can be at the forefront of its future.

Generative Artificial Intelligence (GenAI)

From the perspective outlined in PLA media, GenAI’s most immediate military application lies in significantly enhancing human-machine interaction. Its proficiency in comprehending human and machine languages serves as a bridge between the two realms. According to a PLA author, GenAI enables machines to “listen” and interpret human language, “observe” human actions and expressions, “comprehend” human emotions and intentions, and “articulate” the process and outcomes of calculations in a way humans can easily understand.¹⁶ This

advance is expected to streamline task execution, reduce errors, simplify the utilization of military weapon systems, and enhance the rapid comprehension of extensive datasets in a more intuitive manner. This enhanced human-machine interaction will play a pivotal role in the cognitive domain.

In numerous PLA media outlets, there is a prevalent discourse on the deployment of GenAI in the cognitive domain. In a PLA article titled “How ChatGPT Will Affect the Future of Warfare,” the authors assert that “ChatGPT will raise the intensity of cognitive warfare to a whole new level.”¹⁷ At an individual level, they envision the potential to replicate individuals and produce nuanced, personalized content across diverse Internet topics. This capability could involve mimicking high-profile government officials so believably that it fosters confusion or potentially allows access to sensitive material. On a societal scale, GenAI is seen as having the capacity to “efficiently generate massive amounts of fake news, fake pictures, and even fake videos to confuse the public.”¹⁸ Another PLA article, “Military Application of Large Model Technology,” explores the anticipated consequences of GenAI use, emphasizing the objective to “destroy the image of the government, change the standpoint of the people, divide society, and overthrow the regime.”¹⁹ GenAI is identified as strategically targeting the primary battlefield in the cognitive domain—the human mind—leveraging emotions such as fear, anxiety, and suspicion to cultivate an atmosphere of insecurity, uncertainty, and mistrust. This approach aims to introduce doubts into decision-making processes at the highest echelons of command.

Metaverse

China aspires to be a dominant player in the metaverse, aiming to establish a strategic advantage with the potential to gain an upper hand in the cognitive domain.²⁰ Since 2021 was dubbed year one of the metaverse in China, there has been extensive investment by local government, tech companies, major conferences, and studies related to the development and future of the metaverse. Even the PLA has looked at potential military applications and how to build its own military metaverse, dubbed the “battleverse.” The CCP believes the Internet has evolved into a crucial channel for cultural dissemination and providing public cultural services, becoming a significant element in cultural construction. President Xi frequently characterizes the Internet in China as a communal or “spiritual home.” In a 2016

cyber symposium, Xi emphasized, “Cyberspace is the common spiritual home of hundreds of millions of people.”²¹ On November 19, 2021, in his congratulatory letter to the inaugural China Cyber Civilization Conference, Xi highlighted cyber civilization as integral to social civilization and a crucial domain for constructing a resilient cyber nation. Considering the Internet’s status as China’s “spiritual home” and the metaverse’s perceived evolution from the Internet, it is logical for the Chinese Communist Party to be invested in influencing its development.

The CCP holds the potential to shape the perceptions, experiences, and even emotions of Chinese citizens (and potentially a global audience if market dominance is achieved) as it engages in creating a metaverse civilization aligned with the Party’s objectives and strategic interests. Any content deemed detrimental to the Party’s interests can be precisely excised and subjected to censorship measures. Moreover, as PLA authors write, because the metaverse is an immersive experience, with the possibility that all senses are utilized, the cognitive domain operations success rate could be elevated. The author of “Smart Propagation: An Important Field of Cognitive Domain Operations,” published by China’s National Defense University, states, “Build an immersive virtual environment, which not only expands the user’s sensory space and sensory dimensions, but also naturally comes with strong sensory stimulation and perceptual cognitive bias, which wears on the user’s mind.” With a more tangible and interactive environment, the author argues, you will be better able to “penetrate psychological cracks” and “incite emotions or impose moral coercion, destroy their emotional dependence, destroy their value support, and then shock, occupy or even polarize the mind of the target object.”²²

System Survival

Enhancing Ideology Dissemination with Tech

The Ministry of National Defense Network article “Prevent Mental Rickets,” aimed at a Chinese military audience, explains, “Thought is the forerunner of action, and theory is the guide to practice. To replenish mental ‘calcium’ and prevent mental ‘rickets’ we must arm our minds with scientific theories.”²³ Of course, in the view of the CCP, the theories every good soldier (and citizen) must follow include a belief

in Marxism, socialism, and communism but, most of all, a strict adherence to Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era (XJPT) to fortify the mind. Every PLA member must study and understand XJPT and the Marxist positions, viewpoints, and methods that run through it, so that they can be “clear-sighted.”²⁴

To ensure that the PLA is on track in its continuous objective to fortify the minds of its military, it has an extensive Political Work system in which most individual units (as well as navy vessels) have political officers. The “PLA Dictionary of Military Terms” defines *political work* as “the ideological work and organizational work of the Chinese Communist Party in the People’s Liberation Army. It is an important factor in the combat effectiveness of the army, the fundamental guarantee for the realization of the party’s absolute leadership over the army and the fulfillment of its functions and missions, and the lifeline of the People’s Liberation Army.” Political commissars instill doctrine in the military personnel, monitor morale, and oversee promotions. Under the leadership of Xi Jinping, political work has been strengthened, with estimates that troops spend a quarter of their time on political work.²⁵

Adding to the efforts of political work, technology has been adopted to shape PLA minds with XJPT online classrooms and an app for smartphones. Soldiers stationed anywhere can access online classrooms that help ensure they understand XJPT and loyalty to the Party. As an extension of the online classrooms, the app “Study Xi Strong Country” [学习强国] uses the pun *xuexi*, the word for “study” but also containing the president’s name, playing on the idea that users must study Xi. Released in 2019, the app quickly became the most popular throughout China (fig. 12.1).

The comprehensive little red app enables users to access state media news reports, engage in video chats with friends, create personal schedules, and send monetary “red envelopes.” Featuring a messaging function akin to Snapchat, where messages vanish after being read, one of the app’s paramount functions is aiding users in refreshing their understanding of Xi Jinping’s ideology. CCP members and the PLA are pressured to use the app and do well on weekly quizzes. In essence, the app allows administrators to monitor who has strong *qi* and who may need additional study.



Figure 12.1. Study (Xi) Strong Country app home screen. A screen grab from the Study the Great Nation app. (Source: Javier C. Hernández, “The Hottest App in China Teaches Citizens About Their Leader — and, Yes, There’s a Test,” *The New York Times*, April 7, 2019, <https://www.nytimes.com/>.)

Wearable Tech

The CCP is building a mental toolset for its soldiers that is intended to foster a deep loyalty to and understanding of the ideological underpinnings of the CCP and combat negative information about the Party. In addition, the realities of war bring their own cognitive challenges. The *PLA Daily* article “Cultivate a Good Combat Psychology” notes that officers and soldiers are prone to sensory disorders and other problems that can impact judgment and decision-making.²⁶ To address and overcome the mental stress of combat, the authors emphasize the need to build training environments that will “improve the psychological adaptation, stability and endurance of officers and soldiers on the battlefield.”²⁷

While the use of nontechnical means to assess soldiers are still in use, such as “anti-stress training halls, psychological behavior training fields, and group stress training halls” that act as “a spiritual station for officers and soldiers to provide psychological consultation, emotional release, and physical and mental adjustment,” the PLA has also turned to technology.²⁸ In a growing number of units, each soldier is given a smart sensor bracelet that can provide “physiological data in real time, and promptly dispatches a psychological counselor to carry

out psychological counseling.”²⁹ The bracelets are part of what the PLA has dubbed their Intelligent Psychological Monitoring System [智能心理监测系统]. The system allows each unit to “continuously record the facial information of officers and soldiers, judge the psychological state of officers and soldiers in real time through data feedback, and archive them.”³⁰

VR Therapy

A recent addition to the Intelligent Psychological Monitoring System, VR for therapeutic applications, is being tested by a PLA Army unit for use. A recent Ministry of National Defense Network article, “Give Officers and Soldiers a ‘Brave Heart,’” tells the story of a tank driver named Shi Yongmin [石永敏].³¹ In his assessments, he tested well below average and appeared to have little self-confidence. Sun Zhiqiang, who is described as the psychological backbone of the unit, took Shi Yongmin into the brigade psychological service center to begin the assessment of his mental state. Based on the system data analysis results, the psychological counselor guided Shi Yongmin to use a VR psychological training system to carry out targeted psychological strengthening training.

While the specific details of the VR training used by Shi were not disclosed in the article, the author mentions that the unit has a full immersion VR platform that creates realistic battlefield environments, such as artillery blockades, mixed minefields, and smoke obstacles. The PLA has seen success using high-stress VR simulations to make officers and soldiers feel like they are in actual combat. With firsthand data they collect from training sessions, they can better prepare soldiers for future combat. When soldiers experience mentally demanding scenarios in a VR environment, they can “effectively overcome psychological barriers that commonly occur under actual combat conditions.”³²

Decision-Making

C2 and Technology

In a Ministry of National Defense article, “Insight Into New Changes in Intelligent Command and Control,” the author observes how command and control is evolving because of technology.³³ The traditional command organization has the commander as the core, and the com-

mander's ability largely determines the overall planning and decision-making capabilities of the command organization. In the future of warfare, the author believes command effectiveness will depend not only on the commander's strategy and command art but also on the "combined effect of the commander and the intelligent system."³⁴ Current and emerging technologies can take substantial amounts of data, give better situational awareness, and optimize decision-making.

Generative AI

Along with supporting cognitive domain operations, the PLA believes GenAI can play a pivotal role in helping commanders by providing courses of action to quickly and effectively defeat an adversary. The PLA is actively looking to speed up the research and development of military intelligent decision-making assistance systems.³⁵ The article "Combat + ChatGPT, What Kind of Sparks Will Be Hit?" indicates that "ChatGPT is expected to be used to accurately analyze the combat requirements put forward by the commander, and generate an action reference plan on this basis, providing a new way and means for the rapid and reasonable allocation of combat forces in future wars, and greatly shortening the combat preparation and implementation cycle."³⁶

The concept revolves around integrating GenAI extensively within the OODA loop, ensuring commanders access real-time intelligence on enemy positioning and actions. This capability is achieved by swiftly collecting and analyzing vast intelligence data from diverse sources and enabling rapid and precise threat assessments. Utilizing this assessment, commanders can employ GenAI to scrutinize and compare multiple combat action plans, selecting the one that best aligns with their overarching strategy. Additionally, GenAI could enhance "the autonomy of command and decision-making,"³⁷ potentially yielding multiple advantages by augmenting speed and efficiency. This framework might lead to a level of decentralized command where troops, previously reliant on orders, gain more autonomy, particularly in scenarios where communication channels are disrupted.

Augmented Reality (AR) Helmet

In the military documentary "Chasing Dreams" on China's state-run media CCTV aimed at promoting the PLA's military capabilities and weapons, soldiers were shown wearing helmets with AR capabilities

(figs. 12.2 and 12.3). The high-tech helmets were said to provide soldiers “real-time battlefield information, including minefield detection, route planning, battlefield distance and other useful information.” Additionally, the documentary noted that logistics command center personnel can also wear high-tech helmets to discuss simulated routes with colleagues and transmit combat information to frontline soldiers.³⁸



Figure 12.2. PLA AR goggles prototype. (Source: Zhang Weixuan, “The People’s Liberation Army’s New Helmet Is Exposed! Combined with AR Head-Up Display to Display Real-Time Battlefield Information,” Newtalk News, August 7, 2023, <https://newtalk.tw/>. [Video no longer available.]



Figure 12.3. Simulated perspective of PLA AR goggles. (Source: Zhang Weixuan, “The People’s Liberation Army’s New Helmet Is Exposed! Combined with AR Head-Up Display to Display Real-Time Battlefield Information,” Newtalk News, August 7, 2023, <https://newtalk.tw/>.)

Digital Twin

The People's Liberation Army also sees major value in digital twin technology as it continues to enhance its capabilities in the “battleverse.”³⁹ In a 2021 interview, Maj. Gen. Wang Mingxiao, a deputy to the National People's Congress and a senior engineer at the Army Research Institute, stated that digital twin technology will “help realize the strategic transformation of battlefield situational awareness and planning capabilities.”⁴⁰ The goal is to create a force multiplier that will allow the PLA to better prepare and win future conflicts with an information advantage that creates decision dominance.⁴¹ Digital twin technology could significantly bolster the PLA's understanding of potential outcomes of a Taiwan invasion or other military endeavors. Should the CCP opt for an invasion, digital twins, with GenAI, could assist in formulating optimal strategies, fortifying vulnerabilities, and swiftly adjusting tactics as the conflict unfolds.

Brain-Computer Interface Technology

With brain-computer interface technologies like Neuralink in development, the PLA is beginning to discuss using the technology on the battlefield (fig. 12.4).

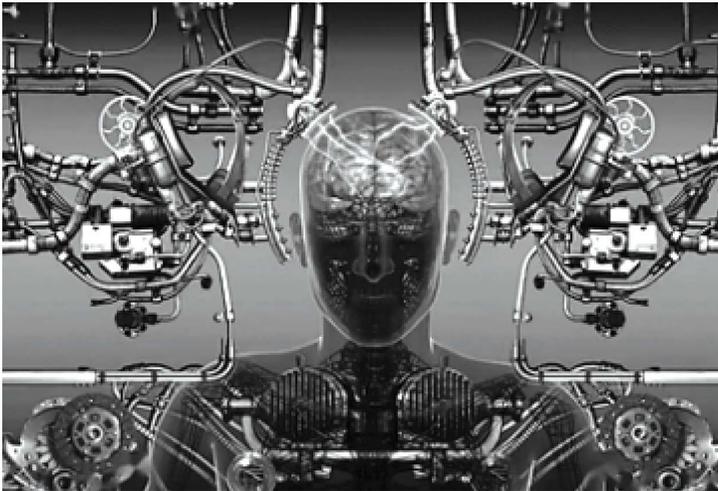


Figure 12.4. Conceptual drawing of brain-computer interface. Li Yue [李悦]; Liu Gang 刘港], “Brain-Computer Interface Technology Has Made New Progress” [脑机接口技术又有新进展], Ministry of National Defense Network, accessed August 19, 2023, <http://www.81.cn/>.

The authors of “Brain-Computer Interface Technology Has Made New Progress” explore the possibilities this technology could bring to warfare. They write that brain-computer interface technology could help humans improve the speed and accuracy of decision-making. On the battlefield, soldiers have to “see in all directions and hear in all directions,”⁴² which adds significant cognitive load to their physical senses. Brain-computer interface technology could theoretically transmit information from front-line survey equipment, such as drones and fighter jets, directly to the relevant areas of the user’s brain, bypassing the use of physical senses, effectively enhancing the user’s observation of the battlefield and improving decision-making speed. The authors conclude that on the battlefield of the future, brain-computer interface technology is likely to become a major combat advantage. In some cases, they believe that human beings will not need to be on the battlefield in person; rather, they will only need to serve as terminals to transfer their thoughts to AI machines so that they can realize “seamless cognitive cooperation.”

Conclusion

Every individual’s mind in the United States, along with our allies and partners, is a battleground on which China wants to prevail. However, in many strategic documents, such as the *2022 National Defense Strategy of the United States*, the cognitive domain is not addressed beyond the mention of misinformation. The PLA and the CCP, more specifically, understand the impact of winning in the cognitive domain and are actively engaged in developing technology to achieve that goal. For example, Taiwan is a nation that the United States supports and views as an ally. However, what happens if enough Americans, politicians, or influential people begin to believe it is simply a territory of China? Perhaps they will be convinced that using resources to defend Taiwan is a waste and simply interference of an “internal matter.” Chinese diplomats in interviews have said, “Do Americans even know where Taiwan is on the map?” For now, most Americans believe Taiwan should be defended, but in time this mindset could be eroded through China’s technologically driven cognitive domain operations. If enough Americans are convinced, when China takes Taiwan, we will do nothing. More perniciously, perhaps more Americans will grow skeptical of our form of government and attempt to sow doubt or disrupt democracy

in some way. Cognition and emotion could be exploited to degrade the United States from within, giving China greater strength to shape the world in its image and according to its ideology.

The United States and its allies and partners must do more to defend our minds, not just of leaders or military personnel, but of all of society. K-12 education must include critical thinking courses where healthy skepticism is taught and how to always look further than headlines or the latest TikTok video. Technology, such as the metaverse, will create more immersive virtual worlds in which all senses are engaged. This environment, particularly if China gains first-mover advantages, will be rife with CCP influence campaigns both obvious and subtle to shape cognition as they desire. Moreover, our decision-makers in the military and elsewhere must fortify their minds and utilize technology to cut through the fog of war and make optimal decisions. In the battle for our minds, the United States and our allies must prevail.

Notes

1. Yang Cunshe [杨存社], "Take the Pulse of Combat in the Quasi-Cognitive Domain" [把准认知域作战之脉], *PLA Daily*, August 16, 2022, <http://www.81.cn/>.
2. Li Minghai [李明海], "Perspective on the Evolution Trend of Cognitive Warfare" [透视认知战演变趋势], *PLA Daily*, accessed September 29, 2022, <http://www.81.cn/>.
3. Zhang Guangsheng [张广胜] et al., "A Brief Analysis of the Basics of Cognitive Domain Operations" [浅析认知域作战的基本要义], *PLA Daily*, accessed September 8, 2022, <http://www.81.cn/>.
4. Wei Changhao [魏昶昊], "Prevent Mental 'Rickets'" [预防精神上的“软骨病”], Ministry of National Defense Network, October 24, 2023, <http://www.81.cn/>.
5. Zhang Zhiwei [张智伟], "Cognitive Domain Operations from the Perspective of Intelligence: Emotional Conflict Becomes a Prominent Attribute of Cognitive Domain Operations" [智能化视阈下的认知域作战:情感冲突成为认知域作战突出属性], *PLA Daily*, December 8, 2022, <http://www.81.cn/>.
6. Yang, "Take the Pulse of Combat."
7. Duan Wenling [段文灵] and Liu Jiali [刘甲立], "Cognitive Confrontation on the Social Media Battlefield" [社交媒体战场上的认知对抗], *PLA Daily*, February 2, 2023, <http://www.81.cn/>.
8. Duan and Liu.
9. Duan and Liu.
10. Duan and Liu.
11. Li Xiaoyang [李晓阳], "Smart Propagation: An Important Field of Cognitive Domain Operations" [智能传播: 认知域作战的重要场域], *PLA Daily*, April 18, 2023, <http://www.81.cn/>.
12. Duan and Liu, "Cognitive Confrontation."
13. Duan and Liu.
14. Duan and Liu.
15. Will Feuer, "TikTok Says It Doesn't Censor Content, but a User Was Just Locked Out After a Viral Post Criticizing China," CNBC, November 26, 2019, <https://www.cnbc.com/>.

16. Zhang Guangsheng and Tian Ling [张广胜; 田玲], “How Generative AI Can Affect the Future of Warfare” [生成式AI如何影响未来战争], *PLA Daily*, April 18, 2023, <http://www.81.cn/>.

17. Si Jia [司嘉], “How ChatGPT Will Affect the Future of Warfare” [ChatGPT将如何影响未来战争形态], *China Youth Daily*, accessed March 31, 2023, <https://zqb.cyol.com/>.

18. Shen Bilong [沈弼龙], “Military Application of Large Model Technology” [大模型技术的军事应用], *PLA Daily*, April 11, 2023, <http://www.81.cn/>.

19. Shen.

20. To learn more about what China is doing in the metaverse, read Josh Baughman, “Enter the Battlevverse: China’s Metaverse War,” *Military Cyber Affairs* 5, no. 1 (May 2022): Article 2, <https://digitalcommons.usf.edu/>

21. “Some People in China Help the Party Police the Internet,” *The Economist*, January 18, 2020, <https://www.economist.com/>.

22. Li, “Smart Propagation.”

23. Wei Changhao [魏昶昊], “Prevent Mental ‘Rickets’” [预防精神上的“软骨病”], Ministry of National Defense Network, accessed October 27, 2023, <http://www.81.cn/>.

24. Wei.

25. *The Economist*, “Xi Jinping Is Obsessed with Political Loyalty in the PLA,” November 6, 2023, <https://www.economist.com/>.

26. Chen Jing [陈静] et al., “Cultivate a Good Combat Psychology” [塑造良好作战心理], *PLA Daily*, December 13, 2022, <http://www.81.cn/>.

27. Chen.

28. Li Qian [李倩] and Xue Weigao [薛维高], “Smart Devices Are Embedded in Wartime Psychological Work” [智能设备嵌入战时心理工作], *PLA Daily*, August 15, 2022, <http://www.81.cn/>.

29. Li and Xue.

30. Li and Xue.

31. Zhang Dongpan [张东盼] and Liu Guanliang [刘冠良], “Give Officers and Soldiers a ‘Brave Heart’” [给官兵一颗“勇敢的心”], Ministry of National Defense Network, October 26, 2023, <http://www.81.cn/>.

32. Zhang and Liu.

33. Nie Xiaoli [聂晓丽], “Insights into New Changes in Intelligent Command and Control” [洞悉智能化指挥控制新变化], Ministry of National Defense Network, October 26, 2023, http://www.81.cn/szb_223187/.

34. Nie.

35. Li Jiajun [李佳君], “Thoughts from the Popularity of ChatGPT” [由ChatGPT走红想到的], *PLA Daily*, March 2, 2023, <http://www.81.cn/>.

36. Hu Yushan [胡玉山], “Combat + ChatGPT, What Kind of Sparks Will Be Hit?” [作战+ChatGPT, 会撞出什么样火花], *PLA Daily*, March 21, 2023, <http://www.81.cn/>.

37. Zhang Guangsheng [张广胜] and Tian Ling [田玲], “How Generative AI Can Affect the Future of Warfare” [生成式AI如何影响未来战争], *PLA Daily*, April 18, 2023, <http://www.81.cn/>.

38. Zhang Weixuan, “The People’s Liberation Army’s New Helmet Is Exposed! Combined with AR Head-Up Display to Display Real-Time Battlefield Information,” *Newtalk News*, August 7, 2023, <https://newtalk.tw/>.

39. *Digital twin*, as defined by IBM, is “a virtual model designed to accurately reflect a physical object.” Alecio Binotto, “Transforming Telecom Tower Workflows with IBM Digital Twin Platform on AWS,” IBM, January 12, 2023, <https://www.ibm.com/>. To learn more about China’s Digital Twin Strategy, see Joshua Baughman, “Enhancing the Battlevverse: The People’s Liberation’s Army’s Digital Twin Strategy,” *Military Cyber*

Affairs 6, no. 1 (2023): Article 1, <https://doi.org/10.5038/2378-0789.6.1.1091>. Available at <https://digitalcommons.usf.edu/>.

40. National People's Congress, "Wang Mingxiao, Deputy to the National People's Congress: Speed Up the Military Application of Digital Twin Technology," *PLA Daily*, March 1, 2021, <http://www.81.cn/>.

41. *Decision dominance* is "a desired state in which a commander can sense, understand, decide, act, and assess faster more efficiently than an adversary." *Information advantage* is "a condition when a force holds the initiative in terms of relevant actor behavior, situational understanding, and decision-making using all military capabilities." "Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art During Multi-Domain Operations," *Cyber Defense Review*, November 15, 2021, <https://cyberdefensereview.army.mil/>. To learn more about these concepts, read Ian Sullivan's work, "Thoughts on Information Advantage," <https://madsciblog.tradoc.army.mil/>; Norman W. Wade, *INFO1: The Information Operations & Capabilities SMARTbook (Guide to Information Operations & the IRCs)* (The Lightning Press, 2021), <https://www.thelightningpress.com/>; and TRADOC (US Army Training and Doctrine Command) Pamphlet 525-92, *The Operational Environment 2024–2034: Large-Scale Combat Operations*, December 5, 2024, <https://rdl.train.army.mil/catalog-ws/>.

42. Li and Liu.

Part 5

**THE QUESTION OF WILL AND
SUPPRESSION OF PERFORMANCE**

Chapter 13

First the Mind, Then the Tech

Focusing on the Human Aspect of the Mind-Tech Nexus for Improved Investments

Ben Connable,

Georgetown University and Center for Naval Analyses

Abstract

This chapter describes a substantial gap in the collective military understanding of the human as the most important element of the Mind-Tech Nexus. Present investments in human enhancement, monitoring, and human-robot teaming have the wrong order of priorities, with technical design and rapid fielding favored over methodical research to anticipate cognitive and psychological impacts on the soldiers intended to wear and apply the new technology. Three sequential steps should be taken to rectify this gap and provide a basis for improved design and investment: Agree upon holistic concepts, definitions, and models of (1) the human, (2) the will to fight, and (3) combat effectiveness.

The use of force demands that we should understand our own natures, for the most basic and the most complicated weapon system is man.

—Brig. Gen. Shelford Bidwell

Modern Warfare: A Study of Men, Weapons and Theories

This chapter describes a fundamental flaw in the general Western approach to developing and funding technology designed to enhance human performance in war. Arguably, most investments in what this book describes as the Mind-Tech Nexus are made in an impractical reverse order: Innovative human-machine technology is envisioned and funded before the need for that technology is clearly described and before the human constraints and restraints on its prospective applications are studied. Concrete steps can be taken to reverse this illogical approach to advanced technology acquisition, all focused on

better defining, understanding, and explaining human dispositions and behavior in war. These include embracing a biopsychosocial concept and model of human behavior, assessing the will to fight, and integrating these behavioral concepts into a holistic description of combat effectiveness.

The Problem: Reverse-Order Theory and Investment

Western enthusiasm for human-machine integration, technical performance enhancement, and monitoring is profuse. Thousands of military technology companies large and small are perpetually engaged in hot competition for a slice of the enormous annual pool of defense funding—potentially \$850 billion in the United States in 2025—to provide a high-tech warfighting edge.¹ Program sponsors in the US Department of Defense and European defense ministries are particularly interested in applications that can reduce uncertainty, an often debilitating constant in war.²

Humans generate much of that uncertainty: They have inconsistent and often unpredictable behavioral patterns; their physical forms are widely varied and susceptible to degradation by every type of weapon and environmental extreme; and their sensors and processors—broadly, eyes, ears, and brains—can appear comparably archaic in an era of drones, thermal imagers, and artificial intelligence. Investing in advanced technology to improve the still ubiquitous human soldier is, *prima facie*, a logical step toward reducing uncertainty in war and increasing the likelihood of victory.

Investment in human enhancement is not, however, an unalloyed good.³ Absent realistic and sequentially logical design and planning, the direct application of technology to humans might actually hinder physical and cognitive performance and effectiveness in combat. Defense technology acquisition for human enhancement and monitoring is, generally, neither theoretically realistic nor sequentially logical. While no two defense programs are alike, and while thoughtful research underlies some new initiatives, the broad approach in at least the US defense-industrial complex can be boiled down to something like, “Wouldn’t it be cool if we could build a [insert technical capability here]?” Once the technical outcome has been envisioned, research and development teams work backward to insert the human into the

human-technology formula. The US Army's Integrated Visual Augmentation System (IVAS) appears to be a good example of this approach.⁴

Example of Reverse-Order Investment: IVAS

Army planners envisioned the Integrated Visual Augmentation System as part of then-Secretary of Defense James N. Mattis's directives to improve Soldier lethality. Mattis intended lethality to be human-centric, with some necessary technical improvements to sharpen human capabilities.

But at the outset, one of the lethality program's advisors, Maj. Gen. Robert Scales (USA, retired), sounded a prescient warning: "All too often when we bring things up inside the Beltway, it immediately devolves to material and programs and technology."⁵ Pressing ahead, Mattis created the Close Combat Lethality Task Force, and the services then created their own mirrored teams to find the best ways to increase lethality at the lowest tactical levels: the infantry squad and individual Soldier.⁶

Building from a decades-old "wouldn't it be cool if" concept—turning individual Soldiers into networked, high-tech, high-speed sensor-shooter processors—the Army's lethality team shepherded a nearly half-billion dollar investment in IVAS, a so-called mixed-reality (MR) goggle designed to provide Soldiers with enhanced vision, constant battle updates, and even a built-in digital compass.⁷ Microsoft quickly adapted its existing business-focused HoloLens 2 augmented reality goggles to meet the Army's rapid prototype and delivery demand for more lethality.⁸

Microsoft and the Army strapped the prototype goggles onto Soldiers to see how they would function in the field and to gauge their acceptance of the new technology. A heavily redacted US Army Inspector General's report on the IVAS program suggested acceptance was low.⁹ Another official report was more direct: "Soldiers continue to lack confidence in their ability to complete the most essential warfighting functions effectively and safely while wearing the IVAS in all mission scenarios." In other words, this half-billion dollar effort to enhance individual Soldier lethality with a high-tech wearable might instead be *reducing* Soldier lethality. Early-stage technology always has teething problems, but clearly something went wrong with the IVAS. What happened, and why does it matter for the Mind-Tech Nexus?

Putting aside all the potentially fixable technical hurdles—including screen fogging, limited field of view, distorted vision, and tech-generated

headaches—there are fundamental issues with IVAS development that exemplify the broader problems with reverse-design technology programming. The entire effort to improve Soldier lethality operates without definition or clear objective.¹⁰ Absent a collectively agreed-upon definition of lethality, it is not clear how the IVAS can make Soldiers more lethal.

There appears to be no good evidence that the Army derived its need statement for the IVAS from human behavioral or performance research, much of which is readily available from the Army's human research laboratories.¹¹ And perhaps most importantly, while Microsoft, the Army, and the DOD Inspector General work through the physiological and ergonomic issues with IVAS, at least in the public record they appear to be paying little attention to prospective psychological and cognitive concerns associated with rapid fielding of what the Army describes as “transformational” technology.¹²

Robotization's Hidden Dangers and Theoretical Gaps

Inadequate focus on the psychological and cognitive aspects of the Mind-Tech Nexus raises a number of concerns. Treating individual soldiers as sensor-shooter nodes in a networked team appears to be more a process of robotization than a narrow technical effort to enhance human performance.¹³ With each enhancement of a soldier's sensors and processors (eyes, ears, brain), uncertainty is ostensibly reduced, human weaknesses might be mitigated, and lethality might be increased. But what if these robotizing enhancements introduce new weaknesses to the soldier's nonrobotic processor—the brain—that might have unintended and difficult-to-perceive negative outcomes?

In the case of IVAS, what if a constant stream of new information overwhelms Soldiers' processing capacity, thereby eroding cognitive reaction time and distracting Soldiers from events transpiring right in front of them? Or what if the nature of that information is not only distracting but psychologically debilitating? How might constant awareness of the larger battlefield, including impending threats and friendly losses, affect a Soldier's *will to fight*, or the disposition and decision to fight, act, or persevere when needed?¹⁴ Can too much information be a bad thing, and has that consideration been built into the Army's design process?

Brain-computer interfacing (BCI) presents many of the same concerns. The Defense Advanced Research Projects Agency (DARPA) and individual technology firms are exploring ways to allow humans to control machines using brain signals, either through wearable headcaps or surgical implants.¹⁵ Instead of being robotized, individual Soldiers would be linked to robots through brain-machine transmission: a literal Mind-Tech Nexus. Implants could also be used to track Soldiers' locations and transmit biomedical information like heart rate and cortisol levels to help leaders monitor and, in some conceptual designs, to regulate stress by inhibiting adrenal function.¹⁶

There are some alarming tactical concerns associated with radio-transmitting brain implants.¹⁷ If friendly forces can track the signal coming out of a Soldier's head, then the enemy might track that signal as well. One could imagine an adversary locking on to Soldiers' implants and sending a drone swarm to finish off an entire unit with precise headshots.

Even if that somewhat fantastical situation does not arise, how might the constant presence of a commander in each Soldier's brain affect that Soldier's decision-making and willingness to take risks? What if an alarmingly high adrenal function is the body's healthy way of staying alive in combat, and artificially reducing that function makes Soldiers less responsive and more vulnerable to enemy fire? What if a Soldier's adaptability and aggressiveness—traits considered essential to success in combat in historical literature—decline as commanders micromanage troops from afar through their IVAS and brain implant?¹⁸

There may be good, practical answers to all these concerns. This is not a condemnation of IVAS, BCI, or any other Mind-Tech innovation. Instead, raising these concerns highlights broader failures that need to be addressed to maximize the benefit of technology and reduce its prospective disruptions: (1) The Western defense community has no generally agreed-upon holistic theory or practical starting point to assess and then help improve human performance in war; (2) fundamental theories and terms like *will to fight* are undefined and generally ignored in defense planning and innovation; and (3) there is no agreed upon theory, terminology, or practical description of the desired outcome of Mind-Tech investment in combat. The next sections of this chapter offer solutions to these three gaps in progressive order to develop a solid foundation for effective Mind-Tech design.

Setting a Holistic Baseline: The Biopsychosocial Conceptual Model

Presently, military investments in human-enhancement and monitoring technology are made without a clear military definition or understanding of the human either as an endogenous physiological, cognitive, and psychological system or as a more broadly realistic entity interacting in complex ways with the environment and other humans. In other words, we do not agree on the terms describing the most basic building block of the Mind-Tech Nexus: the human being. This gap in military knowledge reflects a long-standing roadblock in academic and scientific discourse. Instead of agreeing on a central definition and human model, scientific fields including psychology, anthropology, neurology, and sociology compete with one another to ascribe causal inference and explain human behavior and performance. For example, a psychologist might argue that the best behavioral predictor is the five-factor personality profile, while a neuroscientist might claim that it is the medial prefrontal cortex patterns and an anthropologist that it is cultural influences.¹⁹

Because there is no central understanding of the human, military technology investments intended to enhance or monitor the human are arguably built on a foundation of sand. This endeavor is loosely akin to the efforts to improve lethality without first defining it. To be fair, given the state of scientific knowledge in the early 2020s, it would be effectively impossible to define and model the human accurately and precisely. In any event, it is generally agreed that all models are imperfect and to some extent inaccurate.²⁰ More complex systems typically render less accurate models, and humans are perhaps infinitely complex. But it certainly would be possible for military organizations to settle on a general theory of human functioning and behavioral inclination and, at the very least, to develop a working conceptual model that could stand as the basis for Mind-Tech design and investment.²¹

There is ample research available to develop a basic conceptual model of the human. Probably thousands of proposed human physiological, cognitive, psychological, and even holistic all-factors models exist in the public domain. All are informative but all are imperfect, and none is universally suitable as a causal input-output model. The good news for military innovation designers and acquisition experts is that perfect modeling is unnecessary. Instead of pursuing a perfect

design, settling on a general holistic conceptual model of the human would be more useful, perhaps starting with George L. Engel's biopsychosocial conceptual model and, from that basis, deriving functional models for specific programs.²²

Engel was a cardiologist who believed medical professionals were making dangerously narrow diagnoses based on narrow data (e.g., physical symptoms) rather than viewing a person as a complex entity with important and consequential social relationships and environmental interactions. He proposed a simple holistic—or all encompassing—conceptual model of the human from molecule to nervous system to community to biosphere. Figure 13.1 depicts Engel's original concept of concentric and interrelated factors endogenous and exogenous to the individual human.

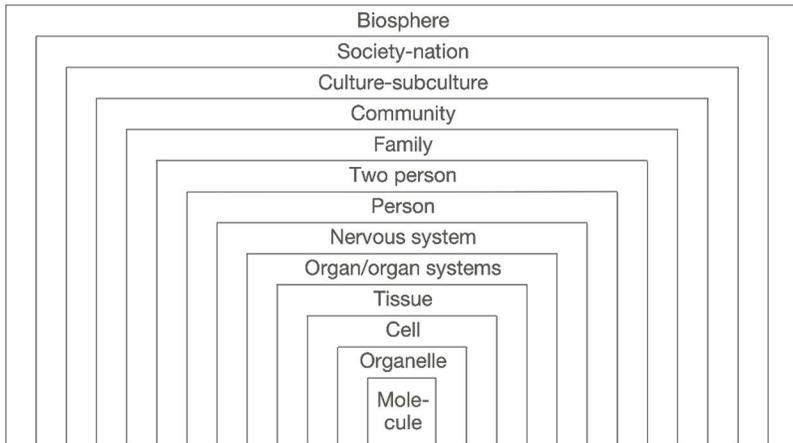


Figure 13.1. George L. Engel's biopsychosocial conceptual model. (Source: Ben Connable, "Authentically Describing and Forecasting Human Behavior for Policy Analysis," in *Adaptive Engagement in Undergoverned Spaces: Concepts, Challenges, and Prospects for New Approaches*, ed. Aaron B. Frank and Elizabeth M. Bartels [RAND Corporation, 2022], 451, <https://www.rand.org/>. Originally adapted from George L. Engel, "The Clinical Application of the Biopsychosocial Model," *American Journal of Psychiatry* 137, no. 5 [May 1980]: 537, <https://doi.org/10.1176/ajp.137.5.535>.)

This model is a basic and knowingly incomplete attempt to organize the latticed elements of human physiological, cognitive, psychological, social, and environmental factors. It has obvious gaps, and Engel was

even taken to task for calling his framework a model.²³ Yet Engel's diagram still provides a simple organizing basis for more involved conceptual and, eventually, functional modeling. Figure 13.2 (next page) depicts a system-of-systems approach to conceptualizing the human derived from Engel's general biopsychosocial concept. This RAND Corporation's centralized model of characteristics organizes the human in five interrelated systems models: (1) a personality model, (2) a cognitive process model, (3) a motivational model, (4) a cognitive schemas model, and (5) a physiological morphology model.²⁴

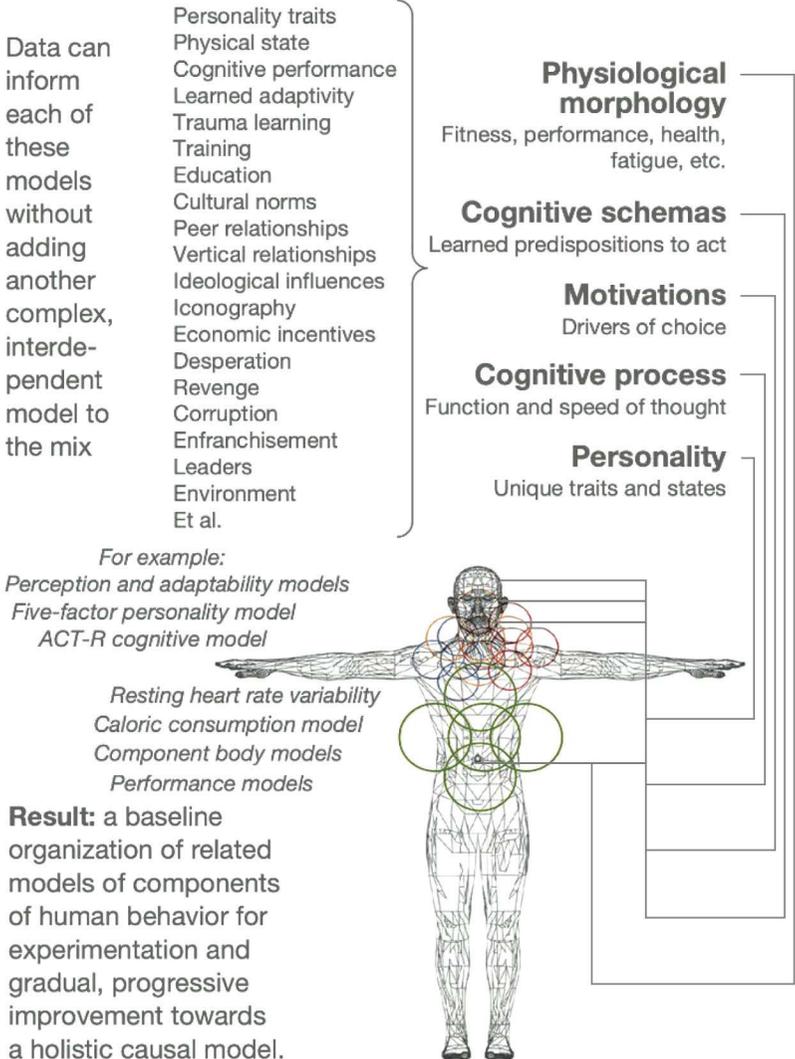
Each of these five system-of-systems models integrates several scientific fields and centuries of collective research. For example, the cognitive process model might include computational cognitive modeling, neurological modeling, and aspects of psychological behavioral modeling. The physiological model is the model of the human body and brain and would include subsystem models of the body's parts and functions as well as environmental and psychological impacts on physiological functioning. Together, this system-of-systems model is intended to be a holistic organizing framework to bring together the competing fields of human-focused scientific study. It progresses Engel's general biopsychosocial theory toward practical applications that can be used to help improve technology investment. Specifically, it provides a conceptual basis for the definition and assessment of the will to fight and then the more all-encompassing, outcome-focused understanding of combat effectiveness.

Understanding the Human Will to Fight

The will to fight is arguably the primary factor in warfare and, therefore, an essential component of human effectiveness in combat.²⁵ All Western military theory and doctrine is predicated on the Clausewitzian idea that war is a contest of opposing and irreconcilable wills and that the purpose of applying violence is to break the enemy's will to fight.²⁶ Yet Western military services generally pay lip service to the concept of will to fight in practice. It is not formally defined or clearly explained to officers or soldiers, and it is only tangentially applied to military planning and operations. Ignoring the will to fight has come at a high cost in places like Vietnam, Iraq, and Afghanistan, and most recently, it has led to strategic surprise in Ukraine.²⁷

Centralize models of human characteristics

Bring together closely-related types of information into one centralized model. Show how exogenous factors like culture, leadership and equipment affect the individual.



Legend ACT-R - adaptive control of thought – rational

Figure 13.2. Example of a system-of-systems model of human performance and behavior. (Source: Ben Connable, “Authentically Describing and Forecasting Human Behavior for Policy Analysis,” 459.)

The will to fight is also almost entirely ignored in the technology acquisition process.²⁸ Defining and improving the understanding of the will to fight can provide innovators and acquisitions professionals with the ability to assess, albeit with imperfect accuracy, the prospective impact of human enhancement and monitoring technology on soldiers' will. In 2018, RAND proposed a definition of the *will to fight*: It is the disposition and decision to fight, act, and persevere as needed.²⁹ Each word in this definition has specific meaning and practical relevance for human behavioral research and performance. *Disposition* equates to likelihood, a forecasting term that drives home the fact that human behavior modeling is uncertain. *Decision* implies human agency, a key underpinning for holistic human behavior modeling. Fighting, acting, and persevering incorporate combat and essential noncombat actions that still require the will to fight, extending this combat-focused concept to all military personnel engaged in war.

Building from a holistic theory of human behavior, and with a definition of the will to fight in place, it is possible to generate a holistic conceptual model of the will to fight and, from that model, an assessment tool. From there, more refined models can be used to help forecast the impact of technology on human behavior. Several models of the will to fight exist, and all should be explored for viability.³⁰ RAND's 2018 model is particularly designed to help military professionals assess and model the will to fight and to help integrate the will to fight into the kinds of computer simulations often used to support human enhancement and monitoring technology.

The RAND model takes a biopsychosocial approach to understanding and explaining the will to fight of both individual soldiers and, more directly, units of soldiers from the squad to the division level. It is intended to be applied as an assessment heuristic, not a quantitative input-output formula. While quantitative data should be included in will-to-fight assessments, complex human behavior does not lend itself to accurate and informative quantification.

Figure 13.3 shows the twenty-nine major factors and sixty-one subfactors of the RAND model in a concentric ring intended to help convey its holistic nature.³¹ The model includes factors at the individual, unit, organizational, state, and societal levels of analysis, including individual psychological profiles, esprit de corps, cohesion, leadership, training, support, discipline, integrity, quality of equipment, civil-military relations, and societal support. Each factor is relevant, as it influences the will to fight of a unit or individual within that unit.

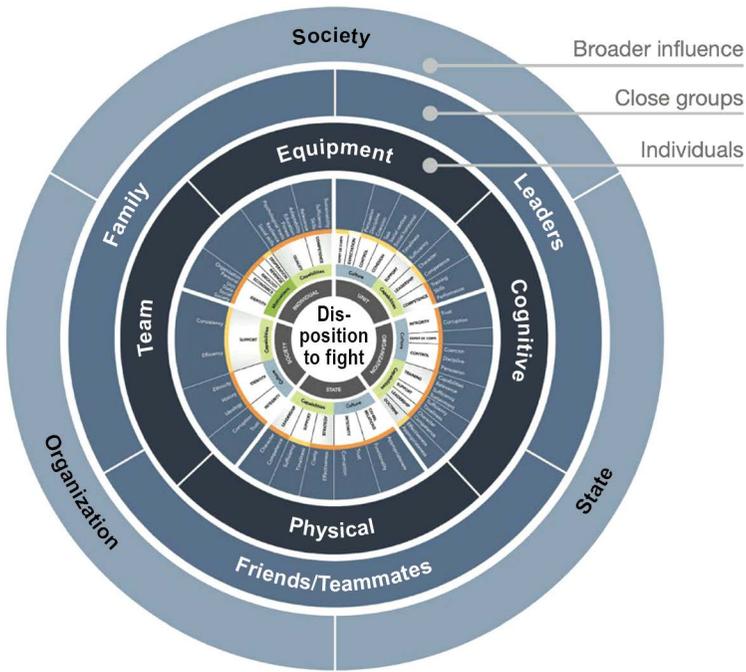


Figure 13.3. RAND will-to-fight model and conceptual rings. (Source: Ben Connable, “Authentically Describing and Forecasting Human Behavior for Policy Analysis,” in *Adaptive Engagement in Undergoverned Spaces: Concepts, Challenges, and Prospects for New Approaches*, ed. Aaron B. Frank and Elizabeth M. Bartels [RAND Corporation, 2022], 448, <https://www.rand.org/pubs/>.)

Focusing on the individual soldier level, the will-to-fight model offers a general roadmap to integrate a wide array of information in a system-of-systems assessment process. Figure 13.4 depicts the progressive layering of behavioral influence factors on a soldier, with clear comparison to Engel’s biopsychosocial concept. The individual has endogenous psychological and physical traits, life experiences, and longstanding cultural influences that have shaped cognitive schemas (basically, dispositional menus for behavioral selection), skills that either engender or weaken confidence. The individual then enters the military and goes through indoctrination, obtaining new behavioral influences while some older influences are weakened. Finally, the soldier joins a military unit, which introduces a specific local culture, immediate and influential social relationships, and

leadership dynamics.³² Individuals are still connected to the broader society and influenced by nonmilitary factors; no military organization is an isolated island.

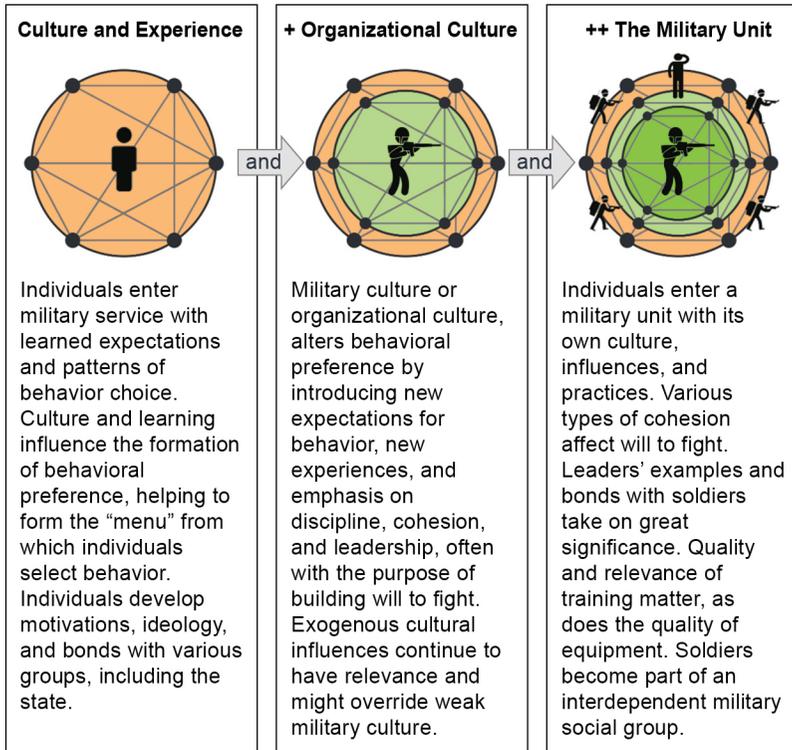


Figure 13.4. Individual will-to-fight factors and conceptual rings.

(Source: Ben Connable et al., *Will to Fight: Analyzing, Modeling, and Simulating the Will to Fight of Military Units* [RAND Corporation, 2018], 50, <https://www.rand.org/>.)

For technology design and acquisition, researchers can take this conceptual model and the holistic factors model, modify them, and then apply them to help identify ways in which specific technologies like IVAS or BCI might increase or weaken the will to fight of soldiers generally. For example, an integrated will-to-fight agent-based model like the one the US Army integrated into its OneSAF combat simulation could be used to create a range of potential-use case problems and opportunities to inform real-world experimentation and design.³³ Holistic human behavioral modeling might also allow for differentiation

between individual soldiers to help modify technology for varying traits. One-size-fits-all physical models do not effectively apply to large groups of soldiers (e.g., not every soldier wears the same uniform and boot sizes), and the same is true of cognitive and psychological models. A soldier deemed to be highly reactive to negative information or easily distracted by visual stimulus might receive an IVAS system tuned to transmit less data.

Agreeing on a will-to-fight definition, conceptual model, and perhaps family of assessment and practical models is an essential step toward building a holistic combat effectiveness model. Like the human being, lethality, and the will to fight, *combat effectiveness* is a key but as-yet undefined military term. Building a generally agreed-upon definition and at least conceptual model of combat effectiveness will provide the final building block in the foundation necessary for improved Mind-Tech investment.

Defining the Outcome: Combat Effectiveness

Absent a formal definition, *combat effectiveness* can be described as the likelihood that a military unit or organization will win a given fight.³⁴ While only loosely defined and understood, it is a common term employed by military leaders and planners to help determine the odds of combat success, to identify and shore up friendly weaknesses and employ friendly strengths, and to avoid the strengths and exploit the weaknesses of adversary forces. Lethality is an essential but subordinate component of combat effectiveness. A military force can be lethal but still have a low likelihood of winning a given fight due to many other factors. Combat effectiveness—like Engel’s biopsychosocial model and the will-to-fight model—is a holistic term intended to bring together all human and material aspects of war into a centralized assessment. Arguably, by defining and actualizing combat effectiveness, the need to define lethality will be minimized and a more useful basis for military Mind-Tech investment will be set.

Many experts have designed models of combat effectiveness for prospective use by Western military forces. Some of these have been applied. For example, for many years the US Army periodically used some version of the Soviet correlation-of-forces calculator, a tool that ascribed combat power ratings to mostly physical assets like tanks, planes, and artillery and then generated a comparative quantitative

output to determine the odds of success.³⁵ Trevor N. Dupuy and Gay M. Hammerman built the Soldier Capability-Army Combat Effectiveness (SCACE) model and tool to examine combat effectiveness in historic cases to inform modern planning, and Huba Wass de Czege designed a combat power assessment tool that incorporated nonmaterial capabilities like leadership and training into a holistic model.³⁶ All of these concepts and tools are informative, but none incorporates human factors with explanatory detail or the essential elements of human behavioral science theories and research. In most Western militaries, combat effectiveness therefore is primarily a calculation of physical power absent the human, mirroring the emphasis on tech in Mind-Tech design and innovation.

Like the conceptual models of the human and of human will to fight, any conceptual model of combat effectiveness will be necessarily imperfect and somewhat inaccurate. There probably are no general rules of military power that can be applied uniformly from case to case. For example, a model that assigned equal value to material and human factors—say, the number of tanks and the will to fight—would almost certainly fail to forecast cases like the 2014 Islamic State defeat of the Iraqi security forces, in which lightly armed but highly motivated Islamist militants shattered a quantitatively larger and far more physically powerful force of comparatively far less motivated Iraqi Army soldiers and Federal Police.³⁷

A realistic and useful combat effectiveness model and assessment tool will incorporate foundational models of human behavior, the will to fight, and material power together, taking into account the full range of existing scientific literature on all subjects rather than ascribing ad hoc values based on the subjective judgments of the modelers. It will provide military leaders, planners, and technology innovators with an output concept, model, and tool to answer essential questions about military capabilities and the Mind-Tech Nexus.

Circling back to IVAS and BCI, designers armed with a working model of the human, an agreed-upon model of the will to fight, and a practical model of combat effectiveness would be well prepared to identify, assess, and then conduct more refined simulations and real-world experiments to determine the holistic and inextricably interwoven material, technical, physiological, cognitive, and psychological aspects of their prospectively transformative innovations. This holistic scientific foundation for research and innovation would apply equally well to most other Mind-Tech designs and investments.

Conclusion

The tech part of the Mind-Tech Nexus is relatively straightforward and simplistic compared to the mind. While humans are complex, varied, and often unreliable and unpredictable, tech is perceived to offer comparatively simple, linear, stable, and finite solutions to military challenges. It is therefore unsurprising that technophilia permeates Western human enhancement design.

Technophilia drives programming and, together with the perverse incentives baked into the military acquisitions system, stifles the necessarily gradual, complex, and imperfect process needed to better understand the most esoteric yet critically important aspects of humans.³⁸ Few designers, program managers, or commercial vendors are incentivized or appear to be willing to take the hard steps necessary to integrate complex human behavioral considerations into human-focused technology strategies. Soldier lethality programs, of which IVAS and some aspects of BCI are part, may be bearing out Robert Scales's 2018 premonition: They appear to be fixated on technical and material innovation, perhaps at the expense of nontechnical innovations in training, leadership, and other aspects of nontechnical combat performance.³⁹

It would benefit everyone involved—and particularly the soldiers who serve as the test subjects for military technology programs—to put holistic conceptualization before technical design, to clearly define terms and desired outcomes before rapidly fielding new gear, and to invest in human behavioral research before sinking half a billion dollars or more into programs that have a good chance of falling short because they reflect a Tech-Mind approach to innovation and design.

Notes

1. Congressional Budget Office, “Long-Term Implications of the 2025 Future Years Defense Program,” November 2024, <https://www.cbo.gov/>.

2. US Marine Corps Doctrinal Publication 1 (MCDP-1), *Warfighting*, June 20, 1997, <https://www.marines.mil/>.

3. Other chapters in this book address ethical and moral concerns with human-technology, or Mind-Tech integration. This chapter focuses on effectiveness.

4. Given the partially closed-door nature of the design and development process, it is necessary to leave open the possibility that IVAS development proceeded differently. This assessment is drawn from publicly available sources, all of which seem to point to a reverse-order design process.

5. Robert Scales, quoted in Sydney J. Freedberg Jr., “Stop Wasting Infantry’s Time: Mattis Task Force,” *Breaking Defense*, April 13, 2018, <https://breakingdefense.com/>.

6. James N. Mattis, Secretary of Defense, Directive-type Memorandum (DTM)-18-001, “Establishment of the Close Combat Lethality Task Force (CCLTF),” March 16, 2018, incorporating change 1, December 28, 2018, <https://irp.fas.org/>.

7. Program Executive Office Soldier, “Product Manager – Integrated Visual Augmentation System,” accessed December 11, 2022, <https://www.peosoldier.army.mil/>.

8. Microsoft, “Hololens 2,” accessed December 11, 2022, <https://www.microsoft.com/>.

9. Department of Defense, (*U*) *Audit of the Army’s Integrated Visual Augmentation System* (Inspector General, April 20, 2022), <https://media.defense.gov/>.

10. If there is a clear definition of *lethality*, it has not been well publicized. For example, the definition is not included in US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, January 2025, Joint Electronic Library Plus. See W. A. Rivera and Arnel P. David, “Towards a More Comprehensive Understanding of Lethality,” *Small Wars Journal*, February 11, 2019, <https://smallwarsjournal.com/>.

11. These include the Army Research Laboratory, the Engineering Research and Development Center, and the Natick Soldier Systems Center. I leave open the possibility that I did not uncover evidence of logically sequential planning derived from a careful reading of existing scientific literature and research on human performance in combat.

12. US Army Chief of Staff James McConville, quoted in Frank Wolfe, “IVAS Will be ‘Transformational’ In Next Few Years, U.S. Army Chief Says,” *Defense Daily*, October 21, 2022, <https://www.defensedaily.com/>.

13. Literature on the robotization of humans is limited and generally focused on human-robot teaming. Zoomorphism, or the description of human behavior using animal behavioral terms, is not applicable here, and reverse anthropomorphism is insufficiently descriptive. Robotization in this context is, generally, a conscious effort to perceive and describe humans as machines and to transplant robotic characteristics and capabilities for endogenous human traits.

14. Ben Connable et al., *Will to Fight: Analyzing, Modeling, and Simulating the Will to Fight of Military Units* (RAND Corporation, 2018), <https://www.rand.org/>.

15. For example, see Anika Binnendijk et al., *Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment* (RAND Corporation, 2020), <https://www.rand.org/>.

16. Binnendijk et al., 16.

17. Ethical concerns with the Mind-Tech Nexus are addressed in other chapters in this book.

18. For more on adaptability and aggressiveness, see Ben Connable, “Warrior-Maverick Culture: The Evolution of Adaptability in the U.S. Marine Corps” (PhD diss., King’s College London, 2016), <https://kclpure.kcl.ac.uk/>.

19. These are broad generalizations that may trigger some readers. They are not intended to define or accurately represent the viewpoints of any individual or group of experts, only to help describe differences in perspective between the different parts of the academic and scientific communities.

20. Statistician George E. P. Box is purported to have said, “All models are wrong, but some are useful.” This phrase is broadly applied to all types of modeling, including human modeling. See George E. P. Box, “Science and Statistics,” *Journal of the American Statistical Association* 71, no. 356 (1976): 791–99, <https://www.sop.inria.fr/>.

21. A conceptual model, or conceptual framework, is a visualization of a process or function. See, for example, “Conceptual Models,” National Center for Postsecondary Improvement, Stanford Institute for Higher Education Research, 2003, <https://web.stanford.edu/>.

22. I describe Engel's model in some detail in Ben Connable, "Authentically Describing and Forecasting Human Behavior for Policy Analysis: A Review and a Path Forward," in *Adaptive Engagement in Undergoverned Spaces: Concepts, Challenges, and Prospects for New Approaches*, ed. Aaron B. Frank and Elizabeth M. Bartels (RAND Corporation, 2022), 431–62, <https://www.rand.org/>. Also see George L. Engel, "The Clinical Application of the Biopsychosocial Model," *American Journal of Psychiatry* 137, no. 5 (May 1980): 535–44, <https://doi.org/10.1176/ajp.137.5.535>; and Roy R. Gringer, ed., *Toward a Unified Theory of Human Behavior* (Basic Books, 1956).

23. See Connable, "Forecasting Human Behavior," for a discussion of these critiques and citation.

24. Connable, 459.

25. For a full discussion of the theories and concepts of will to fight and for a long bibliography of relevant sources, see Connable et al., *Will to Fight*.

26. For example, see US Army Doctrine Publication (ADP) 3-0, *Operations*, 2016; and MCDP-1, *Warfighting*. See also Carl von Clausewitz, *On War*, trans. J. J. Graham (Nicholas Trübner, London, 1873), <https://clausewitzstudies.org/>; and Beatrice Heuser, *Reading Clausewitz* (Pimlico, 2002).

27. For example, see Lt. Gen. Scott Berrier, USA, director, Defense Intelligence Agency, congressional testimony, and Director of National Intelligence Avril Haines Testimony on Global Threats and National Security, C-SPAN, May 10, 2022, <https://www.c-span.org/>.

28. Connable, "Forecasting Human Behavior."

29. Connable et al., *Will to Fight*, xi. The US Congress adopted this definition in the December 6th version of the 2023 National Defense Authorization Act, Sec. 6521(a) (2)(3), <https://www.intelligence.senate.gov/>.

30. For more on definitions, theories, and models of *will to fight*, see Ben Connable, "How to Assess the Will to Fight: A Roadmap for Building Institutional Capability," December 2022, <https://storage.googleapis.com/>.

31. This model is derived from the original model in Connable et al., *Will to Fight*, 2018. The 2018 report provides extensive detail, including explanatory figures, citations, and descriptions of each factor. Anyone interested in seeing how the model is applied should read Ben Connable, *Iraqi Army Will to Fight: A Will-to-Fight Case Study with Lessons for Western Security Force Assistance* (RAND Corporation, 2022), <https://www.rand.org/>.

32. It is entirely possible that societal cultural influences might have dominant influence over any one individual's behavioral selections. This is a broad conceptual diagram intended to help assess the will to fight of individuals, which will vary considerably from individual to individual.

33. RAND built and tested the will-to-fight module for the US Army's simulation program offices. This module was integrated into OneSAF and should remain available for use by OneSAF users as long as the simulation is supported. For more on the RAND process and OneSAF integration, see Glenn A. Hodges et al., "Human Behavior Representation Using the RAND Will to Fight Mode" (conference paper, Interservice/Industry Training, Simulation, and Education Conference [I/ITSEC], Orlando, FL, December 2–6, 2019), <https://www.iitsec.org/>.

34. For discussion and citations, see Connable, "How to Assess the Will to Fight," 5–6.

35. For example, see Dale Spurlin and Matthew Green, "Demystifying the Correlation of Forces Calculator," *Infantry*, January–March 2017, 14–17, <https://www.moore.army.mil/>.

36. Trevor N. Dupuy and Gay M. Hammerman, *Soldier Capability—Army Combat Effectiveness (SCACE)*, vol. 3, *Historical Combat Data Analysis* (US Army Soldier

Support Center, December 1980), <https://apps.dtic.mil/>; and Huba Wass de Czege, “Understanding and Developing Combat Power” (US Army Command and General Staff College, 1992). (Brigadier General de Czege originally wrote the monograph as a Command and General Staff College student in 1976. Unpublished manuscript in the collection of the Combined Arms Reference Library, US Army Combined Arms Center, Fort Leavenworth, KS.)

37. See Connable, *Iraqi Army Will to Fight*, chap. 1, 1–14.

38. For a discussion of the gaps in human theory and modeling in acquisitions, see, for example, Connable, chaps. 1 and 3, 1–14, 37–67.

39. This statement is a subjective judgment based on a review of publicly available information on soldier lethality programs and interactions with program leaders between 2018 and 2021.

Chapter 14

The Will to Fight as a Complex System

A Research Agenda for the Employment of Neuroscience in Military Organizations

Aaron B. Frank, RAND Corporation

Abstract

Discoveries in neuroscience have many implications for developing and defeating the will to fight of military organizations and societies more broadly. While military science may be naturally attuned to the possibilities that neuroscience will enable soldiers to be increasingly capable of performing organizational and operational tasks without suffering adverse psychological and emotional effects of combat stress and losses, a focus on the singular soldier's performance may prove to be a detriment to the will to fight rather than an enhancement. In this chapter, I argue that understanding what neuroscience can and cannot do to affect the will to fight depends on a broader understanding of military organizations as a complex system in which the relations between soldiers are as important as the soldiers themselves. Thus, the links between soldiers within units, between soldiers and the larger organization, and between soldiers and society more broadly are critical and immutable dimensions of the will to fight. Such linkages undergird a complex systems perspective on the will to fight, in which the disposition to accept risk, fight, and sacrifice depends on the individual, the many groups they are members of, and the feedback between them. A complex systems perspective on the will to fight creates space for discoveries in neuroscience to contribute to the will to fight, while establishing a framework for setting realistic expectations, measures of effectiveness, and trade-offs between efforts to improve military effectiveness at individual and group levels.

The will to fight is a crucial yet elusive aspect of military effectiveness.¹ Indeed, historical conflicts, such as the Vietnam War, both Russian and American experiences in Afghanistan, current conflicts in Ukraine and Gaza, and possible military conflicts on the Korean peninsula and in Taiwan all demonstrate the importance of the will to fight within profes-

sional militaries, insurgent and terror groups, and society more broadly. The will to fight is a complex, multidimensional concept involving individual soldiers, their leadership, group dynamics, and the relationship between the military and society. Factors such as tactical situations and broader motivations, like nationalism and religion, all play a role.

This chapter examines the will to fight through the lens of complex systems theory to understand how investments in neuroscience research may impact the will to fight in both friendly forces and adversaries. By considering the interdependence of these factors, we can better evaluate approaches to shaping will-to-fight dynamics and maintain a focus on the relationship between the individual and the group and their responses to changing conditions at many different levels of analysis.

Neuroscience advancements offer both opportunities and risks in influencing the will to fight. Three key considerations include: (1) enhancing individual soldiers' risk-taking and performance through neuroscience-based interventions; (2) employing neuroscience to foster trust and social support within military units by affecting the bonds within and between the armed forces and the state; and (3) using neuroscience as a tool to measure the effects of non-neurological interventions on soldiers' will to fight.

Addressing these questions will help prioritize military neuroscience investments while minimizing adverse effects on the military organizations. By focusing on the group rather than the individual soldier, we can better assess the impact of interventions on the will to fight and overall military effectiveness.

The Complexity of Military Organizations and Will to Fight

Since the earliest speculations about a conventional Revolution in Military Affairs (RMA) enabled by increased availability of information and intelligence, and the ability to share and organize military operations around information, military strategists have sought to apply complexity theory to military organizations and operations.² Indeed, the perceived alignment between complex systems and the military transformation of the late 1990s and early 2000s included the development of new analytic approaches specifically focused on (1) attacking the cohesiveness of adversarial military forces as an alternative to

strategies of attrition,³ and (2) the reimagining of the military targeting and effects analysis based on modeling adversaries as Complex Adaptive Systems (CAS).⁴

While a detailed alignment of military organizations and complex systems theory is not needed for the purposes of the argument presented here, it will suffice to highlight the key elements of what a complex systems approach to the analysis of military organizations and operations entails. The central idea is that through coordinated action, less individually capable platforms can combine maneuver and fires to generate the firepower effects of larger, heavier forces. Thus, a military built on an infrastructure of high-speed, high-resolution communications and intelligence can enable smaller, lighter, and increasingly heterogeneous military forces to achieve the same, or greater, military effectiveness as much heavier forces.⁵

With an emphasis on information, dispersion, and collective action, military organizations took on a renewed interest in natural and engineered systems in which the coordinated action of many units combined to produce outcomes that none could achieve on their own. Inspiration was found in a variety of examples from the physics of spin glasses⁶ and dissipative systems, such as storms and earthquakes,⁷ to behavior of insect colonies,⁸ to equilibrium-seeking social processes such as traders in markets⁹ and commuters in traffic.¹⁰ These and other examples renewed attention on the relationships between individual agents and the groups in which they were embedded, challenging the traditional means for analyzing military organizations and operations.¹¹

Returning to questions regarding the will to fight, complexity, and the linkages between individuals and groups, the biological concept of evolutionary transitions becomes particularly useful. Biologists have identified many such transitions where the driver of natural selection (survival and reproduction) shifts from lower levels of organization to higher ones. Specific transitions include shifts “from individual genes to networks of genes, from gene networks to bacteria-like cells, from bacteria-like cells to eukaryotic cells with organelles, from cells to multicellular organisms, and from solitary organism to societies.”¹² Such transitions result from cooperation at lower levels, allowing collectives to increase in complexity, whether as a result of organizational or behavioral specialization—including the emergence of principals with command over specialized agents—that allow the group to become increasingly robust and resilient to environmental and competitive

pressure.¹³ What is less well appreciated, however, is that such cooperation comes at a cost to the individual.

Cooperative interactions are the basis of more inclusive evolutionary units. Because cooperation reduces the fitness of lower-level units, while increasing the fitness of the group, cooperation drives transitions to higher-level units. Defection, the antithesis of cooperation, is the bane of cooperative groups everywhere, because it is often favored within the group by its frequency-dependent advantages.¹⁴

When viewed through the lens of evolutionary transitions, a natural tension arises between efforts to increase the warfighting capabilities of individual soldiers and the capabilities of the larger group. This trade-off may not be evident when one views the single soldier as a system to be optimized, as opposed to a higher-level system of soldiers from which the will to fight specifically and military effectiveness more generally emerge.

Understanding Military Cohesion

From the context of history, how military organizations have developed, sustained, and projected combat power has been an essential—if not the central—driver of world history, particularly in the modern world.¹⁵ Indeed, the threatened and actual use of force by armed groups able to act in a coordinated and purposeful fashion played essential roles in the emergence of the state, markets, and the international system and its varied transformations, starting from the earliest civilizations in prehistory and continuing until today. Thus, there is a broad and deep body of research that focuses on the military and society that emphasizes the role of coercive power in consolidating (or failing to consolidate) political and economic control over territories and markets. However, such questions and answers rest on more micro-level considerations regarding how armed groups formed and organized into effective fighting units that could exert their will over others and resist the efforts of other groups attempting to do the same to them.

William McNeill posited that effective military organizations emerged out of more primal bonding efforts, such as collective dancing, singing, hunting, and foraging.¹⁶ McNeill theorized that collective action, particularly the performance of physical tasks, forged new bonds within

groups, allowed for the development of skills and expertise, and enabled the arming of people who outside of a military context would have little reason to interact, cooperate, trust one another, or believe in a shared purpose.

Cohesion sits at the center of this ability to coordinate military action, and while it is not the only piece of the larger will-to-fight puzzle, cohesion does provide a point of departure that links the collective performance of whole organizations with the efforts and expertise of the individuals within it. Research on military cohesion offers alternative perspectives regarding how collections of individuals develop the ability to become and remain effective fighting units capable of enduring the most difficult and risky of conditions.

For simplicity, we will consider two contrasting theories of military cohesion—task cohesion and social cohesion—that pertain to the primary groups that soldiers are organized into. Importantly, this treatment of cohesion is primarily motivational—it is intended to place the importance and challenges of neuroscience with regard to cohesion into context—and will not elaborate on increasingly rich and complex research on cohesion itself, such as the increasing consideration of trust and trustworthiness, on individual and collective behavior.¹⁷ Furthermore, we will acknowledge yet leave unexamined the existence of other theories of cohesion that consider increasingly nuanced and fine-grained analysis of secondary groups, including relations between military units and the larger organization and between the military organization and society more broadly.¹⁸

Task cohesion and social cohesion provide two competing views as to how military units develop the ability to work as a cohesive whole. These theories differ based on whether they prioritize the development of individual expertise as the bedrock for building trust between the members of military organizations or whether they prioritize the formation of emotional bonds within the group, allowing for members to feel confident they have the emotional support to endure risk and hardship.

The theory of task cohesion argues that military effectiveness flows from the competent performance of collective tasks and that social cohesion is a result of the group's ability to (1) share a collective mental model of the situation, (2) maneuver as a group in ways that are expected and appropriate for the situation, and (3) verbally communicate in highly efficient and compact ways, particularly when engaged in battle with an adversary.¹⁹ Task cohesion is often regarded as the

basis upon which shared commitments to a common cause allow group members to organize and work together. Task cohesion emphasizes the ability of the group to coordinate their individual efforts to work toward a common goal.²⁰

By comparison, the theory of social cohesion argues that interpersonal bonds of social support enable soldiers to take on greater risks and endure the physical and psychological hardships of military training and operations. From the perspective of social cohesion, social bonding between individuals creates a distinct unit of action characterized by individual commitments to an emergent group defined as “with,” where group members emphasize acting together.²¹ Thus, even in fleeting moments, such as walking down the street or sharing a meal, social cohesion is advanced and enables joint action in which individuals take solace in working together.

Research on military cohesion has sought to determine whether (1) task cohesion emerges from social cohesion, where social bonds enable interpersonal trust that allows for increased risk-taking and the acceptance of interdependencies between group members, allowing for tasks of greater complexity to be learned and performed; or (2) bonds of social cohesion emerge as a result of individual expertise and demonstrated competence, allowing for group members to trust one another based on the belief that each knows their role, can act as needed, and is committed to doing so, even under dangerous conditions. Such research has largely proven inconclusive. Data collected via surveys and observational studies of military members and comparative studies of cohesion in industry or laboratory settings offer support to task cohesion as having a greater correlation with combat effectiveness and is thus often referred to as enhancing military effectiveness.²²

However, advocates of social cohesion note that military units differ significantly from groups used in other studies, such as business organizations, sports teams, or students in university laboratories.²³ Additionally, while task cohesion may be observable based on the completion of assigned objectives, social cohesion may only be observed under conditions where individuals and groups are challenged beyond their innate capabilities. As a result, though social cohesion may be more challenging to isolate, observe, and measure, it is nevertheless considered as enabling military effectiveness.²⁴

An Agent-Based View of Will to Fight

Before considering how neuroscience might enhance military cohesion, we will consider a representation of the soldier as a simple decision-making agent. Joshua Epstein's *Agent_Zero* framework offers an accessible, generalized approach for simulating how unintended and undesired collective behaviors may arise from the endogenous interactions within groups, particularly through the contagion of fear.²⁵ While abstract, Epstein's modeling of contagion behavior included collective violence, military atrocities, mass flight, financial panics, and more—all representing situations where individuals' choices are informed by the information and emotion of those around them. The work's motivation was to link neuroscience research on the brain's amygdala circuit, responsible for triggering fear responses within the brain, with irrational and undesired collective behavior.

The *Agent_Zero* framework posits that agents' decisions are composed of three components: (1) an individual's disposition to take specified action based on its innate emotional state; (2) the agent's limited, boundedly rational capabilities to process what information it possessed; and (3) the weighted disposition of other agents (alters) to which the agent (ego) was connected to. The *Agent_Zero* framework takes a cognitively familiar representation of decision-making, one in which agents possess a hot, intuitive, emotional System 1 decision-making process and a cold, analytic, strategic, System 2 decision-making process; it then situates them into social networks, within which the summed disposition of other agents—using their own decision-making processes—further influences their choices.²⁶ Thus, we may consider a representation of the *Agent_Zero* soldier as a decision-maker that commits to risk-taking action based on the combination of three decision-making processes: (D) innate disposition + (R) boundedly rational assessment + (S) weighted influence of social network.

We will use this DRS framework to consider alternative targets for neuroscience research to affect the capabilities and behaviors of soldiers. Indeed, our point of departure for the remainder of this chapter will consider three types of potential neuroscience-based interventions:

- Interventions designed to block the brain from feeling pain and fatigue, allowing soldiers to continue to fight through increased endurance;

- Interventions designed to increase the brain's cognitive capacity and information processing, allowing soldiers to perform increasingly complex military tasks and operate more sophisticated weaponry and support systems;
- Interventions that increase the brain's response to others' emotional affect, increasing empathy and trust between soldiers.

Each of these investments suggests alternative images of future neuroscience technologies and the ways in which military capabilities might be enhanced. Each of these interventions also suggests that advances in one application area may have unintended consequences on others and, therefore, that researchers should proceed carefully when considering how interventions into the soldier as a system may affect the system of soldiers upon which cohesion is built.

Investments in Neuroscience for Military Applications

For the purpose of this chapter, it will be sufficient to examine how the Department of Defense (DOD) has expressed its neuroscience-based research activities and motivations in funding requests for Fiscal Year (FY) 24. Though simplistic, these high-level descriptions of research offer a window into what outcomes DOD research sponsors are seeking to gain from their investments.

Looking across eighteen broad programmatic investments, totaling more than \$160 million requested for FY24, offers a window into how neuroscience is viewed within the DOD. Broadly, investments may be regarded as falling into three research types—mechanism discovery (M), instrumentation (Ins), and interventions (Int). These research programs, selected descriptions,²⁷ and investment type and target are shown in tables 14.1, 14.2, 14.3, and 14.4.

Mechanism discovery is the focus of basic research investments and seeks to discover how neurological processes work within the brain. Specific investments seek to identify and understand neurological circuits within the brain, mapping the brain's structure and functions. Instrumentation investments seek new ways of accessing information on neurological processes and functions, often in ways that can be employed outside of the highly constrained and controlled conditions of laboratory research settings. Finally, interventions seek ways to mitigate, amplify, or otherwise alter neurological processes to affect lower-level (e.g., physiological) processes such as fatigue or

higher-level (e.g., cognitive) processes such as language acquisition and brain functioning.

Returning to the basic DRS—disposition, rationality, social—formulation presented earlier, the overwhelming bulk of DOD neuroscience research funding is committed to investments in the D and R target bins. Indeed, the portfolio across the services is predominantly focused on improving the individual performance of service members, whether through increasing their disposition and resilience to physical and psychological stress, most notably post-traumatic stress disorder (PTSD) and traumatic brain injuries (TBI), or enhancing their rationality by improving cognitive capabilities and performance for information processing and skill acquisition.

These justifications indicate that the DOD's current investments in neuroscience are covering a small space within the broader field of neuroscience and that prospective applications are focused on singular soldiers rather than larger groups. Indeed, the predominant consideration of team activities within the justifications offered are focused on human-machine teaming, which as a field of research does not necessarily examine the behavior of human groups.

The implications of this research gap are evident by returning to the literature on military cohesion and the two dominant theories of task and social cohesion. While neuroscience has the potential to significantly contribute to cohesion research and the empirical testing of theory, more practical and immediate concerns may be found in the broader concerns over the ways in which cohesive and resilient groups form from individuals. If neuroscience research pushes the boundaries of individual soldier capabilities and performance but does so in a way in which the bonds of trust become increasingly difficult to form and maintain, the result may reverse the gains achieved by effective and coordinated collective effort (i.e., reversing the benefits of evolutionary transitions that push selection pressure off individuals onto the broader team). Such an unraveling may occur if the bases of task or social cohesion are undermined.

Task cohesion may be undermined if the enhancements of soldiers' individual capabilities are uneven, increasing intragroup variance, resulting in a loss of confidence within the group that others are competent at performing necessary tasks. While a first-order analysis would assume that gains in individual performance would correlate with increased task cohesion, such a conclusion is likely unjustified after admitting for a more nuanced understanding of cohesion. Specifically,

an increase in the average capability of soldiers that preserves existing intragroup variation will likely have the desired effects on task cohesion, instilling greater confidence within the group that others will be reliable members of the unit. However, even if, on average, soldiers increase their individual capabilities, if these gains also produce greater variance within the group, there may be decreased confidence that all members can perform their tasks well enough to be trusted, especially if soldiers compare their competencies subjectively.

The undermining of social cohesion may occur if the enhancements of soldiers' individual capabilities disrupt the balance between disposition, rationality, and social influence (i.e., the D, R, and S categories discussed earlier). Decreased social cohesion may result from investments in soldiers' development that are increasingly biased toward individualism and rationality at the expense of developing strong emotional commitments to the group and its members or complicate in-group status hierarchies affecting the acceptability of giving or receiving social support. Indeed, it is possible that highly rational and cognitively enhanced soldiers, with enhanced disposition and rationality, are initially more effective than groups that have not been given the same treatments. However, when stressed, they may lack the social support systems, group affinity, and affective behavior to be resilient to combat stresses and may even display an increased disposition to challenge authority within the group.

Table 14.1. DARPA neuroscience research justifications in FY24 budget request to Congress

<i>Justifying Organization</i>	<i>Project</i>	<i>Description</i>	<i>Investment Type</i> <i>M, Ins, Int</i>	<i>Investment Target</i> <i>D, R, S</i>
DARPA	Neural Signal Interfaces and Applications (NSIA)	The NSIA program is developing noninvasive neurotechnologies that are able to interface with the nervous system with high resolution and precision without surgery. NSIA uses recent advances to transduce neural signals through tissue. Resulting technologies will restore function in wounded warriors.	Ins	R
DARPA	Neurological Assessment and Protection from Brain Injury	The Neurological Assessment and Protection from Brain Injury program will transform our current detection and protection strategies against traumatic brain injury (TBI), such as injury from blast exposure. This program will develop multisensory fieldable TBI assessment tools and prophylactic countermeasures to prevent severe brain injury.	Ins, Int	D
DARPA	Restoring Cognitive Capability	The Restoring Cognitive Capability program is developing novel drugs to provide rapid therapy for neuropsychiatric disorders experienced by warfighters and veterans. Active-duty military personnel face increased risk of acute and chronic neuropsychiatric dysfunction, limiting day-to-day function and return to duty. Current therapeutic approaches for many neuropsychiatric disorders (e.g., post-traumatic stress disorder [PTSD], mood disorders, and substance abuse) rely on individual management with integrated psychiatric therapy and medication. However, most interventions approved for use in these conditions lack long-term efficacy, involve a logistical burden of treatment, and/or carry a risk of serious adverse side effects. Novel drugs developed under this program will be designed to functionally interact with neuronal receptor subtypes known to play a role in these neuropsychiatric conditions, with the aim of enabling fast-acting and effective alleviation of neuropsychiatric dysfunction with single or minimal doses. Additional studies in this area seek to develop a mechanistic understanding of brain injury (UBI) resulting from blast, ultrasound, electromagnetic waves, or other directed-energy sources.	Int	D

Table 14.1 (continued)

Justifying Organization	Project	Description	Investment Type <i>M, Ins, Int</i>	Investment Target <i>D, R, S</i>
DARPA	Strengthening Resilient Emotions and Nimble Cognition Through Engineering Neuroplasticity (STRENGTHEN)	The STRENGTHEN program aims to overcome the limitations of focusing on descriptions of individual disease effects and suicide risk factors by adopting a transdiagnostic approach that addresses the mechanisms (i.e., predictors or causes) of mental health and wellbeing. STRENGTHEN will optimize the brain networks essential for cognitive flexibility and emotional regulation, establishing dose response, time-to-onset, and duration-of-effect curves to quantify the impact of change in cognitive flexibility and emotional regulation on validated measures of suicidality, behavioral health, and wellbeing within DOD.	M, Ins	D, C
DARPA	Physiological Overmatch	Warfighters operate under extreme physiological conditions, sometimes with limited resources and manpower, and must acclimate quickly to changing operational needs. The Physiological Overmatch program is investigating innovative approaches to allow the warfighter to adapt rapidly to operational challenges during deployment by developing novel detection and treatment systems. The program will initiate work in aiding the deployed soldier's ability to defend against biological pathogens, resist fatigue, combat sleep deprivation, receive adequate nutrition and hydration, and maintain a high capacity for teaming and operational synchronization. This program will seek to understand the biological mechanisms of fatigue and how teaming could enable improvements to warfighter health and operational performance. This approach represents a significant enhancement to warfighter performance by providing protection and resilience from variables that impact operational readiness.	-	-

Source: Department of Defense Fiscal Year (FY) 2024 Budget Estimates, Research, Development, Test & Evaluation for DARPA. Department of Defense, Defense Advanced Research Projects Agency, Defense-Wide Justification Book Volume 1 of 5, Research, Development, Test & Evaluation, Defense-Wide (Department of Defense, March 2023), <https://comptroller.defense.gov/>.
 *While not mentioned in the budget justification, DARPA's OPTEMPO program offers an important investment in biological sensing that may include, but is not explicitly seeking neurological measures that predict the performance of military groups. Such a program offers an important, if perhaps rare, example of explicit attention to group behavior within the advanced research community. See DARPA, "Objective Prediction of Team Effectiveness via Models of Performance Outcomes (OPTEMPO)" (DARPA, November 2, 2023), <https://sam.gov/>.

Table 14.2. US Air Force neuroscience research justifications in FY24 budget request to Congress

<i>Justifying Organization</i>	<i>Project</i>	<i>Description</i>	<i>Investment Type</i> M, Ins, Int	<i>Investment Target</i> D, R, S
Air Force	Cognitive and Physiological Performance	Develop technologies in cognitive neuroscience and physical performance to sustain, augment, and recover operator performance and determine performance attributes/metrics for optimal career field alignment. Includes research focused on developing and validating physiological and behavioral assessments of current and predicted cognitive state combined with personalized cognitive performance enhancement techniques and technologies to augment operator performance.	M, Int	D, R
Air Force	Multisensory Perceptions and Communication	Multisensory Perception and Communication focuses on identifying and exploiting the underlying sensory and cognitive mechanisms mediating human perception and communication in order to inform the development of multimodal interfaces and speech/language technologies. Research examines sensory processing, multisensory integration, and human communication processes in simple and complex environments to identify the barriers to effective information transmission and inform the development of technologies to overcome, or exploit, those barriers in order to enhance Airmen performance	M, Ins, Int	R

Source: Department of Defense Fiscal Year (FY) 2024 Budget Estimates, Research, Development, Test & Evaluation for the Air Force. Air Force Justification Book Volume 1 of 4, Research, Development, Test & Evaluation, Air Force (Department of Defense, 2023), <https://www.saffm.hq.af.mil/>.

Table 14.3. US Army neuroscience research justifications in FY24 budget request to Congress

<i>Justifying Organization</i>	<i>Project</i>	<i>Description</i>	<i>Investment Type</i> <i>M, Ins, Int</i>	<i>Investment Target</i> <i>D, R, S</i>
Army	Basic Research in Life Sciences	This effort fosters fundamental discoveries in life sciences with the ultimate goal of facilitating the development of novel biomaterials to greatly enhance Soldier protection and performance. More specifically, (1) molecular genetics research that pursues fundamental studies in molecular and systems biology, and genetics; (2) neurosciences research to investigate the physiology underlying perception, neuro-motor output, and potential methods of monitoring cognitive states during activity; (3) biochemistry research focused on studies in structural and cell biology, metabolic processes, and biophysics; (4) research in microbiology that pursues studies in microbial physiology, ecology, and evolution; (5) social science research that aims to elucidate the social, cultural, and other influences to human actions; and (6) auditory and signal processing research that maps the cognitive implications of multisensory information integration.	M, Ins	D, R
Army	Translational Neuroscience	This effort integrates neuroscience with traditional approaches to understanding Soldier behavior to enable system designs that maximize Soldier performance. Will combine multiple models of abstract representation into a single unified map to simulate spatial reasoning; create neural network with features that mirror the mammalian spatial reasoning system to improve network performance in a spatial reasoning task; investigate the inter-brain system interactions underlying human-technology systems solving complex problems with creative solutions.	M, Ins	D, R, S

Table 14.3 (continued)

Army	Hybridization of Team Thinking	This effort merges novel advances in human-system sciences with neuroscience and training sciences to reconceive human brain processes and optimize human-machine thinking to allow humans to influence technology-enabled decisions previously believed to be outside of human capabilities. The effort aims to optimize how humans could think within complex human-technology ecosystems to maximize human potential to adapt the Army on the battlefield.	M, Ins, Int	D, R
Army	Physiological Health	This effort conducts fundamental research on the physiological mechanisms of sleep, fatigue, and nutrition on Soldier health, readiness, and performance. In addition, this effort discovers basic understanding of physiological and genetic processes leading to biomedical performance enhancement in the physical, cognitive, and psychological domains.	M, Ins	D
Army	Psychological [sic] Health and Resilience	This effort conducts research into the basic mechanisms of the ability to overcome traumatic events including determination of underlying neurobiological mechanisms (nervous system control of cellular and molecular processes) related to acute stress reactions, early characteristics of post-traumatic stress disorder (PTSD), depression, and other neuropsychiatric sequelae of trauma/stress.	M	D
Army	TBI Neurotrauma/ Brain Dysfunction	This effort conducts basic research in poly-trauma (multiple injuries)/traumatic brain injury (TBI) model, mechanisms of cell death, and the discovery of novel drugs and medical procedures to mitigate the effects of TBI.	M, Int	D

Table 14.3 (continued)

Justifying Organization	Project	Description	Investment Type <i>M, Ins, Int</i>	Investment Target <i>D, R, S</i>
Army	Neurosciences CRA	Conduct fundamental neuroscientific studies aimed at understanding the basic mechanisms that support situational awareness, including cognitive priority control, and how those mechanisms are impacted by changes in physical and cognitive workloads; characterize human neural systems that integrate motor skill learning, route planning, and choice behavior during adaptive planning in complex physical scenarios; uncover the cognitive and neural mechanisms underlying individual decision-making conducted under uncertainty; develop models of visual information processing and neural systems under covert and overt attention. If successful, these basic research studies will support Army efforts to augment Soldier performance, increase situational awareness, lighten cognitive workloads, and integrate humans with autonomous systems employing artificial intelligence.	M	D, R

Source: Department of Defense Fiscal Year (FY) 2024 Budget Estimates, Research, Development, Test & Evaluation for the Army, Army Justification Book Volume 1a of 1, Research, Development, Test & Evaluation, Army RDT&E – Volume I, Budget Activity 1 (Department of Defense, March 2023), <https://www.asafm.army.mil/>.

Table 14.4. US Navy neuroscience research justifications in FY24 budget request to Congress

<i>Justifying Organization</i>	<i>Project</i>	<i>Description</i>	<i>Investment Type</i> M, Ins, Int	<i>Investment Target</i> D, R, S
Navy	Human Systems	<p>Sailors and Marines operate across multiple domains: under, on and above the seas. This activity focuses on understanding the human aspects of Naval operations with the objective of planning and execution for mission success. The long-term goal of this research is to increase total system performance by maximizing the effectiveness of human-machine systems to ensure mission effectiveness.</p> <p>Schoolhouse Training</p> <ul style="list-style-type: none"> • Initiate researching neuro-psychometric tests that can reliably predict complex skill learning (e.g., second language & computer programming). • Initiate research to discover neuroimaging analytical techniques to assess learning from written passages. • Initiate work to create new training techniques for spatial ability which facilitates learning STEM skills. <p>Computational Neuroscience</p> <ul style="list-style-type: none"> • Continue research to identify and understand neural circuits and pathways that will be used to develop models of sensorimotor control and spatial navigation. The long-term goal is to understand the neural foundation of intrinsic cognitive skills, such as attention, memory formation, perception, and problem solving to develop novel intelligent systems. • Complete research on neural basis of spatial navigation. • Initiate efforts to explore the neural basis of the control of reaching, grasping, and manipulation to inform robotics. 	M, Int	D, R, S

Table 14.4 (continued)

<i>Justifying Organization</i>	<i>Project</i>	<i>Description</i>	<i>Investment Type</i> M, Ins, Int	<i>Investment Target</i> D, R, S
Navy	Human Systems	<p>Schoolhouse Training</p> <ul style="list-style-type: none"> • Continue research in systematically studying complex skill learning (e.g., second language, computer programming, machine troubleshooting) to understand neurological and cognitive predictors of gaining these skills. • Continue research investigations of neuroimaging analytical techniques to assess learning from written passages. • Continue research efforts regarding training techniques for spatial ability which facilitates learning STEM skills. <p>Computational Neuroscience</p> <ul style="list-style-type: none"> • Continue research to identify and understand neural circuits and pathways that will be used to develop models of sensorimotor control. The long-term goal is to understand the neural foundation of intrinsic cognitive skills, such as attention, memory formation, perception, and problem solving in order to develop novel intelligent systems. • Continue exploring the neural basis of the control of reaching, grasping and manipulation to inform robotics. • Initiate research exploring the combination of robot mobility with dexterous manipulation in assisting humans on naval-relevant tasks, such as shipboard maintenance and building clearing of hazards. • Attention in Sensory Processing and Intelligent Sensing • Initiate research efforts to systematically study the neurocognitive processes of attention and its control. 	M, Int	D, R, S

Table 14.4 (continued)

<p>Navy</p>	<p>Medical and Biological Sciences</p>	<p>The health and performance of Sailors and Marines is a top priority. Extensive research in the medical and biological sciences discovers and leverages breakthroughs to improve naval warfighter performance, so they can fight, win, and come home safe.</p> <p>Research areas include bio-inspired autonomous systems; bioengineering; biophysics; microbial synthetic biology; microelectronics; microbial electrophysiology; microbiome research; bio-inspired multispectral camouflage and sensing; sensory neuroscience and physiology; naval force health protection; undersea medicine; stress responses; health monitoring and modeling research; and health and welfare of the Navy's marine mammals.</p> <p>Stress Response</p> <ul style="list-style-type: none"> • Continue to investigate the clinical, neurobiological, and genetic factors that predict differences in stress reactivity for constructing a multimodal predictor of stress responsiveness and for identifying targets for intervention. • Continue to examine the interaction of a chronically stressful environment and changes in light/dark periods on the function of the stress response system. • Continue to explore the feasibility of continuous and unobtrusive stress detection, tracking, and mitigation for a wearable closed-loop system capable of monitoring stress and providing bioelectronic therapy 	<p>M, Ins, Int</p>	<p>D</p>
-------------	--	---	--------------------	----------

Table 14.4 (continued)

Justifying Organization	Project	Description	Investment Type <i>M, Ins, Int</i>	Investment Target <i>D, K, S</i>
Navy	Physics Based Neutralization of Threats to Human Tissues and Organs	Conduct research into a multiscale, physics-based approach to for use in preventing and mitigating both mild traumatic brain injuries (mTBI) and blast-induced traumatic brain injuries (bTBI). Preventing and mitigating bTBI and mTBI requires advancing the understanding of injury at a cellular level, as the exact force magnitudes and directions that initiate TBI at the cellular scale are still unknown. Knowledge of neuronal TBI thresholds is a critical and currently missing component of developing improved protective equipment, as well as equipment that addresses the full range of injury.	M	D

Source: Department of Defense Fiscal Year (FY) 2024 Budget Estimates, Research, Development, Test & Evaluation for the Navy, Navy Justification Book, Volume 1 of 5, Research, Development, Test & Evaluation, Navy (Department of Defense, March 2023), <https://www.secnav.navy.mil/...>

Social Neuroscience and Military Cohesion

In 2009, the National Academy of Sciences (NAS) issued a report that identified opportunities for applying neuroscience to the needs of the US Army.²⁸ While issued over a decade ago, the NAS report remains a relevant and insightful guide for how scientists, including many of the world's most prominent neuroscientists, imagined the interface between a rapidly developing field of science and the needs of military organizations. The report's recommendations (presented in table 14.5) identified four broad application areas that included (1) training and learning, (2) optimizing decision-making, (3) sustaining Soldier performance, and (4) improving cognitive and behavioral performance—categories that directly cover the motivations found in existing research.

Table 14.5. Recommended neuroscience applications

<i>Application Areas</i>	<i>Sample Objectives</i>
Training and learning	
Training paradigms and methods	Shorten training cycles, assess training effectiveness
Performance assessments of individuals and groups	Detect individual performance degradation; assess group-individual interactions
Identification of training candidates	Improve success rates
Training effectiveness measures	Predict optimal performance; anticipate degraded performance
Optimizing decision-making	
Individual and unit readiness	Utilize neural-state indicators
Adversary assessment and prediction	Act inside adversary decision cycle; disrupt adversary decision-making (psychological operations)
Setting objectives	Reduce risk by matching goals with performance
Sustaining Soldier performance	
Recovery and rest	Mitigate effect of sleep deprivation on recovery; neuropharmacological intervention to mitigate trauma response
Counterstress	Insulate immune system; moderate disease; modify brain functions to contend with combat rigors
Fatigue and pain	Nutritional countermeasures; minimize effects of sleep deprivation; drug therapies
Brain injury	Intervene early to mitigate acute and long-term deficits due to trauma

Table 14.5 (*continued*)

<i>Application Areas</i>	<i>Sample Objectives</i>
Improving cognitive and behavioral performance	
Soldier skills	Optimize brain-machine interfaces; improve image interpretation capabilities
Information utilization and management	Personalize data fusion; prevent information overload

Source: National Academy of Sciences, *Opportunities in Neuroscience for Future Army Applications* (National Academies Press, 2009), 19.

However, the report identified social neuroscience as an explicit line of research that is mostly absent from the DOD's existing research justifications. The report specifically noted that "most of a soldier's actions involve other people, including fellow soldiers, commanders who are giving orders, the enemy, and noncombatants,"²⁹ and made three observations that highlighted creative and limited applications of neuroscience research and technologies to the social circumstances of Soldiers and military organizations.

First, the report noted that many of the experimental and measurement techniques used in neuroscience research are focused on measuring individual responses to stimuli within laboratory environments.³⁰ While the report noted that creative experimental designs for studying interpersonal influence were developing, the techniques for observing neurological processes of individuals performing stressful activities in the field were not yet available to support needed research and were unlikely to develop without Army investment, for example, vertical-bore fMRI, full-motion, interactive stimulation; wide-angle, immersive visual stimulation; and high-temporal-precision stimulation and monitoring.³¹

Second, given instrumentation limits, measured applications of neuroscience research on social relations remained individualistic. For example, experiments on interpersonal influence measured the neurological activity and responses of one individual interacting with others in a group setting, while other research measured brain activity associated with theory of mind, that is, imagining how others may be thinking—all within a single subject—as a way of examining the sophistication of their thinking about others.³²

Third, the report suggested that as Soldiers worked in increasingly distributed teams that relied on sophisticated information processing and communications systems, the ways in which individuals trusted, valued, and processed information provided by machines versus other humans was becoming an increasingly important area of research.³³

Prospective applications of neuroscience included offering the instrumentation for measuring changes in individual trust and attention related to different sources of information, allowing for the development and testing of hypotheses related to human-machine teaming and the design of effective groups.

Social neuroscience has since broadened its many lines of inquiry—often referred to as social, cognitive, and affective neuroscience (SCAN)—to examine consistencies and variation regarding how individuals and groups related to one another at the neurological level. For example, one line of research has examined social hierarchies and the neurological basis by which status and individual rank are represented, challenged, and recoded.³⁴ Another line of research has examined the interplay between behavioral activities and the development of group cohesion, effectiveness, and prosocial behavior within the group, as evident with the synchronization of neurological processes across group members.³⁵ A particularly important line of research regarding the will to fight concerns commitments to group identities, to threat perception, and to risk-taking.³⁶

Broadly speaking, there is increasing recognition that human neurological architectures and cognitive processes are not adequately understood in the context of the rational, singular actor but have evolved to participate in coalitional decision-making in which group membership, status, and survival play essential roles in threat perception and risk-taking.³⁷ Indeed, Michael Thomas and Simon Green noted:

The normal mode of operation of the brain is not logical and deductive. It doesn't like to abstract; it likes to be based in the concrete, the sensorimotor; it is influenced by what's familiar and what's likely to happen; its ideas are painted in shades of grey, not black and white categories and rules, shades influenced by context, settings, and goals; it is a social and emotional device that is prone to give in to peer pressure (what most people believe) and to place trust in authority figures; it is influenced by anticipated rewards and losses; it gets tired and it gets irritable.³⁸

When viewed from this perspective, many of the existing investments in neuroscience may be working against the brain's innate tendencies to situate the individual in a social, hierarchical context, all to support the largest scale and most complex collective action performed by human groups—the organization, mobilization, and conduct of war.³⁹ While there are strong justifications for investing in

research that has the potential to make soldiers more physically, emotionally, and cognitively capable, research sponsors should consider whether such efforts may place the social foundations of the will to fight at risk by threatening group cohesion. Likewise, research sponsors should consider whether alternative research designs may exist that build on the natural tendencies for individuals to make commitments to and take risks in support of their group identities.⁴⁰

Finally, DOD sponsors of neuroscience research should establish criteria regarding the replication and reproducibility of basic neuroscience research findings before making investments in applications that may disrupt cohesion and the will to fight. This criterion would serve two purposes. First, it would insulate DOD-sponsored research from attempting to develop applications without a robust foundation of research at basic levels.⁴¹ Such a requirement should not diminish the need for neuroscience investments, but rather expand it, creating a greater need to test whether promising findings hold across increasingly large and diverse populations and across alternative means of measurement. Second, the specific emphasis on the social consequences of applied neuroscience would encourage an additional research path for programs that seek to enhance individual performance, consistently probing to see whether enhancements have group effects that may enhance or diminish the effectiveness of the group as a whole.

Conclusion

Having raised the issue of the will to fight and cohesion as a problem posed by complexity (i.e., the dynamic interplay between individual soldiers, their immediate groups, and broader society) we can see the need for a broad, group-level context for evaluating military investments in neuroscience. We conclude this chapter by posing a non-exhaustive list of four questions regarding what future military neuroscience research may discover.

Will increasing the cognitive or physical capabilities of individual soldiers reduce or increase the complexity of military organizations?

Increasingly capable soldiers may result in high levels of task cohesion by reducing the complexity and interdependence within military organizations. More specifically, it is possible that as soldiers become more capable, they will be able to operate with greater degrees of independence and therefore reduce the costs associated with coordinated

action, resulting in less complex operations. Alternatively, increasingly capable soldiers may result in even greater and exquisite specialization, demanding higher coordination costs and task cohesion.

Will neurological interventions that reduce fear and the likelihood of combat effects have positive or negative effects on military effectiveness?

Reducing fear may limit the extent to which soldiers experience combat effects resulting from mortal danger, resulting in increased effectiveness. An argument can be made that if soldiers can be more effective, battles may be more conclusive, wars may be decided sooner, and, as a result, conflicts will result in less harm to civilians and long-term damage to society.⁴² However, the fear that one has to fight to survive, as both individuals and groups, has been a long-standing feature of the will to fight.⁴³

Will neuroscience interventions targeting physical performance be more or less effective than those targeting interpersonal communication in increasing the will to fight?

Given the many potential strategies for employing neuroscience within military organizations, it is unclear which interventions will have the largest, most predictable, and longest lasting effects. While interventions designed to enhance the physical and cognitive capabilities of individual soldiers may deliver expected results, a broad portfolio inclusive of SCAN research mechanisms and interventions is also needed to better understand whether alternative investments might produce better, more effective outcomes.

Will neuroscience provide direct interventions into brain processes of direct military significance or provide the instrumentation for measuring the effectiveness of non-neurological interventions?

Many of the military's justifications for investing in neuroscience rest on the argument that interventions in brain processes, whether by physical, electromagnetic, or pharmaceutical means, may have predictable and positive effects on soldiers and military organizations. While such results may occur, research sponsors should be prepared to consider that investments in neuroscience may only be capable of providing the instrumentation that allows for measuring neurological processes and detecting changes that may result from other, non-neurological interventions. While such a result may prove disappointing, the possibility of high-quality, reliable measurements regarding the consequences of training, education, combat, recovery, and other experiences that shape the lives of soldiers and military organizations may nevertheless prove to offer significant benefits to national security.

Acknowledgments

Although the views expressed in this chapter are the author's alone, they could not have been developed without the stimulating conversations and encouragement of my colleagues. I'd like to thank Elisa Bienenstock, Ben Connable, and Adam Russell for their assistance in the development of the ideas discussed in this chapter. Equally important are Nicholas Wright and Michael Miklaucic for providing the opportunity to participate in the Mind-Tech Nexus research program.

Notes

1. Jasen J. Castillo, *Endurance and War: The National Sources of Military Cohesion* (Stanford Security Studies, 2014); and Ben Connable et al., *Will to Fight: Analyzing, Modeling, and Simulating the Will to Fight of Military Units* (RAND Corporation, 2018), <https://www.rand.org/>.

2. Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute* 124 (1998): 28–35, <https://www.usni.org/>; David S. Alberts et al., *Network Centric Warfare: Developing and Leveraging Information Superiority* (Department of Defense, 2000), <https://apps.dtic.mil/>; and David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare* (Aerospace Education Foundation, 2001), <https://secure.afa.org/>.

3. Mark Herman, "Entropy-Based Warfare: Modeling the Revolution in Military Affairs," *Joint Force Quarterly*, no. 20 (Autumn/Winter, 1998–99): 85–90.

4. "Transforming Military Operational Capabilities," Transformation Study Report, Executive Summary, Prepared for the Secretary of Defense, April 27, 2001, <https://apps.dtic.mil/>.

5. Cebrowski and Gartska, "Network-Centric Warfare."

6. Daniel L. Stein and Charles M. Newman, *Spin Glasses and Complexity* (Princeton University Press, 2013).

7. Per Bak, *How Nature Works* (Copernicus, 1996).

8. Eric Bonabeau et al., *Swarm Intelligence: From Natural to Artificial Systems* (Oxford University Press, 1999).

9. Robert Axtell, "Why Agents? On the Varied Motivations for Agent Computing in the Social Sciences," Brookings Institution Working Papers, November 2000, <https://www.brookings.edu/>; J. Dooyne Farmer et al., "The Predictive Power of Zero Intelligence in Financial Markets," *Proceedings of the National Academy of Sciences of the United States of America* 102, no. 6 (February 1, 2005): 2254–59; and Robert L. Axtell and J. Dooyne Farmer, "Agent-Based Modeling in Economics and Finance: Past, Present, and Future," *American Economic Review* (forthcoming), 75.

10. Neil Johnson, *Simply Complexity: A Clear Guide to Complexity Theory*, reprint ed. (Oneworld Publications, 2009).

11. Stephen Peter Rosen, "Net Assessment as an Analytical Concept," in *On Not Confusing Ourselves: Essays on National Security Strategy in Honor of Albert and Roberta Wohlstetter*, ed. Andrew W. Marshall et al., (Westview Press, 1991), 283–301; Desmond Saunders-Newton and Aaron B. Frank, "Effects-Based Operations: Building the Analytic Tools," *Defense Horizons* 19 (National Defense University, October 2002), <http://ndupress.ndu.edu/>; Andrew Ilachinski, *Artificial War: Multiagent-Based Simulation of Combat* (World Scientific, 2004); and Connable et al., "Will to Fight."

12. Richard E. Michod, *Darwinian Dynamics* (Princeton University Press, 2000), 7.
13. John Tyler Bonner, *The Evolution of Complexity by Means of Natural Selection* (Princeton University Press, 1988); John Tyler Bonner, *Why Size Matters: From Bacteria to Blue Whales* (Princeton University Press, 2006); and Geoffrey West, *Scale: The Universal Laws of Growth, Innovation, Sustainability, and the Pace of Life, in Organisms, Cities, Economies, and Companies*, Kindle ed. (Penguin Press, 2017).
14. Frequency-dependent advantages can be summarized as the observation that when cooperative behavior within a population is increasingly frequent, individuals who do not cooperate are increasingly benefited by taking advantage of those who do. Michod, *Darwinian Dynamics*, 3.
15. Robert L. Carneiro, "A Theory of the Origin of the State," *Science* 169, no. 3947 (August 21, 1970): 733–38, <https://doi.org/10.1126/science.169.3947.733>; William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000* (University of Chicago Press, 1982); Caro M. Cipolla, *Guns, Sails, and Empires: Technological Innovation and the Early Phases of European Expansion, 1400–1700* (Sunflower University Press, 1985); Charles Tilly, "War Making and State Making as Organized Crime," in *Bringing the State Back In*, ed. Peter B. Evans et al. (Cambridge University Press, 1985), 169–91; Charles Tilly, *Coercion, Capital and European States, A.D. 990–1992*, rev. ed. (Wiley-Blackwell, 1992); Clifford J. Rogers, ed., *The Military Revolution Debate: Readings on the Military Transformation of Europe* (Westview Press, 1995); Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500–1800* (Cambridge University Press, 1996); Archer Jones, *The Art of War in the Western World* (University of Illinois Press, 2001); MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution: 1300–2050* (Cambridge University Press, 2001); Victoria Tin-bor Hui, *War and State Formation in Ancient China and Early Modern Europe* (Cambridge University Press, 2005); Christon I. Archer et al., *World History of Warfare* (University of Nebraska Press, 2008); Michael Howard, *War in European History*, updated ed. (Oxford University Press, 2009); Philip Bobbitt, *The Shield of Achilles: War, Peace, and the Course of History* (Anchor Books, 2011); and Brian Downing, *The Military Revolution and Political Change: Origins of Democracy and Autocracy in Early Modern Europe* (Princeton University Press, 2020).
16. William Hardy McNeill, *Keeping Together in Time* (Harvard University Press, 2009).
17. Jason A. Colquitt et al., "Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships with Risk Taking and Job Performance," *Journal of Applied Psychology* 92, no. 4 (2007): 909–27, <https://doi.org/10.1037/0021-9010.92.4.909>.
18. Mikael Salo and Risto Sinkko, eds., *The Science of Unit Cohesion: Its Characteristics and Impacts* (National Defence University, Military Sociological Society of Finland, 2012), <https://www.doria.fi/>; Castillo, *Endurance and War*; and Michael J. McNerney et al., *National Will to Fight: Why Some States Keep Fighting and Others Don't* (RAND Corporation, 2018), <https://www.rand.org/pubs/>.
19. Anthony King, "The Word of Command: Communication and Cohesion in the Military," *Armed Forces & Society* 32, no. 4 (July 2006): 493–512.
20. Robert J. MacCoun and William M. Hix, "Unit Cohesion and Military Performance," in *Sexual Orientation and U.S. Military Personnel Policy: An Update of RAND's 1993 Study*, National Defense Research Institute (RAND Corporation, November 18, 2010), 139, <https://www.rand.org/>.
21. Guy L. Siebold, "The Science of Military Cohesion," in *Science of Unit Cohesion*, 47.

22. Robert J. MacCoun et al., “Does Social Cohesion Determine Motivation in Combat?: An Old Question with an Old Answer,” *Armed Forces & Society* 32, no. 4 (July 1, 2006): 646–54, <https://doi.org/10.1177/0095327X05279181>; Robert J. MacCoun and William M. Hix, “Unit Cohesion and Military Performance,” in *Sexual Orientation and U.S. Military Personnel Policy*, 137–65; and James Griffith, “Cohesion Forgotten? Redux 2011: Knowns and Unknowns,” in *Science of Unit Cohesion*, 11–33.
23. Siebold, “The Science of Military Cohesion.”
24. Mikael Salo and Risto Sinkko, “Introduction,” in *Science of Unit Cohesion*, 9.
25. Joshua M. Epstein, *Agent_Zero: Toward Neurocognitive Foundations for Generative Social Science* (Princeton University Press, 2013); and Joshua M. Epstein, “Agent_Zero and Generative Social Science” (Social and Behavioral Sciences Summit, Washington, DC, October 4, 2016), <https://sites.nationalacademies.org/>.
26. Ziva Kunda, “The Case for Motivated Reasoning,” *Psychological Bulletin* 108, no. 3 (1990): 480–98, <https://doi.org/10.1037/0033-2909.108.3.480>; Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2013); and Noah E. Friedkin and Eugene C. Johnsen, *Social Influence Network Theory: A Sociological Examination Of Small Group Dynamics* (Cambridge University Press, 2014).
27. For brevity, project and program descriptions are abbreviated to focus on those aspects that directly mention neuroscience. For many programs this abbreviation simply summarizes programmatic research goals. However, for larger service-level lines of research, the focus on neuroscience activities leaves out large swaths of other research methods and objectives. In such cases, readers should not assume that neuroscience is the main or even a significant component of the service’s larger research activities.
28. National Academy of Sciences, *Opportunities in Neuroscience for Future Army Applications* (National Academies Press, 2009), <https://doi.org/10.17226/12500>.
29. National Academy of Sciences, 31.
30. National Academy of Sciences, 31–32.
31. National Academy of Sciences, 83.
32. National Academy of Sciences, 31–33.
33. National Academy of Sciences, 33.
34. Jessica Koski et al., “Understanding Social Hierarchies: The Neural and Psychological Foundations of Status Perception,” *Social Neuroscience* 10, no. 5 (2015): 527–50, <https://doi.org/10.1080/17470919.2015.1013223>; Noriya Watanabe and Miyuki Yamamoto, “Neural Mechanisms of Social Dominance,” *Frontiers in Neuroscience* 9 (2015), <https://www.frontiersin.org/>; Won Lee et al., “Effect of Relative Social Rank within a Social Hierarchy on Neural Activation in Response to Familiar or Unfamiliar Social Signals,” *Scientific Reports* 11, no. 1 (February 3, 2021): 2864, <https://doi.org/10.1038/s41598-021-82255-8>; Seongmin A. Park et al., “Inferences on a Multidimensional Social Hierarchy Use a Grid-like Code,” *Nature Neuroscience* 24, no. 9 (September 2021): 1292–1301, <https://doi.org/10.1038/s41593-021-00916-3>; Madeleine F. Dwartz et al., “Neural Systems That Facilitate the Representation of Social Rank,” *Philosophical Transactions of the Royal Society B: Biological Sciences* 377, no. 1845 (January 10, 2022): 20200444, <https://doi.org/10.1098/rstb.2020.0444>; and Emanuel Ferreira-Fernandes and João Peça, “The Neural Circuit Architecture of Social Hierarchy in Rodents and Primates,” *Frontiers in Cellular Neuroscience* 16 (2022), <https://www.frontiersin.org/>.
35. Idil Kokal et al., “Synchronized Drumming Enhances Activity in the Caudate and Facilitates Prosocial Commitment—If the Rhythm Comes Easily,” *PLoS One* 6, no. 11 (2011): e27272, <https://doi.org/10.1371/journal.pone.0027272>; Ilanit Gordon et al., “Physiological and Behavioral Synchrony Predict Group Cohesion and Performance,” *Scientific Reports* 10 (May 21, 2020): 8484, <https://doi.org/10.1038/s41598-020-65670-1>; and Alon Tomashin et al., “Interpersonal Physiological Synchrony

Predicts Group Cohesion,” *Frontiers in Human Neuroscience* 16 (2022), <https://www.frontiersin.org/>.

36. James K. Rilling and Alan G. Sanfey, “The Neuroscience of Social Decision-Making,” *Annual Review of Psychology* 62, no. 1 (2011): 23–48, <https://doi.org/10.1146/annurev.psych.121208.131647>; and Darren Schreiber, “Neuropolitics: Twenty Years Later,” *Politics and the Life Sciences* 36, no. 2 (ed 2017): 114–31, <https://doi.org/10.1017/pls.2017.25>.

37. Rilling and Sanfey, “Neuroscience of Social Decision-Making”; and Schreiber, “Neuropolitics.”

38. Michael S. C. Thomas and Simon Green, *How the Brain Works: What Psychology Students Need to Know*, 1st ed. (SAGE Publications Ltd, 2023), 223.

39. McNeill, *Pursuit of Power*; and Peter Turchin, “Warfare and the Evolution of Social Complexity: A Multilevel-Selection Approach,” *Structure and Dynamics* 4, no. 3 (November 7, 2010), <https://doi.org/10.5070/SD943003313>.

40. William Swann Jr., *Resilient Identities: Self, Relationships, and the Construction of Social Reality* (Basic Books, 1999); Scott Atran et al., “Sacred Barriers to Conflict Resolution,” *Science* 317, no. 5841 (August 24, 2007): 1039–40, <https://doi.org/10.1126/science.1144241>; and Scott Atran and Jeremy Ginges, “Religious and Sacred Imperatives in Human Conflict,” *Science* 336, no. 6083 (May 18, 2012): 855–57, <https://doi.org/10.1126/science.1216902>.

41. Lani Cupo, “The ‘Replication Crisis’ in Neuroscience: What’s the Path Forward?” BrainPost, November 29, 2022, <https://www.brainpost.co/>; and Nafisa M. Jadavji et al., “Editorial: Reproducibility in Neuroscience,” *Frontiers in Integrative Neuroscience* 17 (2023), <https://www.frontiersin.org/>.

42. This argument builds on the analysis of precision weapons, which have had the counterintuitive effect of prolonging urban conflicts in some cases. See Michael J. McNerney et al., *Understanding Civilian Harm in Raqqa and Its Implications for Future Conflicts* (RAND Corporation, March 31, 2022), <https://www.rand.org/>.

43. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford University Press, 1971), 111–15.

Chapter 15

Degrading the Performance of Humans in the Mind-Tech Nexus

*Nicholas Wright, Georgetown University, University College
London, Center for Strategic and International Studies*

Abstract

*The US joint force's service personnel, their families, and friends are human.¹ Adversaries and other destabilizing forces threaten to sow discord and disruption among these humans to degrade collective capabilities. Such threats can harness the powerful new digital technologies immersing our lives. Effectively defending the joint force's humans from information threats is crucial to protect its competitive capabilities: in our current era of gray zone competition, during escalation scenarios, and in war. This chapter first describes which minds we are defending in the joint force and then the information threats we are defending them against. The chapter then gives the example of generative artificial intelligence (GenAI) and deepfakes to illustrate how new technologies change the character of information threats—even though the nature of those threats remains the same because the humans on the receiving end remain human. Finally, the chapter describes a practical, effective response centered on “3 D's.” **Detect:** Build capabilities to detect and characterize influence operations against the joint force—who is targeted, by what means, and for what purposes? **Defend:** Human cognition always contains vulnerabilities, which can be minimized and so denied to others. Mass personalization of influence operations is coming; countering it requires new human-AI teams and organizations. **Democratic compatibility:** Make new capabilities compatible with a free society while also mitigating the gaps this entails. Restraint is not just a bug of the US system, it is a strength.*

Introduction

To seduce the enemy's soldiers from their allegiance and encourage them to surrender is of special service, for an adversary is more hurt by desertion than by slaughter.

—Flavius Vegetius Renatus, c. 378 AD

Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.

—President Dwight Eisenhower's Farewell Address, 1961

Put yourself in the shoes of an adversary. The US joint force possesses great strengths but also inevitable vulnerabilities that can be exploited by a thousand cuts over time. Sowing discord and leveraging grievances within a military or between a military and its society are age-old strategies in Western or East Asian societies.

From that adversary's point of view, the millions of humans in the US joint force and its support networks offer a vast patchwork of target audiences—a tempting smorgasbord—most of whom can now be neatly identified, characterized, and reached via social media or other digital means. In 2021 Facebook ad services still kindly let (almost) anyone target US military personnel.² According to recent Pew Research Center statistics, one-third of US adults say they use China's AI-powered TikTok, 59 percent of adults under thirty report using it, and 52 percent of US TikTok users say they regularly get news there.³ It is a huge challenge to defend millions of minds from information operations that can harness our era's powerful technologies.

But US overreactions to information threats do the adversaries' job for them. In a global gray zone competition between democratic and authoritarian states, keeping democracy healthy at home is key. Extended witch hunts or requirements for total political homogeneity are unlikely to help.

Success for the joint force is, then, to react effectively but within the democratic constraints of a free society. That is,

to deny the adversary their objectives by preserving the value of the Joint Force's human and organizational resources (or, in the

event of a successful attack, recovering lost value), and to do this without damaging the health of U.S. democracy.⁴

This chapter first describes the millions of minds in the joint force and its support networks and then the information threats they face. Next, the chapter uses GenAI to illustrate how technology may change the character of information operations. Finally, it describes a practical, effective response that requires the US joint force to harness the Mind-Tech Nexus in a strategy centered on “3 D’s”: **Detect, Defend,** and **Democratic compatibility.**

Which Minds Are We Defending?

The US currently has around 1.3 million active-duty service personnel. They comprise less than one-half of one percent of the US population and differ demographically from the broader US population.⁵ The military is, for instance, younger than the civilian population, with about 70 percent of enlisted Marines aged twenty-four years old or younger.

The joint force and its key support networks further broaden the US defense force’s strength. There are some 1.02 million reservists.⁶ In 2019 about 4.2 million personnel from the federal government and government contractors were cleared for access to Secret and above information, of whom some 3.6 million were Department of Defense employees or contractors.⁷

Moreover, as the poet John Donne wrote, “No man is an island, entire of itself;” with families and friends being hugely important sources of both resilience and influences. Defending families is not a new concern for the US military, for instance, as attested to by debates about the presence of families in South Korea.⁸ Nearly two-thirds of privates in a recent report said a family member influenced their decision to join and that families provide key support when problems arise.⁹ In the old maxim, the “military recruits a Soldier/Sailor but retains a family.”

Any enterprise with millions of humans will include a reasonable number (even if a low proportion) who will suffer from financial stresses, mental health, marital, or other life problems. Life events can be part of the cause, although not the sole cause, of vulnerabilities and can even lead to extremist radicalization—as we know from extremism of many types among the US population.¹⁰ They can increase risk factors and decrease protective factors to provide fertile ground for grievances that adversaries can channel.

Furthermore, the millions of entirely healthy, happy humans in and supporting the joint force are all human and thus exhibit cognitive biases and use heuristics. Heuristics like “familiarity” can make social media users believe false news stories, while the sharing of false news stories may be largely driven by inattention and novelty.¹¹ The members of the joint force also all vary along cognitive or personality dimensions that mean some people, for example, are more likely to perceive conspiracies or develop highly polarized political views.¹²

Moreover, the humans in the joint force also expose potential vulnerabilities as they move through different contexts, for example, across times of the day, their careers, and their lifespans. Digital media magnify this challenge because now adversaries can easily target specific time periods, as we see in standard commercial targeting by US big tech companies.¹³ Now consider these myriad audiences from an adversary’s perspective: these humans present a tempting array of potential target audiences for information operations.

Technology helps adversaries understand these audiences. US citizens are already analyzed by companies like Facebook or by “digital brokers” who aggregate remarkably detailed data about US citizens and sell it. In addition to purchasing data or insights from US sources, adversaries can use other sources like China’s data-hoovering TikTok. Even if an individual in the joint force is not on TikTok or other social media, their siblings, parents, children, or friends may be—providing wonderfully rich data for understanding that audience, finding vulnerabilities and ways to influence.

But vulnerabilities only matter insofar as they might be exploited.

What Are We Defending These Minds From?

In information defense, the goal is to preserve the value of the resources or, in the event of a successful attack, recover lost value.¹⁴ Value in this case is the ability of the humans in the joint force to coordinate and collaborate to successfully carry out their missions, which requires a level of commitment and trust in those around them and in the broader organization. Adversaries and other destabilizing forces threaten to sow discord and disruption among the humans in the joint force to degrade collective capabilities.

We discuss how information threats arise from external sources (i.e., foreign) and internal sources (i.e., domestic) and then how these interact.

External Adversary Information Operations

State and non-state actors threaten to disrupt, degrade, or distract the joint force. As old as warfare itself, contemporary examples include Russian operations against Ukrainian and NATO troops (described in Box 15.1). Consider the following four overlapping ways the external challenge can manifest.

- “*Active measures*”: Semi-covert or covert intelligence operations to shape an adversary’s political decisions, these were used and developed extensively by Warsaw Pact countries in the Cold War including against US and Allied militaries. Scholar Thomas Rid describes three key features.¹⁵ First, active measures are not spontaneous lies by politicians but are the methodical output of large bureaucracies (typically intelligence agencies). Second, they all contain an element of disinformation (e.g., forged content). Third, they are always directed against an end, usually to weaken a targeted adversary (e.g., creating wedges between groups or trust in societies), although they may have a single narrow objective (e.g., against a specific weapons system, like in the 1970s/’80s rousing of European opposition to the US “neutron bomb”). Active measures are very human activities devised by creative people to exploit others’ psychological vulnerabilities.
- “*Foreign Influence Efforts*”: A 2020 Princeton study identified and described seventy-six “foreign influence efforts” in which foreign governments have used social media to affect politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation.¹⁶ They define these as (1) coordinated campaigns by one state to impact one or more specific aspects of politics in another state, (2) through media channels, including social media, by (3) producing content designed to appear indigenous to the target state.
- “*Sharp power*”: Sharp power is an approach to international affairs that typically involves efforts at censorship or manipulation to sap the integrity of independent institutions.¹⁷ Broader than just “information operations,” it seeks to use the openness of Western societies against them and applies multiple instruments of national power, as seen with Chinese sharp power against Australia and New Zealand.

- *Long-term shaping and recessed capabilities:* Billions of smart devices are penetrating our homes globally. If the toasters, refrigerators, telephones, and lights in the homes of most citizens in the US, its allies, and partners have authoritarian surveillance capabilities baked into their design, clearly this is a challenge for all US institutions including the joint force.¹⁸ Now consider the long-term recessed capabilities that an adversary can derive from TikTok's data and analyses about millions of humans in and around the joint force. Or consider "smart cities" being built across the world, which currently center on surveillance and will be future battlespaces. All these factors will shape the information terrain to the benefit of US adversaries.

Box 15.1. Russian gray zone information operations against Ukrainian and NATO troops¹⁹

Shortly after fighting started in eastern Ukraine in 2014, soldiers deployed to the combat region received "fake texts" to threaten and demoralize them: "Ukrainian soldiers, they'll find your bodies when the snow melts," or "Nobody needs your kids to become orphans." Other text messages aimed to undermine unit cohesion and morale. Texts, which often appeared to come from fellow soldiers, claimed the commander had deserted and that "we should run away." Text messages sent to one's phone are much harder to ignore than leaflets or radio messages.

Russia also combines information and kinetic operations, as in the following example. A text message to a soldier first tells him he is "surrounded and abandoned." Ten minutes later, his family receives (via his recent contacts) a text message stating, "Your son has been killed in action." Family and friends then likely call him to see if the news is true. Seventeen minutes after the initial text message, he receives another message telling him to "retreat and live," and shortly thereafter, an artillery strike follows to the location where the large group of targeted cell phones were detected. This strategy blurs the geographical boundaries between the front line and the home front.

NATO troops deployed in the Baltics and Poland to deter Russia have also been targeted. This includes hacking their Facebook accounts, erasing data, or receiving a message stating "someone is trying to access your iPhone" that includes a map with Moscow at its center. This may intimidate soldiers, by letting them know that Russian intelligence forces are tracking them and that their data is at risk.

Box 15.1 (*continued*)

Texts that falsely announce infidelity and injuries are sent to NATO soldiers' loved ones back home, as described by Commander Michael Widmann of NATO's Co-operative Cyber Defence Centre of Excellence based in Tallinn, Estonia.²⁰ "It throws you off," he said. When he led the world's biggest military cyber-exercise in April 2021, NATO's Locked Shields 2021, it included the hacking of participants' mobiles.

Russia has also targeted local support networks for the US military in Europe, attempting to decrease its military readiness and that of its NATO allies. Russian media outlets have, for instance, reached out to mayors of towns outside of the Hohenfels training area in Germany, inquiring about military training noise disrupting the local population.

In 2020, a Canadian-led NATO battle group in Latvia was targeted by a pandemic-related disinformation campaign ahead of a major exercise, which commanders said they believe originated in Russia.²¹ Reports circulated in Baltic and Eastern European media outlets falsely suggesting that the contingent at Camp Adazi in Kadaga, outside the capital of Riga, had "a high number" of Covid-19 cases.

Internal Threats from Extremists

All societies and their institutions will face challenges from extremism because there will always be extreme humans. An analysis of the US showed that, in 2019, some 1.5 percent of all domestic terrorist incidents were linked to active-duty and reserve personnel, and 6.4 percent were linked in 2020.²² The challenge for the joint force is how to minimize their numbers and, given the special capabilities they possess, their impacts on society and on the Joint Force's collective capabilities.

Interactions between external and internal threats: The US has long distinguished between internal and external threats. Americans have entrenched historical traditions that abhor military involvement in civilian affairs, at least under ordinary circumstances. These find tangible expression, for example, in the nineteenth-century Posse Comitatus Act, which forbids the Army (and other military organs) to execute civil law except where expressly authorized.²³ The long-term health of US democracy requires the clear-cut distinction between "external" and "internal."

But although the internal-external distinction is enormously beneficial, it also means that a fundamental challenge for the US will always be a "seam" between the external and internal that adversaries can

exploit. A great analogy was related to me by a retired US Army colonel who originally started as a beat cop in Houston:

Working “across the seams” [is] something that all government and commercial enterprises struggle with. As a beat cop in Houston (radio patrolman), and subsequent crime analyst searching for patterns of criminal activity throughout the city and region, analyzing and working across the seams of the geographic separations of the city were most troublesome. The “seams” between the six police substations and areas of responsibility in a city the size of Houston were indeed problematic. There were criminal entities that knew both the geographic boundaries and times of shift change (another seam if you will) that existed within the Houston Police Department, and they routinely sought to exploit those self-imposed separations of authority and responsibility to their benefit.²⁴

A free society can mitigate but never eliminate the vulnerability from this seam, certainly outside a total war.²⁵ For example, once a Russian narrative gets picked up by US news outlets, the US government cannot employ all available instruments of power against this threat because it can now propagate as protected speech. Authoritarian adversaries—like the Cold War Soviet Union—may suffer from other weaknesses relative to democracies, but they have powerful domestic organs to shut down undesired information. This seam poses a greater challenge for the United States.

The joint force must recognize and manage significant linkages across this seam:

- External and internal information threats often combine, not least because existing domestic social discord is a prime target for foreign adversaries. Soviet Cold War active measures, for instance, leveraged existing fissures.²⁶ Internal and external threats can harness the same tactics with information, e.g., spreading misinformation and disinformation.²⁷
- Many key actions to defend the joint force against external and internal information threats are the same, as described below.
- Digitization changes the character of information threats because hugely denser interconnections between societies blend “domestic” with “foreign” and so vastly increase the attack surface for external

adversaries. Sowing discord in Delaware used to be tricky for foreign adversaries; now, they can do it from bed.

- Finally, many powerful digital technologies are built for US companies to influence domestic audiences for commercial ends (to buy more beverages or a new phone) but can be harnessed by external adversaries.

We must meet these age-old challenges. But how will they manifest in our AI-enabled era?

New Technologies: Generative AI as an Example of Evolving Challenges

The nature of information threats remains the same because the humans on the receiving end remain human, but factors like technology change their character. This section illustrates how GenAI may change the character of information threats—particularly the “deepfakes” that arise from GenAI.

Generative AI is AI that can learn the structure of a type of data (e.g., pictures of dogs or cats) and use that to generate new instances of that data. It does this by learning how the properties of each type of thing varies, so it learns what pictures of dogs or cats can look like. From this knowledge, it can generate new instances of pictures of dogs or cats—or even “dog-cats,” a photo that mixes the two categories.

As well as doing this for pictures, the data could be language—so for example GenAI could learn the structure of how a computer coding language is written and then create new instances of computer code. Or it could learn the structure of videos of Tom Cruise, the US president, or the US CENTCOM commander and generate new instances of such data. GenAI can also write text like a particular person if it has enough of their personal messages to work with.

Generative AI is fashionable at the time of this writing, helping students do (or cheat on) homework through programs like ChatGPT (“Chat *Generative* Pre-trained Transformer”) and driving trillions of dollars of tech company stock price changes. And it is a powerful technology.

In the commercial world, the two big 2023 use cases for GenAI seem to be computer coding and marketing. For computer coding, Microsoft’s GenAI “Copilot” uses GenAI to suggest large chunks of

code when someone starts typing; it now has 1.3 million paid Copilot accounts, with over 50,000 companies using the software.²⁸

In marketing, one of the world's largest marketing companies, WPP, recently demoed its internal AI workspace, which gives employees managed access to a range of GenAI models across text and imaging.²⁹ WPP also discussed training models for particular brands' voice (what you say) or tone (how you say it). It already has almost 30,000 users and millions of prompts (the command the user inputs into the GenAI). Meanwhile, Coca-Cola talked about using GenAI to create thousands of marketing assets automatically. Marketing is related to many aspects of information operations: information operations specialists in Russia, China, or America would be failing in their duties if they did not think about how to use these new technologies and defend against them.

Deepfakes are one of the products that GenAI can make. They are called deepfakes because the GenAI that made these fake media used an AI technique called "deep learning." *Deepfakes* can be defined as AI-generated synthetic media (e.g., images, video, or audio) that most commonly involve a person saying or doing something that they did not say or do.³⁰

Deception and forgery are old. Entire books have been fabricated. For instance, the infamous *Protocols of the Elders of Zion* first appeared in 1903 and was largely copied from an obscure, French-language political satire.³¹

What is different with deepfakes is largely that new technology—GenAI—makes powerful tools of fakery available much more cheaply, rapidly, easily, and widely. Deepfakes arose chiefly from dual-use technology as a byproduct of AI advances and civilian uses of synthetic images for entertainment. Indeed, deepfake-like technologies will likely become commonly used globally for synthetic personal or retail assistants and healthcare applications, such as aiding those whose disability affects their speech. They emerged around 2018 to make fake pornography.

Deepfakes provide adversaries with new openings for mis- and disinformation in three primary ways:

- *Unexpectedness*: Currently, as individuals and collectives we are poorly prepared for realistic fake videos, pictures, or audio—when deepfakes are used creatively, the surprise they cause can catch our attention³² or even fool us into believing they may be real.

Importantly, these reactions will likely fade as we become used to deepfakes. Emails or computer-generated imagery (CGI) in movies were novel when introduced.

- *Mass-produced disinformation*: Deepfakes are now easily mass produced and “broadcast.” They might be distributed in a cheap and dirty way, for example, by enterprises like the “troll farms” of Russia’s “Internet Research Agency” or the Macedonian entrepreneurs who flooded US social media audiences with fake posts.³³ More sophisticated and potentially much higher impact ways to use broadcast information are described in Box 15.2.
- *More exquisite “active measures”*: High-quality, carefully crafted deepfakes also have uses. Reportedly, for example, a deepfake of the voice of a company boss successfully fooled a subordinate into transferring a large sum of money, a financial crime that required detailed knowledge of the company.³⁴ In another potential use, high-quality deepfakes might be hidden among troves of genuine stolen media and leaked to the media—a trick successfully used with other media during and after the Cold War.³⁵

But deepfakes are also limited, particularly if one remembers the key fact that *the main aim of mis- and disinformation is to create effects in audiences’ minds*. Limitations include the following:

- *Expectation of deepfakes*. Children now play with GenAI to generate images, write stories, or help with their homework. This new generation will develop different criteria for judging an image or phone voice as real or fake or something in between. The criteria the GenAI “natives” use for such judgments will not necessarily be better or worse than those of previous generations but different. For example, they may rely more on other metrics, such as whether the content is shown by a news source they trust (e.g., the BBC, *The New York Times*, or Fox News).
- *Insufficient quality or quantity of data*. Highly convincing deepfakes still require a lot of computational power and, more importantly, data about the people to be faked. Videos of Tom Cruise can be faked so well in large part because we have many videos of him. Except for deepfakes of people for whom many videos exist, unless there is a new technological leap (e.g., in the ability to generalize learning from small amounts of data), we are unlikely to see mass-produced and highly convincing video deepfakes soon.

- *Good detection mechanisms.* The systems in place are effective in discovering deepfakes and can often catch up quickly with advances in deepfake manufacturing.³⁶ Many AI researchers believe this may change so that deepfakes become undetectable, even if digital “watermarks” are used, but this outcome is uncertain.³⁷ Indeed, given the uncertainty about future detectability, adversaries are likely to keep back their novel deepfake tech to act as a “zero-day” exploit, a vulnerability previously unidentified by the defender so that it has zero days of notice to fix it before damage is done. To help mitigate such novelty, defenders should set up a “zoo” to share deepfakes.³⁸
- *Capability of the creative talent.* Most importantly, a convincing picture or video requires ideas and points of leverage for the minds in the target audiences—requiring creative, talented people to design effects. Will the media produced be funny, shocking, or believable enough?

For these reasons, deepfakes used alone will likely exert only limited influence. Instead, deepfakes will most likely be useful as one tool in “combined arms” information operations to create effects in audiences, much like the German panzer forces combined infantry, tanks, and artillery to devastating effect. Consider some other tools with which deepfakes can be used in “combined arms” information operations.

- *Cropping real media* or mislabeling media with a *fake context* can be as effective as fancy AI to create effects in audiences (see fig. 15.1, next page). Combining deepfakes with other types of fakery can help keep things fresh for audiences and create problems for defensive content moderators (human or AI)—particularly if “ironic” or “funny” versions are used to push the boundaries of what is allowable.
- *Conversational systems* can drive realistic fake bot identities on social media, which can be given plausible “faces” by deepfakes. *Social bots* are algorithmic software programs designed to interact with, or send information to, humans. Bots powerfully amplify commercial messages.³⁹ Again, they have political uses. Bots published perhaps a third of all tweets about the Brexit referendum. They may have spread propaganda in fifty countries.⁴⁰ Most bots are not yet powered by sophisticated AI, although they are becoming available to further semi-automate campaigns.⁴¹ Con-

versational “chatbots” or AI personas form another huge commercial and research area.⁴²

- *Microtargeting* is a form of online targeted advertising that analyzes personal data—a role AI can play—to identify a specific audience or individual’s interests to influence their actions.⁴³ Facebook’s original social network produced the data that afforded commercial microtargeting, and then that microtargeting apparatus afforded political use.⁴⁴

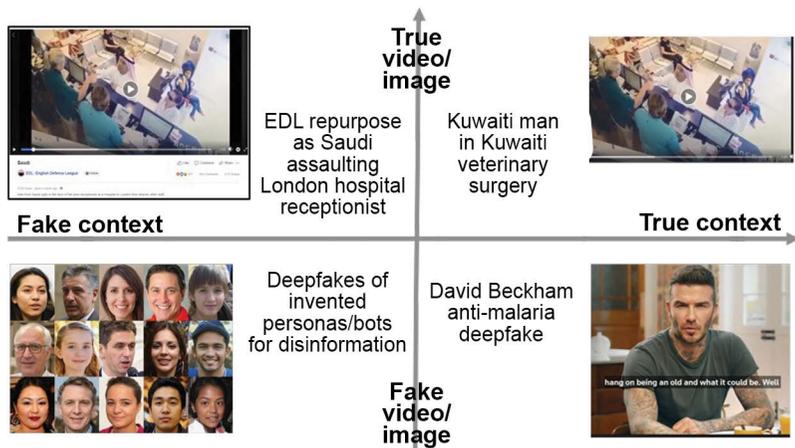


Figure 15.1. Deepfakes and context in disinformation campaigns.

A true video of an angry Kuwaiti man (top right) was repurposed on social media by the far-right “English Defence League” in a fake context (top left). Deepfakes can enable footballer David Beckham to promote an anti-malaria campaign across many languages (bottom right), or malign actors can create fake faces for fake personas (bottom left). The top two images are from Remi Banet and Salima Lebel, “No, This Is Not a Video of a Saudi Assaulting a London Hospital Receptionist,” Fact Check, July 30, 2018, <https://factcheck.afp.com/>. The bottom left image is from Paige Leskin, “The AI Tech behind Scary-Real Celebrity ‘Deepfakes’ Is Being Used to Create Completely Fictitious Faces, Cats, and Airbnb Listings,” Business Insider, February 26, 2019, <https://www.businessinsider.com/>; and the bottom right image is from Reuters, “David Beckham’s ‘Deep Fake’ Malaria Awareness Video,” Reuters Video, accessed June 2021, <https://www.reuters.com/>.

Box 15.2. Mass personalization and deepfake injections: the joint force in an escalation scenario

Mass personalization of retail has already been rolled out at scale by companies like Amazon, where recommendations based on big data contribute to vast profits. Mass personalization of healthcare that tailors treatments to individual patients versus big groups is on the way.⁴⁵ Facebook sells the ability to influence humans in highly precise ways at mass scale.⁴⁶ Meanwhile, China's tech titans like Alibaba are no slouches at using big data for mass personalization.⁴⁷ Why would mass personalization not be applied to information operations in security?

Personal data on joint force members will be a key fuel for exploitation, such as from medical and financial records, TikTok use, or dating sites. Data about family can also be leveraged: that fun genomic data bought as a birthday present may reveal that somebody's father is not who they think he is or that a partner had an affair.

Many options exist for how adversaries can use this information. Firstly, the data can train AI, with some human help, to find tempting target audiences in the joint force. Secondly, weaponized personal data on millions in the joint force or their families can be injected into their social networks.

Leaking damaging data on members of the joint force at key moments, such as during a China-US escalation scenario or limited war, might have some utility. And while embarrassing details are coming out, what about slipping in some invented damaging data where none exists? It could be targeted at individuals' social media. Or perhaps troves of analyzed data could be released by "free speech" third parties like a new Wikileaks. Or a leak could be an Ashley Madison-style data dump from hacked databases revealing personal information, such as financial problems, gambling habits, computer pornography, sexual health treatments, the results of drug or alcohol tests, or sexual experimentation. It could never happen, one might say. Soviet Cold War information operations included publishing *Who's Who in CIA*, listing agents and others incorrectly labeled as agents, to which the US responded by publishing its own list of KGB agents.⁴⁸ In a China-US escalation scenario or limited war, would the US hold off attacking parts of the digital authoritarian apparatus, such as the Social Credit System by which the Chinese Communist Party (CCP) increasingly maintains its authority? Such an attack by the US might be

Box 15.2 (*continued*)

perceived as a threat to regime security (the CCP's top priority) and thus perhaps be more escalatory than leaking personal data about humans in the joint force.

New *human-AI teams* and *organizational* advances to bring them are needed at the scale of this defensive challenge.

GenAI and deepfakes also illustrate the criticality—for information offense and defense—of harnessing neither humans nor tech alone but *the Mind-Tech Nexus*. Humans alone could not cope with the scale of the challenge. And humans plus AI will be vital because of the limitations of AI currently (and almost certainly in the near future too).

AI is the cutting edge of the constellation of AI-related technologies that together provide powerful, wide-ranging, and new capabilities. These include AI more tightly defined (i.e., are machines doing things thought intelligent in humans), machine learning, big data, and digital things (e.g., the “Internet of Things”). Together, they enable a new industrial revolution—taking the vast reams of data produced by computers and the internet and turning them into useful information. While none are entirely new, recent transformative improvements—particularly in “deep learning” around 2012 and then generative AI around 2018—mean that together these technologies have revolutionary applications.

But these advances have not been uniform, and we must understand three key strengths and three key limitations. AI is currently good at three things:

- (1) Perceiving, for example, images, speech, or patterns in big data.
- (2) Choosing actions in tasks that are bounded enough to be well described by vast amounts of (often labeled) data, for example, logistics in a warehouse.
- (3) Understanding human language commands (“prompts”) to generate new examples of language or other types of media (e.g., ChatGPT).

Thus, real-world impacts now relate largely to perception (e.g., perceiving faces or speech), some bounded decision tasks (e.g., logistics), or new language and media generation (e.g., text, computer code, or deepfakes). Continued rollout in these areas will likely dominate for the next few years at least.

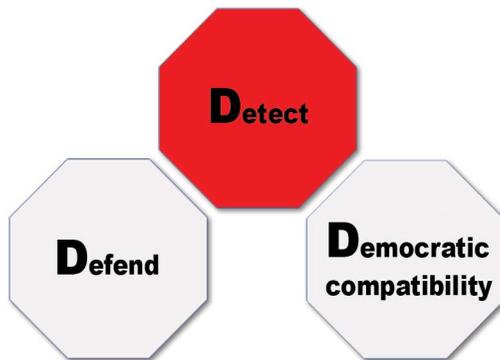
Rolling out AI alone in the real world has been tough in many fields due to its limitations (e.g., medicine, despite all the hype). Currently, AI has three key weaknesses:

- (1) AI deals badly with context, so humans are often needed to make even common-sense judgments.
- (2) AI requires huge amounts of often labeled data, so setting up datasets is frequently a crucial precondition.
- (3) AI often generates new cases that humans easily perceive as silly, such as hallucinating things in text, making basic mathematical errors, or generating pictures of cars with no door handles and two steering wheels.

Consequently, AI's current limitations require extensive human involvement to help deal with context: the Mind-Tech Nexus.

Harnessing the Mind-Tech Nexus to Defend the Joint Force

Defending the joint force from information threats requires humans plus tech, with the organizational structures that most effectively bring together those humans and technologies. Such defense also requires describing what success looks like, which I proposed in the introduction as “to deny the adversary their objectives by preserving the value of the joint force’s human and organizational resources (or, in the event of a successful attack, recovering lost value), and to do this without damaging the health of U.S. democracy.” This objective can be achieved through a strategy centered on “3 D’s” that we discuss in turn: *Detect*, *Defend*, and *Democratic compatibility*.



DETECT

The joint force will be blind without the ability to detect and characterize adversary influence operations against the joint force (fig. 15.2). It must have the capability to identify who is targeted, by what means, and for what purposes. Such detection must operate at multiple scales, including specific instances of mis- and

Figure 15.2. The 3 D's: Detect

disinformation coordinated campaigns and how adversaries may shape the information terrain over years or decades (fig. 15.3).

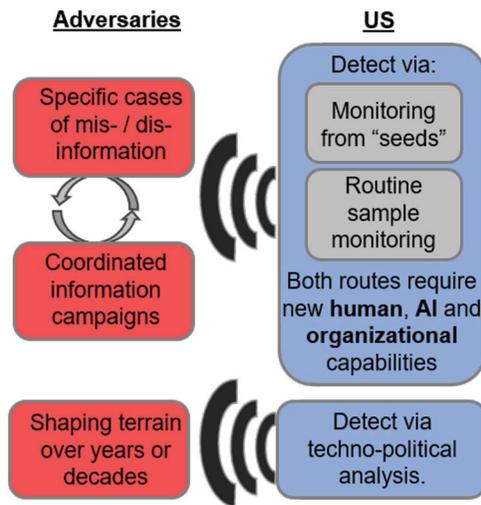


Figure 15.3. Detection at multiple scales. Detection may involve routine monitoring of social media/online interactions of a sample of those within the joint force and its support networks who have already submitted themselves for enhanced monitoring in order to detect adversary activities that can then be investigated more closely. It may also involve building wider (but still carefully limited) digital investigations of social media/online activity by groups in the joint force based on investigative “seeds” derived from other legitimate sources (e.g., individuals identified as compromised by other sources or who are unknowingly in contact with adversary influence networks).

Detecting specific instances of mis- and disinformation. Detecting specific instances of misinformation—such as a particular fake story or deepfake—helps efforts to reduce the noise of untrustworthy information in the information environment. It is also vital to feed into counterintelligence at scale to detect coordinated campaigns. To detect specific instances of misinformation at scale, neither humans nor AI alone is sufficient. Consider the example of deepfakes “broadcast” as part of a mass information operation, for which effective detection at scale must employ

- *technology* for deepfake detection at scale,

- trained *humans* who can add contextual understanding that helps defeat adversary “combined arms” techniques to avoid detection (e.g., use of “irony”), and
- *organizations* like a “deepfake zoo” to share deepfakes so that many deepfake detectors can learn, as well as organizational links that can distribute knowledge about specific deepfakes at the speed of relevance so social media platforms can stop them from being uploaded or shared.⁴⁹

Specific media or stories are, however, often only one part of a broader influence campaign.

Detecting coordinated campaigns. External adversaries like China or Russia can mount broad, coordinated campaigns employing “combined arms” information operations. Characterizing coordinated adversarial campaigns will involve detecting aspects of the campaign like its multiple “lines of effort” (e.g., sowing discord between racial or political groups in the joint force to provoke demonstrations or reduce morale) or the campaign’s activities across multiple platforms (e.g., X [formerly Twitter], Facebook, WhatsApp). Such counterintelligence at scale once again requires human, AI, and organizational capabilities.

- *Technology* includes AI such as that funded by DARPA that can address parts of this problem (e.g., Influence Campaign Awareness and Sensemaking [INCAS] or Collection and Monitoring via Planning for Active Situational Scenarios [COMPASS], even though DARPA’s entire budget is small compared to the big tech companies that make dual-use offensive tech).
- Trained *humans* and *organizational* systems are needed to coordinate and integrate across multiple sources of intelligence (not only digital and derived from sources including the joint force, intelligence community, and cyber sources) in order to characterize digital social networks at the scale of the audiences targeted in the joint force. The target audiences may be dozens, thousands, or even millions of humans.

Working outside the joint force might help to provide sufficient experience to adequately train the human, AI, and organizational components of this counterintelligence at scale. For instance, we might include allies and partners who are subject to more active adversarial information operations (e.g., the Ukraine, Baltic states, Taiwan, or Middle Eastern states).

Detecting how adversaries shape the terrain over years. The US benefits enormously from having shaped the global information terrain in which the joint force's humans live and work—through US global tech giants, its position at the center of global communication networks (particularly as part of the “Five Eyes” intelligence-sharing apparatus) and global financial networks (e.g., the Society for Worldwide Interbank Financial Telecommunication [SWIFT] banking system).

But now China's heft enables it to shape the global information terrain more in its favor: from global AI standard setting to the global social media platform TikTok to building global undersea and outer space communication networks. The humans in the joint force will be ever more immersed in digital technologies, and the US must be able to detect the risks posed as China increasingly shapes this terrain.

Consider the Chinese social media company TikTok. It is hugely popular with young Americans. TikTok owns and shapes the terrain on its platform, not only the algorithms that determine what people see and what becomes popular but also how millions of users are split into target audiences, how insights are derived about those target audiences, and how effective those insights are for driving influence. What can the US reliably detect on such terrain? And, of course, TikTok is harvesting vast amounts of data to build profiles of many of the humans who will populate the present and future joint force.

It is unclear how the joint force can be adequately defended while crucial social media are owned or operated by nations beyond trusted allies and partners. The joint force should recognize that “the market” on its own will not build and deploy all the capabilities needed to detect adversary information operations or surmount the challenge posed by a hugely popular Chinese owned or embedded entity like TikTok. However, requirements for the security of the joint force are seen as important in US politics, and other interest groups, such as those for copyright theft or children's rights, have successfully used clear and forceful arguments to compel changes from big tech.⁵⁰ The joint force must help correct market failures by specifying the capabilities it needs, arguing for them in appropriate forums, and, where necessary, funding their development.

DEFEND

Individuals' cognition will always contain vulnerabilities as targets for disruption, which the joint force can help minimize and so deny to others (fig. 15.4). No panacea can exist. Instead, minimizing these vul-

nerabilities requires ongoing improvements to defense at multiple scales: the individual human, coordinated campaigns, and shaping the information environment over years or decades. We discuss each in turn.

Defending at the individual human scale. The joint force can help defend an individuals' vulnerabilities, enhance their resilience, and give them the technological tools to defend themselves online. No single intervention is decisive, so effective defense must rely on combining multiple interventions.

Helping individuals when they have problems can *make individuals harder targets* for grievance merchants both foreign and domestic. The joint force should strive for continuous, evidence-based improvement to the provision of pastoral care, mental health services, family support, and training for future employment. Predictable periods of enhanced vulnerability should be anticipated, for example, by providing additional social support for military families as they go through transitions like new postings. None of this is “sexy” policy, and it is no panacea, but such measures can help reduce vulnerabilities in potentially attractive target audiences for adversaries.

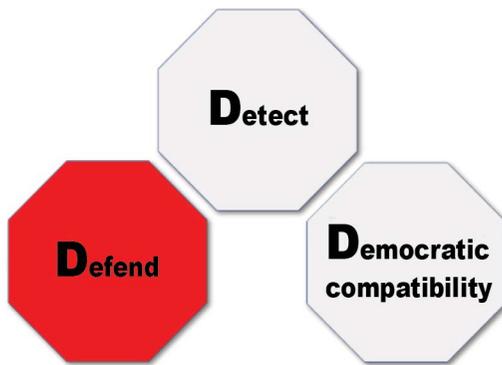


Figure 15.4. The 3 D's: Defend

Give individuals the *technological tools* to defend themselves online. “Middleware” is software that rides on top of an existing platform and can modify the presentation of underlying data.⁵¹ One example is NewsGuard, which uses a team of human journalists to rate news sources for reliability (e.g., *The New York Times* or Fox News) and should be free to all joint force personnel.⁵² NewsGuard has begun collaborating with AI systems. Clearly, such tools will mostly appeal to the already news savvy unless they can be bundled with browsers, apps, or similar platforms.⁵³

Training can address simple things like how to ensure that individuals' digital privacy settings are set as high as possible, what apps might be risky (e.g., TikTok), or what military rules mean for social media (e.g., the *Uniform Code of Military Justice*). Training in more formal

settings can be aided by outreach at places like local shops or other communal areas on topics like changing the settings on phones or other devices (which big tech makes deliberately difficult to understand).

Designers of training programs should put themselves in the shoes of the audience—in this case, the humans in the joint force—and find ways to offer information the audience values. Telling people that they are “illiterate” about media is unlikely to provide a good route to help them better defend themselves. Nor will telling people they need “education” in how to think properly. But training in how to evaluate social media content can be beneficial and should be justified to the joint force by explaining how simple techniques can help prevent adversary information operations from sowing discord and degrading the force’s capabilities.⁵⁴ Engaging documentaries or other media explaining adversaries’ use of social media—for example, by China in Taiwan or Russia in its near abroad—and the broader social media business models may also be helpful for some.

The joint force must also establish *clear expectations* in the individuals’ minds.⁵⁵ For example it should be clear that high privacy settings are expected, so it will be frowned upon to do otherwise. Similarly, clear codes for political content exist on posting political content (and that also specifically encourage political engagement),⁵⁶ and it should be clearly understood that breaking these existing rules can and will result in disciplinary action up to and including legal sanctions.⁵⁷ The aim is to change social norms in the joint force.

For all these interventions to defend the individual level, more research is needed on effectiveness.⁵⁸ Fashionable as “education” currently is, for example, as a recent RAND review notes, “there is little causal, evaluative research in the ML [media literacy] field that isolates the effects of ML interventions.”⁵⁹

Defending individuals at the organizational scale. Individuals in the joint force cannot defend themselves alone. They must entrust their information to others, such as medical facilities, banks, and personnel departments.

To defend data about individuals, a key principle is to *silo* the sources of data about an individual.⁶⁰ The disastrous Chinese hack on the US Office of Personnel Management computer systems that accessed intimate data on about 22 million individuals, including security clearance applicants and current or former federal employees, illustrates an inherent problem of building a giant honeypot.⁶¹ Received wisdom among many in the public and private sectors is to structure “silos” in which

data in one department is isolated from the rest of the organization, much like grain in a farm silos.⁶² But there is a trade-off. Adversary information campaigns require data to understand and thus influence target audiences in the joint force. As AI becomes more prevalent, denying adversaries integrated data on individuals will become more critical. Denial becomes preeminent because AI learning requires large amounts of data—and it is particularly helpful to have integrated data that includes high-quality “ground truth” information, such as tax returns, medical records, or personnel files.

To bolster defense, the joint force should also prepare in advance to deploy *deterrence*, *offense*, and *emergency response*. However, it should implement such capabilities sparingly outside of escalation or war, and organizations should avoid overreacting. This response was arguably seen with aspects of US domestic surveillance after 9/11 or in some East Asian countries for surveillance of Covid-19.⁶³

Defensive information operations should employ *evidence-based methods for influence*, for which many good frameworks exist.⁶⁴ Defense should anticipate vulnerability at the *seam between domestic and foreign* entities, both to maintain this important distinction and to enable US information defenses to coordinate from both sides.

Defending against shaping of the information terrain over years.

If the joint force conducts defensive information operations on TikTok, it will compete on terrain designed by a highly capable competitor. If TikTok is not banned in the US, the joint force should ban its use where it can and discourage its use more broadly. The same is true of a host of smart cities and other technologies where the US and its allies should aim to set standards and where the joint force can help identify and mitigate potential information threats. Key efforts would include building alternatives to 5G technologies (in which China is strong), gaining leadership in 6G, and reinvigorating US innovation alongside allies.

Moreover, the joint force should encourage and where necessary help build a thriving news and information ecosystem for the joint force and its support networks as far as it can. That should include trusted messengers tailored to the distinctive needs of the multiple audiences in the joint force and its support networks. The human communities in the joint force require trusted and engaging news sources, analogous to local newspapers that help report on stories of local interest and importance—which are themselves under threat.⁶⁵ This is unlikely to be met by market forces alone.

Detection and defense at the scales of the individual, organizational, and information terrain-shaping over years are all needed, but they are not enough for democratic success.

DEMOCRATIC COMPATIBILITY

US success in Cold War information operations rested in large part on what the US chose not to do. Scholar Thomas Rid's book *Active Measures* (2020) describes how US information operations showed considerable restraint after the early stages of the Cold War against the far more aggressive and well-resourced Soviet Union apparatus. US Cold War capabilities were employed—not, of course, without imperfections—within ethical, legal, and political frameworks that rendered them compatible with a free society (fig. 15.5). So, too, must the latest US capabilities, as the joint force has embarked on a new gray zone conflict also likely to last decades. And this time, the US joint force must *defend* itself from information threats in an AI-enabled world. In doing so, it must accomplish the following.

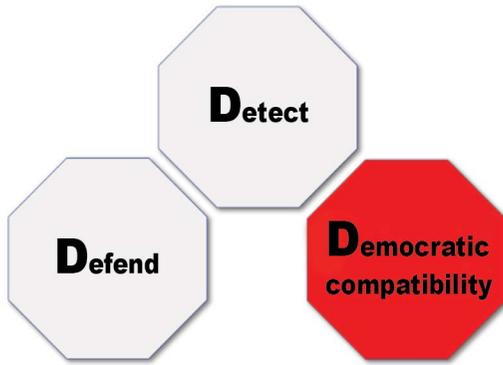


Figure 15.5. The 3 D's: democratic compatibility

First, maintain the seam between domestic and foreign—and manage the vulnerabilities that brings. The joint force should build detection and defensive capabilities without eroding safeguards such as posse comitatus and intelligence oversight—which, as discussed above, requires new methods of coordination to mitigate the gaps and lack of agility this seam entails. In addition, many of the key actions needed to defend the joint force against external and internal information threats are the same (e.g., mental health and social support); thus, focusing more on these efforts will raise fewer domestic problems.

Second, focus on minimizing vulnerabilities in ways that pose the least dangers to democracy, for example, by helping individuals become more resilient, protecting their data, and reducing TikTok's large US presence. Some detection and defensive capabilities carry fewer risks

to democracy (e.g., enhancing social and mental health support) than others (e.g., building offensive information capabilities that can turn inward), and we can prioritize safer options, which I have tried to emphasize in this chapter.

Third, build robust ethics into the mindsets of individuals charged with detecting and defending against adversary information operations and into the cultures and processes of their organizations. One must remain grounded in the realities these communities face because while ethics is crucial, not least for effectiveness and success, the topic often makes practitioners' eyes glaze over a little when they are bombarded with well-meaning, high-level admonitions. It is also often perceived as yet another hurdle for getting things done effectively. Thus, recognize that ethics is a key component of longer-term success, and provide concrete, practical guidelines.⁶⁶ AI alone does not have these capabilities, given its problems with hallucinations (inventing facts that don't exist) and trouble with gray areas (like irony or provocation) in which much influence occurs. The Mind-Tech Nexus will be key.

Fourth, ensure existing frameworks for democratic oversight can operate across the Mind-Tech Nexus, including current and near-future technologies such as AI, the humans who work with these technologies, and how these human-tech teams operate as more than the sum of the parts. That is, oversight will increasingly require expertise across the Mind-Tech Nexus.

Conclusions

This chapter began by asking you to put yourself in the shoes of an adversary. From that point of view, digital technologies now give you unprecedented opportunities to reach deep into US society, so you can directly target myriad audiences among the millions of humans in the joint force and its support networks. From a competitor's perspective, the future looks bright if you can harness both sides of the Mind-Tech Nexus to combine technical sophistication and human creativity.

How can the US joint force respond? Competitors would much prefer it if the US joint force left itself blind to information threats by failing to build adequate detection, leaving itself poorly defended, or overreacting in ways that were not democratically compatible. No simple answers exist. But we can do much to make the humans and

their support networks in the joint force more frustrating targets for adversaries to influence.

Notes

1. This chapter is an adapted and updated version of a report produced for the United States Department of Defense Joint Staff Strategic Multilayer Assessment (SMA) Group, which sponsored that research as part of a project for Headquarters Air Force to examine Integrating Information in Joint Operations. That report was first published as Nicholas D. Wright, “Cognitive Defense of the Joint Force in a Digitizing World,” ver. 1 (July 2021, Intelligent Biology), <https://apps.dtic.mil/>.

2. Lily Hay Newman, “Facebook Ad Services Let Anyone Target US Military Personnel,” *Wired*, January 28, 2021, <https://www.wired.com/>.

3. Kirsten Eddy, “8 Facts about Americans and TikTok,” Pew Research Center (blog), December 20, 2024, <https://www.pewresearch.org/>.

4. This definition of success is adapted from Dorothy Elizabeth Robling Denning, *Information Warfare and Security* (ACM Press, 1999), with the addition of human and democratic elements.

5. Adversaries might begin identifying target audiences within this 1.3 million using characteristics such as demography, race, or where recruits are enlisted from. For a discussion of these characteristics across services, see, for example, “Demographics of the U.S. Military,” Council on Foreign Relations, July 13, 2020, <https://www.cfr.org/>.

6. Congressional Research Service, “Defense Primer: Reserve Forces,” In Focus, IF10540, June 11, 2024, <https://www.everycrsreport.com/>.

7. C. Todd Lopez, “DOD to Take Over Background Checks by Fiscal 2020,” Department of Defense, June 25, 2019, <https://www.defense.gov/>.

8. Phil Stewart, “U.S. Military Families in South Korea? Top U.S. General Wants a Rethink,” Reuters, December 3, 2020, <https://www.reuters.com/>.

9. Todd C. Helmus et al., *Life as a Private: A Study of the Motivations and Experiences of Junior Enlisted Personnel in the U.S. Army* (RAND Corporation, 2018), <https://www.rand.org/>.

10. Ryan Andrew Brown et al., *Violent Extremism in America: Interviews with Former Extremists and Their Families on Radicalization and Deradicalization* (RAND Corporation, 2021), <https://www.rand.org/>.

11. Gordon Pennycook and David G. Rand, “The Psychology of Fake News,” *Trends in Cognitive Sciences* 25, no. 5 (2021): 388–402, <https://doi.org/10.1016/j.tics.2021.02.007>; and Soroush Vosoughi et al., “The Spread of True and False News Online,” *Science* 359, no. 6380 (2018): 1146–51, <https://doi.org/10.1126/science.aap9559>.

12. Shauna M. Bowes et al., “Looking under the Tinfoil Hat: Clarifying the Personological and Psychopathological Correlates of Conspiracy Beliefs,” *Journal of Personality* 89, no. 3 (2021): 422–36, <https://doi.org/10.1111/jopy.12588>; Max Rollwage et al., “Metacognitive Failure as a Feature of Those Holding Radical Beliefs,” *Current Biology* 28, no. 4 (December 2018): 4014–21, <https://doi.org/10.1016/j.cub.2018.10.053>; and Max Rollwage et al., “What Underlies Political Polarization? A Manifesto for Computational Political Psychology,” *Trends in Cognitive Sciences* 23, no. 10 (October 2019): 820–22, <https://doi.org/10.1016/j.tics.2019.07.006>.

13. Such targeting is prominent on the Google and Facebook advertising websites or online marketing advisers such as Neil Patel, <https://neilpatel.com/>.

14. Offense aims to disarm adversaries, while defense aims to deny them their objective. Success with information requires effective offense and defense, although this chapter focuses on defense.

15. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, illus. ed. (Macmillan, 2020).

16. Diego A. Martin et al., “Trends in Online Influence Efforts,” ver. 2.0, Princeton University, August 5, 2020, <https://drive.google.com/>.

17. Christopher Walker, “What Is ‘Sharp Power’?,” *Journal of Democracy* 29, no. 3 (2018): 9–23, <https://doi.org/10.1353/jod.2018.0041>.

18. Nicholas D. Wright, *Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challenge* (National Endowment for Democracy, August 2020), <https://www.ned.org/>.

19. Except where otherwise referenced, Box 15.1 draws on information from Lionel M. Beehner et al., “The Fog of Russian Information Warfare,” in *Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations*, ed. Bradley S. Loudon and Mark D. Vertuli (Army University Press, 2018), 31–50, <https://www.armyupress.army.mil/>.

20. “NATO Increasingly Sees Its Soldiers’ Phones as a Liability,” *The Economist*, May 22, 2021, <https://www.economist.com/>.

21. Murray Brewster, “Canadian-Led NATO Battlegroup in Latvia Targeted by Pandemic Disinformation Campaign,” *CBC News*, May 24, 2020, <https://www.cbc.ca/>.

22. Seth G. Jones et al., “The Military, Police, and the Rise of Terrorism in the United States,” Center for Strategic and International Studies (CSIS), April 12, 2021, <https://www.csis.org/>.

23. Jennifer K. Elsea, “The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law” (Congressional Research Service, November 6, 2018), <https://crsreports.congress.gov/>.

24. Col. Carl W. Hunt (retired), PhD, private communication with author.

25. Even in war, this must be time limited.

26. Rid, *Active Measures*.

27. *Misinformation* can be defined as the spreading of unintentionally false information. Examples include Internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. Unlike misinformation, disinformation is intentionally false. Examples include planting false news stories in the media and tampering with private or classified communications before their widespread release. Congressional Research Service, “Defense Primer: Information Operations,” In Focus, IF10771, January 14, 2020, <https://crsreports.congress.gov/>.

28. Will Knight, “AI Is Rewiring Coders’ Brains. Yours May Be Next,” *Wired*, February 8, 2024, <https://www.wired.com/>.

29. Benedict Evans, newsletter no. 528, Tuesday, February 20, 2024, <https://www.ben-evans.com/>, list@ben-evans.com.

30. No universally accepted definition exists. In a good report by scholar Tim Hwang, “Deepfakes: A Grounded Threat Assessment” (Center for Security and Emerging Technology, 2020), <https://cset.georgetown.edu/>, he notes that in his paper,

the term “deepfakes” refers to the broad scope of synthetic images, video, and audio generated through recent breakthroughs in the field of ML [machine learning, a form of AI], specifically in deep learning. This term is inclusive of ML techniques that seek to modify some aspect of an existing piece of media, or to generate entirely new content. While this paper emphasizes advances in neural networks, its analysis is relevant for other

methods in the broader field of ML. The term “deepfakes” excludes the wide range of techniques for manipulating media without the use of ML, including many existing tools for “cutting and pasting” objects from one image to another.

31. Steven J. Zipperstein, “The Conspiracy Theory to Rule Them All,” *The Atlantic*, August 25, 2020, <https://www.theatlantic.com/>.

32. Nicholas D. Wright, “From Control to Influence: Cognition in the Grey Zone,” ver. 3, Institute for Conflict, Cooperation and Security Report for the US DOD Joint Staff (Intelligent Biology, January 2019), <https://www.intelligentbiology.co.uk/>.

33. P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018).

34. Jon Bateman, “Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios” (Carnegie Endowment for International Peace, July 2020), <https://carnegieendowment.org/>.

35. Rid, *Active Measures*.

36. Hwang, “Deepfakes.”

37. “Many AI Researchers Think Fakes Will Become Undetectable,” *The Economist*, January 17, 2024, <https://www.economist.com/>; and Madeleine Daepf and Robert Osazuwa Ness, “Video Will Kill the Truth if Monitoring Doesn’t Improve, Argue Two Researchers,” *The Economist*, March 26, 2024, <https://www.economist.com/>.

38. Hwang, “Deepfakes.”

39. Nicholas Confessore et al., “The Follower Factory,” *The New York Times*, January 27, 2018, sec. Technology, <https://www.nytimes.com/>.

40. Samantha Bradshaw and Philip N. Howard, “The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation,” Working Paper 2019.2 (Project on Computational Propaganda, 2019), <https://digitalcommons.unl.edu/>.

41. Samuel Woolley, “We’re Fighting Fake News AI Bots by Using More AI. That’s a Mistake,” *MIT Technology Review*, January 8, 2020, <https://www.technologyreview.com/>.

42. Andreas Vogel and Nicholas D. Wright, “Alexa Is Both Friend and Sales Robot. That’s a Problem,” *Slate Magazine*, May 10, 2019, <https://slate.com/>.

43. Information Commissioner’s Office (ICO), “Microtargeting,” accessed May 8, 2019, <https://ico.org.uk/>; and Nitasha Tiku, “Get Ready for the Next Big Privacy Backlash Against Facebook,” *Wired*, May 21, 2017, <https://www.wired.com/>.

44. John Naughton, “The Goal Is to Automate Us: Welcome to the Age of Surveillance Capitalism,” *The Observer*, January 20, 2019, sec. Technology, <https://www.theguardian.com/>.

45. David M. Kent et al., “Personalized Evidence Based Medicine: Predictive Approaches to Heterogeneous Treatment Effects,” *BMJ [British Medical Journal]* 363 (December 10, 2018): k4245, <https://doi.org/10.1136/bmj.k4245>.

46. Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press, 2020).

47. Hendrik Laubscher, “Tmall 2.0 Goes Big on Customization,” *Forbes*, July 11, 2019, <https://www.forbes.com/>.

48. Rid, *Active Measures*.

49. For two good reports specifically on deepfakes rather than the broader range of challenges addressed here, see Bateman, “Deepfakes and Synthetic Media”; and Hwang, “Deepfakes.”

50. To protect copyrighted content on YouTube, Google has since 2007 applied a system (later called Content ID) that compares uploaded videos to audio and video files registered by content owners. By 2018 it claimed to have invested \$100 million in Content ID and paid over \$3 billion to rights holders. Paul Sawers, “YouTube:

We've Invested \$100 Million in Content ID and Paid over \$3 Billion to Rightsholders," VentureBeat (blog), November 7, 2018, <https://venturebeat.com/>. Other companies have similar systems; see Josh Constine, "Pex Buys Dubset to Build YouTube ContentID for TikTok & More," TechCrunch (blog), March 5, 2020, <https://social.techcrunch.com/>. While far from perfect in enforcement, children have various protections online in the US. Michael H. Keller and Gabriel J. X. Dance, "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?," *The New York Times*, September 28, 2019, sec. U.S., <https://www.nytimes.com/>.

51. Francis Fukuyama et al., "How to Save Democracy From Technology: Ending Big Tech's Information Monopoly," *Foreign Affairs*, January/February 2021, <https://www.foreignaffairs.com/>.

52. Personal communication with author. See NewsGuard at <https://www.newsguardtech.com/>.

53. Rani Molla, "It Will Take More than NewsGuard's Team of Journalists to Stop the Spread of Fake News," Vox, February 13, 2019, <https://www.vox.com/>.

54. For an accessible recent review of available techniques, see Alice Huguet et al., *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay* (RAND Corporation, 2019), <https://www.rand.org/>. Simple options could be chosen, appropriate for the various audiences within the joint force and its support networks.

55. This statement draws on evidence for the power of "norms" to drive behavioural and cultural change. For a review of this evidence, see Wright, "From Control to Influence."

56. For example, see US Army, "Social Media Guide," accessed June 2024, <https://www.army.mil/>.

57. A recent example was a TikTok video by two deployed Michigan Army National Guard Soldiers. Davis Winkie, "Deployed Soldiers Face Punishment for Their 'Message to Liberals' Video," *Army Times*, October 16, 2020, <https://www.armytimes.com/>.

58. For a recent review of some examples, see Jon Bateman and Dean Jackson, "Countering Disinformation Effectively: An Evidence-Based Policy Guide" (Carnegie Endowment for International Peace, January 31, 2024), <https://carnegieendowment.org/>.

59. Huguet et al., "Exploring Media Literacy Education."

60. Wright, "Artificial Intelligence and Democratic Norms."

61. David Perera, "Lawsuit Seeks Relief from Cyberspying – CIA and OPM: Rethinking the Silo," Politico, July 14, 2015, <https://www.politico.com/>; and David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Penguin Random House, 2018).

62. Public sector examples include the Flagship World Bank reports World Bank, *World Development Report 2016: Digital Dividends* (The World Bank Group, 2016), <https://www.worldbank.org/>; and World Bank, *World Development Report 2021: Data for Better Lives* (The World Bank Group, 2021), <https://www.worldbank.org/>. For the private sector, see Edd Wilder-James, "Breaking Down Data Silos," *Harvard Business Review*, December 5, 2016, <https://hbr.org/>.

63. Nicholas D. Wright, "Coronavirus and the Future of Surveillance: Democracies Must Offer an Alternative to Authoritarian Solutions," *Foreign Affairs*, April 6, 2020, <https://www.foreignaffairs.com/>.

64. One framework produced for SMA is Wright, "From Control to Influence." It provides detailed, evidence-based influence, with chaps. 2–4 addressing the audience, message, and messenger, respectively.

65. For a local newspaper analogy, see, for example, Bateman and Jackson, "Countering Disinformation Effectively."

66. For example, the former head of the UK's GCHQ (Government Communications Headquarters) proposed six ethical guidelines for security and intelligence agencies,

which were designed for all intelligence activity. David Omand, “Ethical Guidelines in Using Secret Intelligence for Public Security,” *Cambridge Review of International Affairs* 19, no. 4 (December 2006): 613–28, <https://doi.org/10.1080/09557570601003338>. I adapted these to the specific case of influence in Wright, “Cognitive Defense.”

Part 6

**CONCLUSIONS FROM HUMANS—AND
CONCLUSIONS FROM MACHINES**

Chapter 16

Conclusions Written by Three Humans

Nicholas Wright, Georgetown University, University College
London, Center for Strategic and International Studies

Michael Miklaucic, National Defense University

Todd Veazie, Joint Staff, Operations Directorate

Abstract

The three human editors consider what success looks like in the Mind-Tech Nexus, for which we present six conclusions from this volume: (1) Set high and realistic ethical standards; (2) maintain balance by accounting for the bias toward technological solutions that don't adequately address how technology works with humans; (3) take the interface between humans and technology seriously; (4) build iterative and agile processes to promote Mind-Tech advances as they emerge because the most effective forms may be "unprestatable"; (5) anticipate and prepare for vulnerabilities; and finally, (6) consider both the Mind-Tech capabilities that change the character of war, as well as the fundamentally human nature of war in which the will to fight can be decisive.

This chapter brings together the different strands of the book—as seen by its three human editors—to chart possible future trajectories for the United States and its allies in leveraging the Mind-Tech Nexus (fig. 16.1). That nexus of human factors and technology shapes the character and outcomes of competition. But perhaps first we should ask a central question that we believe technology will be unable to answer for some time yet, because this important question rests on human goals and requires an understanding of context: How do the United States and its allies devise a theory of success for managing the Mind-Tech Nexus?

We suggest that successful *mastery of the Mind-Tech Nexus means leading innovation at the interface and convergence of human factors and technology—to assure our friends and enable us to outcompete,*

deter, and defeat rivals within the ethical constraints of a free and democratic society.

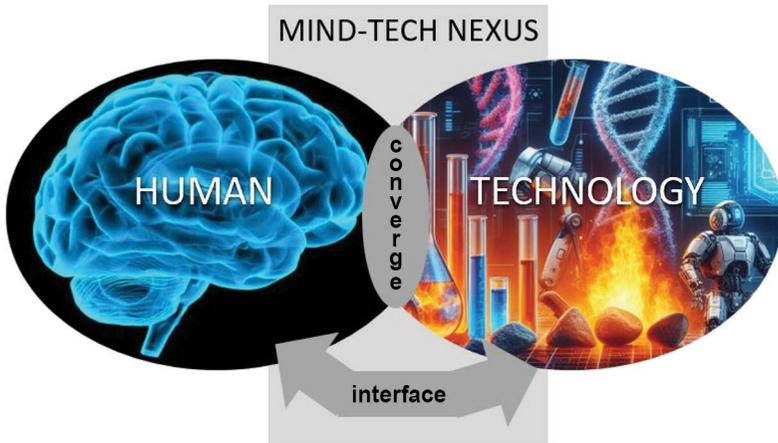


Figure 16.1. The Mind-Tech Nexus is how human factors and technology will interface and converge to shape the character and outcomes of competition.

Even the scholarly and practical expertise of this volume’s authors cannot hope to provide comprehensive prescriptions for achieving this goal or the many other challenges raised by the Mind-Tech Nexus. Instead, we hope this book will open apertures and help frame better questions. In this chapter, we provide six provisional conclusions, along with their associated implications.

Conclusion 1: Ethics

Advances in the Mind-Tech Nexus raise profound ethical challenges, some previously unknown, and to meet them, we must lead the establishment of a new international security regime to set guiding principles, political structures, and high ethical standards and hold ourselves to them; anticipate how these standards may apply or change in war; and appreciate that adversaries may not operate within or share our ethical parameters.

To give one example of a new challenge, AI technologies make some age-old human ethical decisions explicit in ways previously unknown. Once machines make judgments, they can be programmed with explicit numbers that, for example, guide how acceptable certain types of casualties are. We see an analog with self-driving cars that

can be programmed in the case of accidents to make decisions that at the extreme care only about (a) the potential death of the car's occupants, or (b) the deaths of those inside or outside the car so they could sacrifice the car's occupants to save other road users. One study asked respondents to make such judgments and found that they wanted other people to drive cars that sacrifice their passengers for the greater good, but the respondents would themselves prefer to ride in autonomous vehicles that protect their passengers at all costs.¹

Who gets to choose the setting to be applied for warfighters controlling swarms of AI-enabled drones in hostile environments or how to balance the lives of troops and civilians? Related decisions have been made in the past, but now they will be explicit and recorded in detail. What *is* our risk tolerance? What *ought* to be our risk tolerance?

We must also anticipate that our ethical considerations may evolve during war—and do so in predictable ways. In the 1920s and 1930s, Americans were broadly against unrestricted submarine warfare. But just four hours after the Pearl Harbor attack, all US Navy ship and submarine commanders received the order “EXECUTE AGAINST JAPAN UNRESTRICTED AIR AND SUBMARINE WARFARE.”² The 1920s and 1930s saw Britain and America firmly against the strategic bombing of cities, but that judgment eventually changed with respect to Germany and Japan. This type of situation does not mean anything goes—throughout World War Two, the democracies held themselves to higher standards and must do so again—but it does mean that we should anticipate that our ethical judgments may evolve so we can prepare required capabilities when we might need them.

Finally, we must appreciate that our ethical parameters are not the same as those of our adversaries. In the development of Mind-Tech advances, for example, Chinese labs have very different rules on issues such as inserting human genes into monkey brains—which led macaques to perform better on short-term memory tasks and to develop more similarly to how human brains develop over a longer period.³ Russia has shown its casual disregard for civilian casualties and civic destruction in Chechnya, Georgia, Syria, and Ukraine. Effective warfighting in the twenty-first century will require a reconsideration of our self-imposed moral and ethical limits if we are to compete successfully and perhaps also require some degree of moral/ethical compromise.

Conclusion 2: Balance—Avoiding Twenty-First-Century Maginot Lines

More than for any other country, advanced technology has been central to the American way of war at least since World War Two⁴—but technology alone is insufficient to win wars, and policy should actively correct for the bias against adequately addressing how technology works with humans.

This factor does not mean technological excellence isn't vital, but military effectiveness is at least as much about factors like raw human courage. There should be a balance to help get the most out of the humans *and* the technology. As David Omand's chapter described for intelligence during the Cold War, for example, there was a huge overspend on fancy satellites at the expense of the minds that had to interpret and understand the data they produced.

What can be done to better achieve an optimal balance?

Partly, an awareness of such bias is one vital step to correcting for it.⁵ We should recognize there is a bias toward focusing too exclusively on technology. For example, when senior leaders discussed Joint All-Domain Command and Control (JADC2), far too much focus was on the technology in isolation and far too little on how the humans who would have to use JADC2 might interface and converge with the technology. Senior leaders and staffs should ask this general question: Are we taking a balanced enough approach?

Another approach applies the old adage that “what gets measured gets done.” Jack Shanahan, founding leader of the Joint AI Center, discusses in his chapter the creation of new metrics for developing new technologies that capture not just the readiness of the technology but also how ready the technology is to operate with humans. Technology Readiness Levels (TRL) are a well-known type of measurement system to assess the maturity level of a particular technology.⁶ It goes from TRL-1 in which scientific research is beginning to TRL-9 that is “flight proven.” Alongside the TRL, a Human Readiness Level (HRL) from HRL-1 to HRL-9 can similarly provide a simple number that indicates the state of integration within the system with respect to humans and technology.⁷ It can go from HRL-1, involving basic research on human characteristics and performance to HRL-9, in which the system is successfully used in operations across the operational envelope with systematic monitoring of human-system performance.

A further way to achieve better balance is to identify which stages in a process—such as the “OODA” loop—particularly favor humans, technology, or a blend of the two. Tim Grayson’s chapter demonstrates doing so at the tactical, operational, and strategic levels. Where humans and tech must work together closely—e.g., “Orient” and “Decide” in the OODA loop—those stages can be a particular focus for efforts to improve how humans and tech interface and converge.

Conclusion 3: Take Interfaces Seriously

Technologies and humans interface. The interface is where these separate systems interact. However, although interfaces can be a source of significant competitive advantage (if done well) or disadvantage (if done poorly), they are often largely ignored except as an add-on to the technology late in the development process.

As Jack Shanahan describes, user interfaces and experience (UI/UX) are seen as central to success in much of the commercial world—but not in defense. It was the interface between the tech and the human that made the iPhone so much more successful than the Microsoft smartphones it left in the dust. Military fascination with technology tends to occlude the critical interface between tech and human. Mesmerized by the latest and greatest tech, planners may miss opportunities to use less advanced technologies that interface more effectively with humans for greater strategic impact.

Interfaces should be a focus from the early stage of equipment and concepts, such as JADC2, not added on at the end. Considering interfaces at the front of development can be accomplished in many ways. For example, sandboxes can be used throughout development to bring together operators, technologists, and experts in human-machine interfaces, reinforcing a culture of “human-centered design.”⁸ The military could promote interfaces as an important field of study and excellence, as it is in many shops in Silicon Valley, and that field could work at many different levels: individual warfighters, teams, large platforms (like missile defense), JADC2, and commanders’ aids. Given that many leading advances in Mind-Tech are now developed first commercially, the US military and its allies could explicitly seek out the latest techniques and capabilities for interfaces from the commercial world—for example, involving GenAI.

Conclusion 4: Convergence and the “Unprestable”

Humans and technology converge through an often iterative process of development to create interdependent entities that have military effectiveness—like a soldier with a well-balanced sword, a “human-horse team,” or a crew in their tank or ship. Because we often cannot predict precisely how new technologies will best create military effectiveness, we should build agile processes to promote Mind-Tech advances as they emerge.

Early twentieth-century technologies like the airplane and tank were almost certain to be important on the battlefield, but precisely how? The machines and the ways of using them changed radically over decades. During our discussions about the Mind-Tech Nexus with experts on military innovation, some argue passionately for “bottom-up” innovation from a hubbub of ideas, while others argue equally passionately for “top-down” visionary leadership. We suggest both are needed: Agility to best use Mind-Tech advances in our era will require bottom-up appraisals of what is possible *and* top-down visions of where one might wish to go.

For the bottom-up approach, a useful concept is the “adjacent possible” introduced in the 1990s by scholar Stuart Kauffman.⁹ The adjacent possible can be described as the imaginative exploration of what is feasible next given what exists now, or it can be defined as the set of possibilities available to individuals, communities, institutions, organisms, productive processes, and so forth at a given point in time during their evolution. This view provides structured ways to think through complex problems, and strategic multilayer assessment (SMA) has recently applied it to complex, dynamic challenges such as escalation management in twenty-first-century information operations.¹⁰ It allows observers to consider how different factors may converge to become more than the sum of the parts (e.g., as combined air and land operations converged in blitzkrieg). It also introduces a healthy humility about what can be predicted because we cannot pre-state what the combination of existing factors may produce. The “unprestable” axiom will be a source of US surprise, threat, and opportunity—and US specialized and integrative systems and their human teammates must be resilient and agile enough to identify antecedent patterns of convergence and take advantage.

In the bottom-up approach to innovation, sandboxes, red teaming, and other techniques can also be vital. As David Omand’s chapter suggests, this approach can help us see crucial second- and third-order

effects. And as Andrew Gainer et al.'s chapter describes for command and control, this bottom-up learning becomes pivotal as we face competition in increasingly complex environments. Ben Connable describes the failure of a half-billion dollar investment in “mixed reality” headsets intended to improve Soldiers’ lethality but actually decreased their military effectiveness. This example reinforces the point that we cannot have lopsided development of Mind-Tech advances, which focus too exclusively on the tech side and only bring in the human factors late in the development process.

We must also focus on top-down vision, on the imagination of pioneers who can see further. As Michael Groen, another former head of the Joint AI Center, describes in chapter 6, we need to *reimagine* entire processes and not only tinker incrementally with processes that already exist. To be sure, we humans often first make a tool to fit the work—the tank as cavalry—but then we can also change the work to fit the tool.

Only with top-down plus bottom-up approaches can we seize opportunities from Mind-Tech advances and defend against vulnerabilities.

Conclusion 5: Vulnerabilities

Every new technology, every new Mind-Tech advance may bring brilliant new strengths—but it will also bring new vulnerabilities that adversaries can exploit (and that we can exploit), for which we must anticipate.

Pioneers of German blitzkrieg in World War Two used speed of communication to provide a huge edge in May 1940 to defeat democratic France catastrophically. But British code breakers went on to decipher the German codes, giving the Allies a very real edge in World War Two. American code breakers did the same against the Japanese, which was vital to winning the Battle of Midway. In our era, as Josh Baughman’s chapter describes, the Chinese are focused on *system survival*, which could provide them with a vital edge if we do not look equally at our own vulnerabilities.

Some vulnerabilities will be more obvious, such as from code breaking in our increasingly networked digital age. Others will be less obvious—such as the dangers of newly possible micromanagement by commanders (or even the White House Situation Room) when “mission command” emphasizing centralized command and decentralized control might be far more effective. And others will require new balances that we have yet to understand. As Nick Wright describes in chapter 8,

brain-computer interfaces (BCI) from companies like Neuralink or Synchron are being implanted in human brains to restore lost function. However, if BCIs are implanted in the brains of healthy warriors to enhance the ability to command machines, what new vulnerabilities will be introduced on or through them for electronic warfare (EW), hacking, or other attacks? Moreover, as so much tech in our era is now “dual use”—originally built for commercial purposes but adapted to military applications—defense against vulnerabilities or weaponized proliferation may not have been an integral design consideration.

We must also recognize that the potential to use Mind-Tech advances to enhance warfighter performance is matched by the potential to use Mind-Tech advances to suppress adversary performance. The US and its allies and partners must—within ethical constraints—be willing to leverage technology that disables or suppresses adversary warfighting performance.

Conclusion 6: Adversaries with the Will to Fight

*We are dangerously ignorant of our adversaries’ advanced and emerging Mind-Tech capabilities for warfighting that may change the **character** of war. But in addition to better anticipating the changing character of future war, as its **nature** will remain fundamentally human, we must ensure that the United States and its partners give as much thought to the will to fight as to any technologies used.*

There is a risk of being unpleasantly surprised on the battlefield by unanticipated enemy application of human-machine warfighting abilities. Many seemingly powerful militaries have experienced defeat when they failed to anticipate the changing character of conflict. The United States and its partners must remain agile and proactive in their use of new technologies and how those new technologies interface and converge with the humans who use them.

We must sharpen our focus on the Mind-Tech Nexus, including the cutting-edge technologies that can revolutionize warfare (such as machine guns, tanks, barbed wire, or nuclear weapons), while *also* appreciating the intrinsically human nature of war that is so often decisive and exemplified by the will to fight. How technologies interface and converge with humans can always provide an edge in war. Which side, in our era, will most benefit?

Endings and Beginnings

This chapter would normally provide a natural end point in the narrative arc of this book—and hopefully we do achieve that aim—but here we also open the door for a new beginning. Many future books will not be static objects, but through GenAI and other technologies they will become more dynamic objects. We don't know precisely how that will happen. But to sketch out one beginning we introduce Dave Vernal, a retired USAF colonel in intelligence who has spent time at Stanford University to learn about GenAI. In chapter 17 he provides a brief introduction, and in chapter 18 we will see what GenAI gets from this book and what products it can make for national security practitioners.

Notes

1. Jean-François Bonnefon et al., “The Social Dilemma of Autonomous Vehicles,” *Science* 352, no. 6293 (2016): 1573–76, <https://doi.org/10.1126/science.aaf2654>.
2. Paul Scharre, *Army of None – Autonomous Weapons and the Future of War* (W. W. Norton & Company, 2018), 101.
3. See, for example, Jean-François Monier, “Chinese Scientists Insert Human Brain Gene into Monkeys, Spark Ethical Debate,” April 25, 2019, *NBC News*, <https://www.nbcnews.com/>; and Sigal Samuel, “Scientists Added Human Brain Genes to Monkeys. Yes, It’s as Scary as It Sounds,” *Vox*, April 12, 2019, <https://www.vox.com/>.
4. Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (Columbia University Press, 2010).
5. For a discussion of how improving our self-awareness and “thinking about thinking” can help correct biases, see, for example, Nicholas D. Wright, “Why Are We Integrating Now—and How Can We Integrate Better? History, Complexity and Metacognition,” Report for the Strategic Multilayer Assessment Office (Intelligent Biology, 2022), <https://nsiteam.com/>.
6. Catherine G. Manning, “Technology Readiness Levels,” NASA, September 27, 2023, <https://www.nasa.gov/>.
7. George Salazar et al., “Understanding Human Readiness Levels,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 64, no. 1 (June 1, 2020): 1765–69, <https://doi.org/10.1177/1071181320641427>.
8. See, for example, “Seven Tenets of Human-Centred Design,” Design Council, accessed January 2025, <https://www.designcouncil.org.uk/>; and Lauren Landry, “What Is Human-Centered Design,” *Harvard Business Review Online*, December 15, 2020, <https://online.hbs.edu/>.
9. Introduced in Stuart A. Kauffman, “Investigations: The Nature of Autonomous Agents and the Worlds They Mutually Create,” vol. 96, issues 8–72 of Santa Fe Institute working papers (Santa Fe Institute, 1996); and Stuart A. Kauffman, *Investigations* (Oxford University Press, 2000). See the references below for more accessible and applied descriptions.
10. For recent application of SMA to national security, see Lawrence A. Kuznar and COL (ret.) Carl W. Hunt, “Escalation Management in 21st Century Operations in the Information Environment” (Strategic Multilayer Assessment, June 2021), <https://nsiteam.com/>.

.com/. See also Carl W. Hunt et al., *Paradoxes of Power: A Collection of Essays on Failed Leadership—and How to Fix It* (Independently published, 2020). The definition is from Lennart Björneborn, “Adjacent Possible,” in *The Palgrave Encyclopedia of the Possible* (Springer International Publishing, 2020), 1–12, https://doi.org/10.1007/978-3-319-98390-5_100-1.

Chapter 17

A New Beginning with Generative AI

David Vernal

Gordian Knot Center for National Security Innovation,

Stanford University

Colonel, United States Air Force, Retired

Humans have long used technology in their decision-making, and an unexpected technological revolution in cognitive affairs may already be upon us.

Straddling the line between biology and technology, human language is so ubiquitous and transparent that it's easy to overlook how foundational to human cognition it is, and how miraculous its powers. When we verbalize language, we communicate information from one mind to another. When we concretize it in written form, we can communicate across time and space. That you can relate with an ancient Sumerian customer's complaint to his copper merchant, captured in cuneiform thousands of years ago, is a technological marvel, but no more so than reading and comprehending this book or this sentence.¹

Literacy itself already creates a biological Mind-Tech Nexus, affecting the left ventral occipitotemporal region, improving verbal memory, and thickening the connection between hemispheres.² If you are literate in English, *you cannot help but read and understand these words you see*—the interface becomes involuntary. Orality in preliterate cultures created shared culture and group cooperation, and writing has allowed for knowledge accumulation and transmission to enable large-scale and intercultural transmission no other species can boast.

Like all large-scale group activities, military actions rely on language and literacy to ensure command, control, and alignment. Doctrine, strategies, orders, message traffic, CONOPS, commander's intent, emails, intelligence reports, tactical system messages, and even heads-up displays and an aircraft's spoken audio warning systems all rely on language to direct cognition and change actions.

Large Language Models

The rise of generative artificial intelligence, specifically large language models (LLM), forces us to confront again this power of language. Bursting out of research labs into popular consciousness in 2022, LLMs have captured the public imagination and a tsunami of investment.³ Unlike prior machine-learning algorithms specialized for one task, LLMs appear to be a general purpose technology, useful for multiple tasks, and even more so when paired with other tools.⁴ LLMs or something like them will potentially seep into nearly any computing task that touches language.

Under their hood, LLMs like OpenAI's ChatGPT and Anthropic's Claude—the two LLMs we use to produce the next chapter—are an evolution of natural language processing (NLP) techniques to establish the statistical relationships among words, their meanings, and their syntax. These embeddings, or numerical vectors, are the building blocks of a mathematics of words that captures information about their definitions and contexts so that, in a famous example, “king” minus “man” plus “woman” equals “queen.”⁵

What changed over the last few years was the invention of the transformer algorithm (the “T” in GPT) that allows for massive parallel processing of words (or even smaller snippets of words, both collectively called “tokens”) in vast corpora of written data, at enormous scales determining more of these inter-token relationships than earlier architectures. Through manipulation of these vectors, the models predict what is likely the next token in a sequence, creating meaning by plucking the strands in the web of embeddings to predict which note resonates best next, and next, and next.

With billions of relationships mapped from the incredibly large datasets, and with fine-tuning based on many iterations of human feedback, researchers have progressed from simple and stilted sentence completion to the extraordinarily fluid and nuanced responses of ChatGPT or its competitors.

Precisely because language is embedded directly or indirectly in nearly all human endeavors, LLMs have unleashed widespread imagination about their application for knowledge work. While many national security tasks fit comfortably in this category, the initial establishment reaction to LLMs varied between vague worries of supercharged disinformation or hacking at scale to dismissal of the technology as prone to “hallucinations”—the confident prediction of factually incorrect infor-

mation—and therefore inherent unsuitability for vital, high-consequence government work.⁶

But LLMs are not (just) answer bots like a Google search bar. What if the new killer app is not to find an existing answer somewhere in the training data but for humans to partner with the computer to create it? Precisely because we are so steeped in keyword searches (or if our work roles are better served by quantitative analysis, then in more sophisticated data-driven approaches), we may not have models for the creative exploration of novel solutions with computers. The nearest analogs may be deep introspection and rigorous interrogation of our reasoning in conversation with a trusted confidant, or systematic and laborious scientific inquiry that changes our mental models and therefore our cognition. Interestingly, we may have at long last come back to the aspirations of Douglas Englebart and other computer pioneers who saw computing's potential in “augmenting human intellect, [by which] we mean increasing the capability of . . . [an individual] to approach a complex problem situation, to gain comprehension to suit . . . [their] particular needs, and to derive solutions to problems.”⁷

Beyond language, transformers seem able to ferret out underlying relationships between tokens derived from large enough datasets for any phenomenon with nonrandom connections. The vocabularies of climate and weather, chemistry, and biology are likely amenable to tokenization, building on similar machine-learning advances in the sciences, such as the AlphaFold protein folding tool.⁸ Even if it is not the transformer algorithm and LLMs that prove the most reliable or efficient at every task, LLMs have lit a spark fueling the imaginations of millions worldwide to apply AI to solve their own problems. Because the technology has spawned code-writing copilots and, more ambitiously, AI software engineers, the rate of change may be staggering.

National Security Applications

Based on the trends since the introduction of ChatGPT, I offer the following observations or predictions.

The current computing interface will change. We're already seeing the power of plain language to become new software code, increasing computers' functionality; first, by the power of millions of new coders and, eventually, perhaps by a gradual breaking down of software as a discrete object we interact with on the device. Think beyond text-based

chat interfaces, and imagine graphical user interfaces that morph to display what's most relevant and useful in an ongoing human-machine dialogue, conducted in plain language.

Relatedly, parallel NLP improvements in understanding and generating human speech mean that transcription will be ubiquitous and possibly the default tool for structured conversations like meetings or briefings. AI distilling the important takeaways from conversations or meetings will be the norm. In written text and spoken speech, translation across languages will be, if not seamless, then exponentially easier. New generative AI tools have already debuted to re-render a speaker's audio and video fluently in foreign languages, in their own voice.⁹

In the military context, information delivery will likewise change. Imagine plain language queries of operational databases and recompilation of analysis on the fly ("only show me formations of greater than fifty combatants" . . . "no, make it twenty" . . . "now zoom in there") or intelligence updates generated as podcasts for a future POTUS to absorb during a daily treadmill run. Static text may become as quaint as faxes, as interactive reports allow readers to go as deep as they want on the subject matter, tailored and remixed to match an individual's learning style and work role. Likewise, imagine personalized instruction delivered at the appropriate knowledge level or tailored briefings delivered for audiences segmented by, say, security clearance and nationality.

There will absolutely be challenges! It's unclear how much true reasoning occurs in next-token prediction, and models are limited in "knowledge" to the materials ingested during training. However, academia and industry have already created LLM-powered tools to allow models to retrieve and process outside data from the internet or a private dataset, use tools like traditional software, and constrain answers to reduce hallucination. In the longer term, new forms of deceptions like deepfakes and advanced social engineering as well as the disruption of knowledge work may have substantial impacts on societies and economies. Even at the biological level, ubiquitous AI may affect how we use our own brains; Plato complained that writing was destroying the younger generation's memory, and since the introduction of cell phones, how many phone numbers do you remember? Will our cognitive skills decline as we offload more processing to our intelligent devices?

Perhaps by the time this book reaches publication or shortly thereafter, LLM technologies will have decisively hit a wall, and another cyclic "AI winter" will have settled in. Given the recent trajectory of advancement and investment, I find it more persuasive that we stand

on the precipice of a new age with unclear consequences for the economy, society, international relations, the balance of power, and human flourishing. We come full circle to the Mind-Tech Nexus.

With the above in mind, we would like to share the results of experimentation with processing the text and themes of this volume through available LLMs. We entered individual chapters and the full text of this volume¹⁰ into OpenAI's GPT4 and Anthropic's Claude Opus, their most advanced models publicly available at the time of writing. We asked each LLM to perform actions using commands called "prompts" or, simply put, the plain-language instructions we would like the model to follow. Prompting can be as simple as "tell me a joke" or a lengthy, complicated instruction specifying a tone, a rationale, a desired end goal, an example of the desired result, and even strangely effective exhortations like "I know you can do it!"

In the next chapter, we iterated prompts and answers to yield interesting results for our readers, but the final prompts and answers are reproduced verbatim, unless otherwise noted.

Notes

1. "Complaint letter from Nanni to Ea-Nasir," clay tablet, Mesopotamia, 1750 BCE, British Museum, museum no. 131236, <https://www.britishmuseum.org/>.
2. Joseph Henrich, *The WEIRDest People in the World: How the West Became Psychologically Peculiar and Particularly Prosperous* (Farrar, Straus and Giroux, 2020), 3.
3. Global private investment in generative AI increased from about \$3 billion in 2022 to \$25 billion in 2023. Nestor Maslej, "Inside the New AI Index: Expensive New Models, Targeted Investments, and More," Stanford Institute for Human-Centered Artificial Intelligence (HAI), April 15, 2024, <https://hai.stanford.edu/>.
4. Tyna Eloundou et al., "GPTs Are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models," arXiv (preprint), posted March 17, 2023, <https://arxiv.org/abs/2303.10130>.
5. "King – Man + Woman = Queen: The Marvelous Mathematics of Computational Linguistics," *MIT Technology Review*, September 17, 2015, <https://www.technologyreview.com/>.
6. Sydney J. Freedberg Jr., "Pentagon Should Experiment with AIs Like ChatGPT — But Don't Trust Them Yet: DoD's Ex-AI Chiefs," *Breaking Defense*, April 6, 2023, <https://breakingdefense.com/>.
7. Douglas C. Engelbart, "Augmenting Human Intellect: A Conceptual Framework," SRI Summary Report AFOSR-3223 (Stanford Research Institute, October 1962), <https://www.dougenelbart.org/>.
8. "AlphaFold," DeepMind, <https://deepmind.google/>.
9. Jose Antonio Lanz, "AI Startup Can Now Generate Speech Using Your Voice in 30 Languages," *Decrypt*, August 23, 2023, <https://decrypt.co/>.
10. We did not include part 6, "Conclusions," to avoid leading the GenAI down any particular route. For practical reasons, we did not include the foreword by Sir Lawrence Freedman or chapter 8 on performance enhancement by Nicholas Wright.

Chapter 18

Conclusions Written by Generative AI

Generative AI Prompted and Annotated by David Vernal

Gordian Knot Center for National Security Innovation,
Stanford University; Colonel, United States Air Force, Retired

The following text documents the prompts that the author gave to the large language models (LLM) GPT4 and Claude 3 Opus and the responses they generated. These generative AI systems were the most advanced models publicly available at the time of writing, but in the last year, many more advanced models are now part of the conversation. The outputs demonstrate LLM capabilities and are presented as artifacts for examination, not as authoritative statements. Any errors or inconsistencies readers may discern should be viewed as informative indicators of these systems' limitations, inviting the readers to consider LLMs' strengths and boundaries.

Analyze the book's chapters and summarize the book's themes and findings in one hundred words.

(GPT4)

The book "Human, Machine, War: How the Mind-Tech Nexus will Win Future Wars" explores the interplay between human cognition and technological advancements, particularly in military contexts. It is divided into six parts, addressing various facets of the relationship between mind and technology.

****Themes of the Book:****

1. ****Integration of Human and AI****: The book discusses the potential and challenges of integrating artificial intelligence with human cognitive capabilities to enhance decision-making and operational efficiency in military strategies.
2. ****Ethical and Practical Challenges****: It delves into the ethical implications and practical challenges of neurotechnology and AI in warfare, including the issues of autonomy, control, and the impact on the human operators.

3. **Adaptation and Innovation**: The role of technological innovation in adapting to modern warfare is analyzed, considering both the potential enhancements and the risks of dependency on advanced technologies.
4. **Comparative International Perspectives**: It provides insights into how different countries, particularly China and Russia, are incorporating technology with military strategy, emphasizing the competitive edge in global military power dynamics.
5. **Future of Warfare**: The book speculates on the future trajectory of warfare and defense strategies influenced by rapidly evolving technologies and the shifting landscape of global power.

Findings of the Book:

The book underscores that the effective use of technology in military contexts does not simply replace human judgment but rather complements and extends human capabilities. It highlights the necessity of maintaining a balance between technological reliance and human decision-making prowess to navigate the complexities of modern warfare. Ethical considerations are stressed as paramount, especially as the boundaries of technology and its capabilities continue to expand. The comparison between nations illustrates differing approaches and priorities in technology integration, pointing to a broader strategic landscape shaped by these developments.

In essence, the book advocates for a nuanced understanding of the “Mind-Tech Nexus,” arguing that future success in warfare will depend on how well technology and human cognitive abilities are integrated, managed, and ethically aligned.

That’s an excellent summary, but you disregarded the length limitation. Try again.

The book “Human, Machine, War” explores the integration of human cognition and technology in military contexts, particularly focusing on artificial intelligence (AI) and neurotechnology. It discusses the ethical implications and practical challenges of these technologies in warfare, emphasizing the necessity to balance technological reliance with human decision-making. The book highlights various national approaches, especially from the US, China, and Russia, illustrating competitive strategies in global military dynamics. Ultimately, it advocates for a

nuanced understanding of the “Mind-Tech Nexus,” stressing that future success in warfare hinges on effectively blending technology with human cognitive capabilities while maintaining ethical integrity.

Act as a defense industry analyst. Generate a detailed summary of each chapter. Note author, title, thesis, and main themes and conclusions. Call out any specific reference to generative AI or LLMs. Identify any specific follow-on action or recommendation the author makes to the Department of Defense. For each chapter, suggest three follow-on questions for the author.

(Claude 3 Opus)

Chapter 1: Lauren Kahn, “Artificial Intelligence: A Strategic Augmenter, Not a Replacement” [original chapter 1 title]

Thesis: AI should be viewed as a strategic augmenter of human capabilities in military operations, not as a replacement. The successful integration of AI applications depends on effective human-machine interaction.

Main themes and conclusions:

1. AI enhances military operations by providing more information, faster decision-making, and improved situational awareness.
2. The human element is crucial in AI’s successful deployment, as AI remains a tool to be wielded by human operators.
3. Understanding and optimizing the human-AI relationship is essential for realizing AI’s full potential and avoiding adverse outcomes like automation bias.

Reference to generative AI or LLMs: None specifically mentioned.

Recommendations to the Department of Defense: None explicitly stated.

Follow-on questions:

1. What specific policies and training programs should the DOD implement to ensure the success of human-machine teams?
2. How can the DOD address challenges like automation bias in the development and deployment of AI systems?

3. What metrics should the DOD use to evaluate the effectiveness of human-AI collaboration in military contexts?

Chapter 2: James Giordano, “Accessing the Brain to Affect the Mind: Neuroethics of the Mind-Tech Nexus in Military Contexts”

Thesis: Developing and applying neuroscience and technology (neuroS/T) in military and defense contexts require a comprehensive approach to address ethical and policy issues at the intersection of mind and technology.

Main themes and conclusions:

1. NeuroS/T capabilities include methods for assessing, accessing, and affecting brain functions, as well as force multipliers like AI and machine learning.
2. The effectiveness of neuroS/T in military contexts relies on human involvement in task delegation and reliance on outcomes.
3. Addressing ethical and policy issues surrounding neuroS/T in military contexts requires a multi-disciplinary approach, informed by historical case studies and guided by a cosmopolitan neuroethics framework.

Reference to generative AI or LLMs: The chapter mentions that quantum computing at scale could enable large multiscale simulations of the brain, which is relevant to the mind-tech nexus.

Recommendations to the Department of Defense: The author suggests that the DOD should establish task-agile, scientifically and situationally knowledgeable, and ethically responsible groups to inform and influence the formulation of international policies, treaties, and laws related to the use of mind-tech capabilities in national security and defense initiatives.

Follow-on questions:

1. How can the DOD foster international collaboration to establish guidelines and regulations for the use of neuroS/T in military contexts?

2. What specific measures should the DOD take to ensure that the development and deployment of neuroS/T in defense initiatives are guided by ethical principles?
3. How can the DOD maintain public trust when employing neuroS/T capabilities for national security and defense purposes?

Summarize Chapter 14 as an Elizabethan sonnet.

(GPT4)

Certainly! Here's an Elizabethan sonnet summarizing the themes of Chapter 14 on the intersection of neuroscience and military effectiveness, particularly focusing on the will to fight:

Sonnet on the Neuroscience of Combat's Will

In shadows deep where mind and matter meet,
 The sages pore o'er scrolls of neural arts,
 To bind the soldier's heart in steadfast beat,
 And steel the sinews of their martial parts.

This complex weave where threads of courage lie,
 Doth spin from studies deep within the brain,
 Where bonds of troop 'neath stress of battle tie,
 And wills are tested, forged anew through pain.

Yet caution holds, for what the mind can bend,
 Might fracture too the spirit it should brace;
 Thus scholars weigh with care the means and end,
 Intrigue with nerves to win the fearful race.

A complex system, will-to-fight, thus stands,
 Enriched, yet bound by neuroscience's hands.

This sonnet reflects the nuanced and multifaceted approach the chapter takes toward understanding the will to fight in military contexts, integrating neuroscience to potentially enhance military effectiveness while considering the profound implications of such interventions.

(Claude 3 Opus)

Here is a summary of the chapter as an Elizabethan sonnet:

Neuroscience's pow'r to shape the will to fight,
 A complex system where soldiers intertwine,

Demands we view cohesion with new light,
Beyond the individual, to bonds that bind.

Task cohesion from skill and trust may rise,
While social ties forge resilient bands,
But which path best the will-to-fight supplies?
Enhancements raise new risks that none foresaw.

If made too capable, the soldier's mind
May from the unit's fabric come undone.
Fear's roots, once severed, the will declined,
Though physical feats more ably may be won.

To neural study of the group we must incline,
Lest might dissolve the very will to fight we'd refine.

Lt Gen Shanahan and LtGen Groen are both past commanders of the DOD's Joint AI Center. Compare and contrast their chapters to list similarities in their theses and arguments, as well as differences. Call out specific reference to generative AI or LLMs, and any specific follow-on action or recommendation to the DOD.

(Claude 3 Opus)

Similarities in LtGen Groen and Lt Gen Shanahan's theses and arguments:

1. Both emphasize the importance of human-machine teaming and the need to optimize the integration of humans and AI-enabled machines to gain competitive advantages in future military operations.
2. They agree that AI will fundamentally alter the landscape of warfare and impact national security on a grand scale.
3. Both discuss the potential of AI to help manage large volumes of data, detect patterns, and draw useful connections across domains that humans might otherwise miss.
4. They acknowledge the risks and challenges associated with AI, such as the need for ethical considerations, proper governance, and the potential for adversarial attacks on AI systems.

Differences in their theses and arguments:

1. LtGen Groen focuses more on the historical context of competitive advantage in warfare and how AI represents a shift from physical lethality to cognitive mass. In contrast, Lt Gen Shanahan emphasizes the unique characteristics of AI that differentiate it from previous technologies, such as its self-learning capability and the unprecedented pace of change.
2. LtGen Groen discusses the potential of generative AI to help imagine future states and assist in creative problem-solving, while Lt Gen Shanahan does not specifically mention generative AI.
3. Lt Gen Shanahan delves more deeply into the cognitive risks associated with AI, such as automation bias and the potential for AI to reinforce human biases and blind spots. LtGen Groen touches on these issues but does not explore them as extensively.

References to generative AI or LLMs:

1. LtGen Groen specifically mentions generative AI, stating that it “moves the mind-tech nexus from deterministic outputs of narrow AI to a generative environment much more conducive to collaboration with human minds.” He argues that generative AI can help imagine future states and assist in creative problem-solving.
2. Lt Gen Shanahan does not explicitly mention generative AI or LLMs in his chapter.

Specific follow-on actions or recommendations to the DOD:

1. LtGen Groen suggests that the DOD and its international partners should dedicate efforts to capturing how we think about human-machine teaming and the roles of both humans and machines, similar to the approach taken for responsible AI and related technologies.
2. Lt Gen Shanahan recommends that the DOD change how systems are designed and developed, how humans are trained to work with AI-enabled machines, and how these systems adapt to human interaction and intervention. He also suggests that the military should dedicate more time to the study of the human condition, war and warfare, and culture, even in an AI-dominated future.

Act as the world's best open-source researcher. Develop an open-source collection plan to monitor Chinese government purchases or contracts for equipment, services, and research and development (R&D) in the areas identified in this book.

(Claude 3 Opus)

Here is a suggested open-source collection plan to monitor Chinese government purchases, contracts, and R&D related to the mind-tech areas covered in this book:

Collection Objectives:

- Identify Chinese government and military entities involved in mind-tech related research, development, and acquisition
- Track solicitations, purchases, and contracts for AI, neurotechnology, virtual/augmented reality, human performance enhancement, information operations, and related technologies
- Monitor academic partnerships, industry collaborations, and international joint ventures supporting Chinese mind-tech development
- Assess trends in Chinese mind-tech investments and gauge overall scale of efforts

Information Sources:

1. Official government procurement websites and databases
2. Chinese university and institute websites, publications, job postings
3. Company websites, press releases, financial disclosures of major Chinese tech firms
4. Defense industry trade publications and market research reports
5. Chinese social media (WeChat official accounts, Weibo, etc.)
6. Scholarly literature and patent databases
7. Findings from U.S. government agencies monitoring Chinese tech development
8. English and Chinese language media reporting

Collection Methods:

- Systematic searches of identified information sources using mind-tech related keywords

- Web scraping and indexing of relevant Chinese websites
- Social media monitoring for posts by key individuals/organizations
- Compiling and geolocating information on mind-tech conferences, competitions, demonstrations
- Gathering and translating procurement notices, contract award data
- Analyzing Chinese budget documents for mind-tech related allocations
- Extracting entity relationships and tech transfer networks from multiple sources

By continuously collecting information from diverse open sources, it should be possible to establish baseline knowledge and identify notable developments in Chinese mind-tech research and acquisition efforts over time. This collection plan would need to be adapted as collection priorities shift and new information sources and methods become available.

List all recommendations to the Department of Defense or U.S. federal government, by author.

(Claude 3 Opus)

Here are the recommendations to the Department of Defense or U.S. federal government, listed by author:

Lauren Kahn:

- Change how systems are designed and developed, how humans are trained to work with “smart” machines, and how AI-enabled systems adapt to human interaction and intervention.

James Giordano:

- Develop a comprehensive approach to addressing automation bias at the individual, system, and organizational levels.
- Adopt a cosmopolitan palette of (neuro)ethics that can be employed in particular community circumstances to obtain local and global utility and worth.

Josh Baughman:

- Develop technology to achieve information advantage and decision dominance in the cognitive domain.
- Ban TikTok for Joint Force use and discourage its broader use.

Ben Connable:

- Agree upon holistic concepts, definitions, and models of the human, will to fight, and combat effectiveness.
- Invest in human behavioral research before sinking significant funds into programs that reflect a tech-mind approach to innovation and design.

Aaron Frank:

- Establish criteria regarding the replication and reproducibility of basic neuroscience research findings before making investments in applications that may disrupt cohesion and the will-to-fight.
- Consider a broad portfolio inclusive of social, cognitive, and affective neuroscience research mechanisms and interventions to better understand effective investments.

Nicholas Wright:

- Implement a cognitive defense strategy centered on the “3 D’s”: Detect, Defend, and ensure Democratic compatibility.
- Build capabilities to detect and characterize influence operations, defend against them at multiple scales, and ensure new defensive capabilities are compatible with a free and open society.

You only listed six authors. Did you miss any authors and their recommendations?

I apologize for the oversight. Here are the recommendations from the remaining authors:

Andrew Gainer, Karl Van Orden, Jamie Lukos:

- Develop systems that shift the human burden away from sensing, processing, and intelligent filtering while leveraging computing advantages.

- Improve seamless human-system interactions through iterative testing and evaluation throughout the development and sustainment lifecycle.

David Omand:

- Recognize that new technologies, once used, can be reverse-engineered or copied, and plan accordingly.
- Establish ethical codes to maintain public support for new technological applications.

Sam Bendett:

- Monitor Russian efforts to enhance human performance and human-machine teaming through neurotechnology, information technology, and biotechnology.
- Anticipate Russian development of AI-enabled autonomous systems and human-machine interfaces for military applications.

Timothy Grayson:

- Apply AI to help manage complexity and provide decision support at the tactical, operational, and strategic levels.
- Develop AI-driven decision aids and act with operational practicality and speed to avoid institutional traps of over-complicating complex challenges.

Michael Groen:

- Develop an “operating system” and norms for human-machine teaming and mind-tech applications in military contexts.
- Ensure that the development of mind-tech capabilities proceeds with robust ethical guidelines and responsible AI principles.

William Casebeer:

- Invest in physiologic intelligence (PHYSIOINT) capabilities to assess and enhance warfighter performance.
- Develop human-machine interfaces and predictive models that integrate physiological, neurological, and behavioral data.

David Huberdeau:

- Advance the scientific understanding of human attributes to enable reliable measurement and analysis for military applications.

- Leverage artificial intelligence and machine learning algorithms to quantify human states and performance from multimodal sensor data.

With these additions, the list now covers all the authors and their key recommendations to the Department of Defense and U.S. federal government.

Did Jack Shanahan have any recommendations?

Yes, you're correct. I missed Jack Shanahan's recommendations. Here they are:

Jack Shanahan:

- Prioritize the redesign of human-machine interfaces and the recalibration of human and machine roles and responsibilities to optimize human-AI collaboration.

- Recognize that while AI will not change the nature of war, it will unquestionably change the character of warfare when combined with other emerging technologies.

- Dedicate more time to the study of the human condition, war and warfare, and culture, as war remains the ultimate human endeavor even in an AI-enabled future.

Thank you for pointing out this omission. The list of authors and their recommendations is now complete.

Act as a senior DOD leader such as the four-star combatant commander of INDO-PACOM. Taking the conclusions and recommendations of this book, identify your top mission concern in your Area of Responsibility, and create one task each for your J1, J2, J3, J4, J5, and J6. List the tasks in an email format not to exceed 200 words.

(Claude 3 Opus)

From: Commander, U.S. Indo-Pacific Command
(CDRUSINDOPACOM)

To: INDO-PACOM J-Dirs (J1, J2, J3, J4, J5, J6)

Subject: Countering PLA Cognitive Warfare Capabilities

Our top mission concern is the rapid development and potential use of cutting-edge Chinese mind-tech capabilities to gain cognitive advantages in the Indo-Pacific theater. To address this, I am directing the following actions:

J1: Develop a comprehensive personnel strategy to build cognitive resilience and counter PLA information operations. Implement training programs on digital hygiene, media literacy, and psychological defense.

J2: Establish a dedicated cell to monitor, analyze, and disseminate intelligence on PLA mind-tech research, development, and acquisition efforts. Provide quarterly assessments of PLA cognitive warfare capabilities and intentions.

J3: Conduct wargames and exercises to test our ability to operate effectively in a cognitively contested environment. Identify gaps in our cognitive defenses and develop mitigation strategies.

J4: Assess the sustainability of our forces in a prolonged cognitive conflict. Identify and address logistical vulnerabilities that could be exploited by PLA cognitive warfare tactics.

J5: Develop a theater-wide cognitive warfare strategy that integrates all elements of national power. Engage with allies and partners to build shared resilience against Chinese mind-tech threats.

J6: Accelerate the development and fielding of AI-enabled decision support systems, human-machine interfaces, and counter-cognitive warfare technologies. Ensure the security and reliability of our digital infrastructure.

Act as the world's best open-source intelligence expert working within the INDO-PACOM J2. Develop a comprehensive intelligence strategy to meet the Commander's intent in this email. Draft a response outlining this strategy with references to specific disciplines and targets to achieve the J2 task.

From: INDOPACOM J2

To: Commander, U.S. Indo-Pacific Command (CDRUSINDOPACOM)

Subject: Re: Countering PLA Cognitive Warfare Capabilities

Commander,

To meet your intent and address the J2 task, I propose the following comprehensive open-source intelligence (OSINT) strategy to monitor, analyze, and disseminate intelligence on PLA mind-tech research, development, and acquisition efforts:

1. Establish a dedicated OSINT cell focused on PLA cognitive warfare capabilities:
 - a. Assign analysts with expertise in Mandarin Chinese, AI, neuroscience, and military technology.
 - b. Develop a network of subject matter experts from academia, industry, and partner nations to provide specialized insights.
2. Identify and prioritize key intelligence targets:
 - a. PLA research institutions, such as the Academy of Military Science and the National University of Defense Technology.
 - b. Chinese tech giants, including Baidu, Alibaba, Tencent, and Huawei, focusing on their military-related projects.
 - c. PLA General Staff Department's Third Department (3PLA) and Strategic Support Force (SSF), responsible for cyber and electronic warfare.
3. Employ a multi-disciplinary approach to collect and analyze relevant data:
 - a. Systematically monitor Chinese government procurement websites, military forums, and research databases for indicators of mind-tech development.
 - b. Conduct sentiment analysis on Chinese social media platforms to gauge public opinion and identify potential PLA narratives.
 - c. Leverage advanced AI tools for data mining, pattern recognition, and predictive analytics to process large volumes of unstructured data.
4. Produce actionable intelligence products:
 - a. Develop quarterly strategic assessments of PLA cognitive warfare doctrine, capabilities, and intentions.
 - b. Issue regular intelligence updates on key PLA mind-tech research breakthroughs, technology acquisitions, and personnel changes.

c. Create visualizations, such as network graphs and geospatial overlays, to illustrate PLA cognitive warfare threat vectors and potential targets.

5. Foster intelligence sharing and collaboration:

a. Establish information-sharing mechanisms with key allies and partners, particularly Japan, South Korea, and Taiwan, to expand collection capabilities and fuse insights.

b. Participate in cross-functional working groups with other INDOPACOM J-codes to ensure seamless integration of OSINT into theater-wide planning and operations.

By implementing this strategy, the J2 will provide you with timely, relevant, and actionable intelligence to support decision-making and counter PLA cognitive warfare threats in the Indo-Pacific theater.

Respectfully,

INDOPACOM J2

Conduct internet research as needed. Draft a short email in Japanese inviting the appropriate office within the Japan Self Defense Force to collaborate on this open-source intelligence effort. In a pithy email, outline the concerns of this book and suggest areas of cooperation based on the above categories, cross-referenced with any recent official pronouncements or reports from the Government of Japan with concerns that overlap with the themes of this book. Output as sentence-by-sentence translation with English following the original Japanese.

(GPT4)

Subject: 提携の提案：オープンソースインテリジェンス活動に関する日米協力強化に向けて

Subject: Proposal for Partnership: Towards Strengthening Japan-U.S. Cooperation in Open Source Intelligence Activities

拝啓

Dear Sir/Madam,

日本の安全保障環境は厳しさを増しており、その対応として政府は新たな国家安全保障戦略（NSS）、国防戦略（NDS）、防衛力整備計画（DBP）を承認しました。

The security environment in Japan has become increasingly severe, and in response, the government has approved new National Security Strategy (NSS), National Defense Strategy (NDS), and Defense Buildup Plan (DBP).

これらの文書は、サイバーセキュリティ、情報戦、および国際的な協力の強化を含む多岐にわたる防衛能力の向上を目指しています【<https://www.rand.org/pubs/commentary/2023/03/japans-new-security-policies-a-long-road-to-full-implementation.html>】【https://www.mofa.go.jp/fp/nsp/page1we_000081.html】。

These documents aim to enhance a wide range of defense capabilities, including cybersecurity, information warfare, and the strengthening of international cooperation.

この文脈で、私たちは次の分野での協力を提案いたします：

In this context, we propose cooperation in the following areas:

1. ****専門家ネットワークの構築:**** 日本のアカデミア、産業界、そして同盟国からの専門家と共に、中国の軍事技術、AI、ニューロサイエンスに関する情報を共有し、分析能力を高めること。

1. ****Building Expert Networks:**** *Collaborating with experts from Japanese academia, industry, and allied nations to share and enhance analytical capabilities regarding Chinese military technology, AI, and neuroscience.*

2. ****データ収集と分析:**** 中国政府の調達ウェブサイトや軍事フォーラムからのデータをシステムティックに監視し、AIツールを用いて大量の非構造データを分析する。

2. ****Data Collection and Analysis:**** *Systematically monitoring data from Chinese government procurement websites and military forums, and analyzing large volumes of unstructured data using AI tools.*

3. ****情報共有の強化:**** 同盟国との間で情報共有メカニズムを確立し、地域安全保障を共同で向上させる。

3. ***Enhancing Information Sharing:*** *Establishing information sharing mechanisms with allies to jointly improve regional security.*
 日本が新たに設定した情報戦やサイバー防衛のポスチャーは、今後の脅威に対してより強固な抑止力を発揮するために重要です。貴職との協力が、この目標達成に向けた重要なステップとなることを願っています。

The new posture on information warfare and cyber defense that Japan has established is crucial for presenting a stronger deterrence against future threats. We hope that cooperation with you will be an important step towards achieving this goal.

何卒ご検討のほどよろしくお願い申し上げます。

We kindly request your consideration.

敬具

Sincerely,

[あなたの名前] [Your Name]

[あなたの職位] [Your Position]

[あなたの組織] [Your Organization]

Act as a senior DOD acquisition official specializing in R&D. Suggest five actions, tied to appropriate DOD offices, to translate Aaron Frank's insights about neuroscience into operational requirements to develop relevant technology to equip service members in combat. Describe the potential equipment and which service members might benefit.

(Claude 3 Opus)

As a senior DOD acquisition official specializing in R&D, I suggest the following five actions to translate Aaron Frank's insights about neuroscience into operational requirements for developing relevant technology to equip service members in combat:

1. Collaborate with the U.S. Army Medical Research and Development Command (USAMRDC) to develop advanced neuroscience-based training systems that enhance cognitive flexibility and emotional regulation in high-stress combat situations. These systems could incorporate virtual reality and biofeedback technologies to help service members, particularly those in frontline combat roles such as infantry, special operations forces, and

combat medics, to maintain optimal performance and decision-making capabilities under duress.

2. Partner with the Office of Naval Research (ONR) to invest in research on neural mechanisms underlying team cohesion and trust. Leverage this research to create evidence-based training programs and technologies that foster strong interpersonal bonds within small tactical units, such as Navy SEAL teams and Marine Corps infantry squads, ultimately enhancing their collective will to fight and mission effectiveness.
3. Work with the Air Force Research Laboratory (AFRL) to develop neuroscience-inspired human-machine interface technologies that optimize cognitive load and information processing for pilots, air battle managers, and other airmen operating in complex, data-rich environments. These technologies could include adaptive automation, augmented reality displays, and AI-assisted decision support tools that dynamically adjust to individual cognitive states and capabilities.
4. Engage with the Defense Advanced Research Projects Agency (DARPA) to explore the potential of neurotechnology for enhancing situational awareness and intuitive decision-making in urban combat environments. This effort could involve developing lightweight, non-invasive brain-computer interfaces that augment service members' natural sensory and cognitive abilities, benefiting ground forces operating in complex, rapidly evolving urban terrain.
5. Collaborate with the Joint Program Committee for Military Operational Medicine (JPC-5) to prioritize research on neuroscience-based interventions for mitigating the effects of sleep deprivation, chronic stress, and traumatic brain injury on service members' cognitive and emotional functioning. Translate these findings into field-deployable technologies, such as wearable devices and pharmacological countermeasures, that can help sustain the performance and resilience of service members across all branches during prolonged, high-intensity operations.

By pursuing these actions in partnership with key DOD research and development organizations, we can harness the insights from Aaron Frank's work to drive the development of cutting-edge neuroscience-based technologies. These innovations will directly support the cognitive,

emotional, and social aspects of service members' performance in combat, ultimately enhancing their individual and collective will to fight.

Analyze the attached chapters (note: Bendett and Baughman chapters). Write a 200 word pitch for a science fiction story that is a retrospective on how the United States lost a future conflict to Russia and China based on the trends Bendett and Baughman identify. Identify specific mechanisms where the adversary nations would take advantage of a strategic blind spot. The science fiction story is in the long tradition of speculative fiction meant to warn current policymakers, so reality-based plausibility is key.

(Claude 3 Opus)

In a not-so-distant future, the United States found itself on the losing end of a global conflict against a Sino-Russian alliance. Blinded by its own technological hubris, America failed to recognize the strategic advantages its adversaries gained through their relentless pursuit of cognitive dominance and human-machine symbiosis.

As the PLA harnessed the power of generative AI, the metaverse, and brain-computer interfaces to manipulate perceptions, sow discord, and undermine the will to fight, Russia's military enhanced its soldiers' performance with neural helmets, AI-driven decision support, and autonomous drone swarms. American warfighters, though technologically advanced, were ill-prepared for the psychological onslaught and the speed of their enemies' AI-augmented decision-making.

In this cautionary tale, set in 2040, a veteran journalist recounts the critical failures that led to America's downfall: the dismissal of China's cognitive warfare strategy, the underestimation of Russia's human-machine integration, and the reluctance to adapt in the face of an unconventional, mind-centric battlefield. Through vivid accounts and haunting hindsight, the story serves as a dire warning to today's policymakers, urging them to confront the realities of a new era of conflict, where the battleground extends from the physical to the psychological, and the line between human and machine blurs.

Write the first paragraph of this cautionary tale. Adapt the first-person point-of-view of this veteran journalist, in the voice of a Marlowe-esque hard-bitten, world-weary patriot who is anguished by the consequences of the United States loss.

(Claude 3 Opus)

The year is 2040, and I'm sitting in the ruins of what was once the beating heart of American democracy, Washington D.C. The scars of our defeat are etched into the crumbling monuments and the haunted eyes of the survivors. I've spent the last decade trying to piece together how we lost the war, how our once-great nation was brought to its knees by the insidious machinations of our adversaries. It's a story that needs to be told, a warning to future generations, if there are any left who will listen. We thought we were invincible, that our technological superiority would always keep us ahead of the game. But while we were building bigger, faster, and smarter machines, our enemies were perfecting the art of infiltrating and manipulating the human mind. We never saw it coming, and by the time we realized the true nature of the threat, it was already too late.

Generate a photo-realistic, 35mm film shot of the referenced author at the end of the text, wide aspect ratio.

(OpenAI's DALL-E)



Author Biographies

Editors

Nicholas Wright

Dr. Nicholas Wright combines neuroscientific, behavioral, and technological insights to understand emerging technology and global strategy in ways useful for policy. He is an affiliated scholar at Georgetown University, an honorary senior research fellow at University College London (UCL), a scientist at Intelligent Biology, and an adjunct fellow (non-resident) at the Center for Strategic and International Studies. He is currently writing a book for Pan Macmillan (UK) and St. Martin's Press (US) on the brain and war. He works closely with various parts of the US and UK Governments. On artificial intelligence (AI), he advises Europe's largest tech company, SAP. DARPA used his definition of *gray zone conflict* for its recent AI program on the gray zone. *Foreign Affairs* chose his piece on AI and the global order for its Top 10 of 2018 on the net. He edited the book *Artificial Intelligence, China, Russia and Global Order* (Air University Press, 2019). He previously worked in nuclear policy at the Carnegie Endowment for International Peace, Washington, DC, and in functional brain imaging at UCL at the Department of Government at the London School of Economics and was a clinical neurologist in Oxford and London. He has many academic (e.g., Proceedings of the Royal Society), general (e.g., *The Atlantic*, *Foreign Policy*, *Foreign Affairs*), and policy publications (e.g., <https://www.intelligentbiology.co.uk/>) and has appeared on the BBC and CNN. He has a medical degree from UCL, a BSc in Health Policy from Imperial College London, Membership of the Royal College of Physicians (UK), and an MSc in neuroscience and a PhD in neuroscience, both from UCL.

Michael Miklaucic

Michael Miklaucic is a senior fellow of the National Defense University (NDU), and the Editor-in-Chief of PRISM, NDU's flagship journal of national and international security affairs. Mr. Miklaucic is also recently named the inaugural Oswaldo Aranha Chair Professor of Security and Defense at the University of Sao Paulo (Brazil), a member

of the academic faculty at the University of Chicago, and adjunct lecturer at the George C. Marshall European Center for Security Studies. Previously he served in various positions at the US Agency for International Development (USAID) and the Department of State, including USAID representative on the Civilian Response Corps Inter-Agency Task Force, as the senior program officer in the USAID Office of Democracy and Governance, and Rule of Law Specialist in the Center for Democracy and Governance. In 2002–3 he served as the Department of State deputy for war crimes issues. In that position, he was responsible for US relations with the International Criminal Tribunal for Rwanda (ICTR), the Special Court for Sierra Leone (SCSL), war crimes issues and negotiations in East Timor and Cambodia, and the early implementation of the Sudan Peace Act. His publications have appeared in *Financial Times*, *The Diplomat*, *The Hill*, *Real Clear Defense*, and others. He studied at the University of California, the London School of Economics, and the School for Advanced International Studies.

Todd Veazie

Todd Veazie serves as director of the Strategic Multilayer Assessment (SMA) office in the Joint Staff's Operations Directorate. SMA supports senior military leaders by assessing complex operational environments and technical challenges that require collaborative multiagency, multidisciplinary, mixed-method approaches to expand strategic horizons and inform effective strategy.

Prior to reentering public service, he was the chief operating officer at Kiernan Group Holdings, Inc., a global consulting firm specializing in law enforcement, risk services, defense, intelligence, emergency management, and critical infrastructure resiliency. Mr. Veazie served for thirty years in the United States Navy, attaining the rank of captain. He transitioned to the federal executive service and was assigned to the National Counterterrorism Center. At NCTC he led a talented team that provided dispassionate, whole-of-government assessments and strategic decision support to the president and his National Security Council staff.

He earned a bachelor of science degree in marine science from the University of South Carolina and was commissioned in 1986. After commissioning he reported to Basic Underwater Demolition/SEAL training and graduated in Class 140. As a naval special warfare (NSW) SEAL officer, he served in East and West Coast SEAL Teams and deployed to over fifty countries. He led naval special warfare formations in the

execution of combat and peacetime special operations missions in Latin America, Europe, Africa, the Western Pacific, Central Asia, and the Middle East. Command tours include SEAL Team SEVEN in San Diego and Naval Special Warfare Unit THREE in Bahrain as well as duty as commodore, Naval Special Warfare Group FOUR in Virginia Beach.

Mr. Veazie served in numerous staff assignments that include the executive director of Joining Forces in the Office of the First Lady at the White House, personnel policy at the Bureau of Naval Personnel, the assistant chief of staff for resources, requirements, and assessments (J8) for the commander, Naval Special Warfare Command, and in the Operations Directorate (J3) on the Joint Staff at the Pentagon. He is a 2003 graduate of the National War College where he earned a master's degree in national security strategy.

Forewords

GEN James E. Rainey, US Army

General Rainey is the commander of the Army Futures Command (AFC). Headquartered in Austin, Texas, AFC is the Army's newest major command, responsible for transforming the Army to ensure war-winning future readiness, employing 30,000 Soldiers and civilians at 128 locations worldwide. In his previous position, General Rainey served at the Pentagon, where he oversaw the Army's operations and plans. General Rainey commissioned as an infantry lieutenant upon graduating from Eastern Kentucky University in 1987. He has commanded at every level from platoon to division and has served in numerous combat deployments in both Iraq and Afghanistan. He earned a master's degree in advanced military arts and science from the School of Advanced Military Studies and another in public administration from Troy University. He also completed a Senior Service Fellowship at the University of Denver's Korbel School of International Relations.

Sir Lawrence Freedman

Sir Lawrence Freedman is Emeritus Professor of War Studies at King's College London. He was a professor of war studies at King's College London from 1982 to 2014 and vice-principal from 2003 to 2013. He was educated at the Universities of Manchester, York, and Oxford.

Before joining King's, he held research appointments at Nuffield College Oxford, the International Institute of Strategic Studies (IISS), and the Royal Institute of International Affairs. Elected a fellow of the British Academy in 1995, he was appointed the official historian of the Falklands Campaign in 1997. In June 2009 he was appointed to serve as a member of the official inquiry into Britain and the 2003 Iraq War.

Professor Freedman has written extensively on nuclear strategy and the cold war as well as commenting regularly on contemporary security issues. Among his books are *Kennedy's Wars: Berlin, Cuba, Laos, and Vietnam* (2000), *The Evolution of Nuclear Strategy* (4th ed., 2019), *Deterrence* (2005), the two-volume *Official History of the Falklands Campaign* (2nd ed., 2007), *A Choice of Enemies: America Confronts the Middle East* (2009), *Strategy: A History* (2013), *The Future of War: A History* (2017), and *Ukraine and the Art of Strategy* (2019) and the Adelphi Paper *The Transformation in Strategic Affairs* (2004).

Chapter Authors

Josh Baughman

Joshua "Josh" D. Baughman currently serves as an analyst at Air University's China Aerospace Studies Institute (CASI). His research centers on China's People's Liberation Army (PLA) activity in the cyber and information domain as well as work on the PLA Rocket Force. He guest lectures at the National Defense University and Institute of World Politics in master's and doctoral level courses on topics such as China's cyber strategy and misinformation efforts. He presents and publishes regularly and has received international recognition for his work on the metaverse and generative AI. Mr. Baughman previously worked at the National Defense University (NDU) College of Information and Cyberspace (CIC), US Air Force Academy, and Tsinghua University in Beijing. Collectively, he spent three years living in Beijing working as an editor and journalist on China security issues as well as a television host, director, writer, and producer. In his spare time, Josh volunteers for the Military Cyber Professionals Association, a 501(c)(3) educational nonprofit charity, as part of national leadership as the chief marketing officer.

Samuel Bendett

Mr. Samuel Bendett is an adviser with CNA Strategy, Policy, Plans and Programs Center (SP3), where he is a member of the Russia Studies Program. He is also an adjunct senior fellow at the Center for a New American Security. His work involves research on the Russian defense and technology developments, unmanned and autonomous military systems and artificial intelligence as well as Russian military capabilities and decision-making during crises. He is also an honorary “Mad Scientist” with the US Army Training and Doctrine Command’s (TRADOC) Mad Scientist Initiative and a Russian military autonomy and AI subject matter expert for the DOD’s Defense Systems Information Analysis Center. Prior to joining CNA, Mr. Bendett worked at the National Defense University on emerging and disruptive technologies for the Department of Defense response in domestic and international crisis situations. His previous experience includes working for the US Congress, private sector, and nonprofit organizations on foreign policy, international conflict resolution, and defense and security issues. Mr. Bendett’s analyses, views, and commentary on Russian military robotics, unmanned systems, and artificial intelligence capabilities appear in *Forbes*, *CAISRnet*, *Defense One*, *War on the Rocks*, *Breaking Defense*, *The National Interest*, and *The Strategy Bridge*. Samuel Bendett received his MA in law and diplomacy from the Fletcher School, Tufts University, and BA in politics and English from Brandeis University. He has native fluency in Russian.

William D. Casebeer

Dr. William D. Casebeer is the director of the Intelligent Systems Center at HRL Laboratories. His lab uses next-generation technology to advance human-machine teaming, machine learning, and intelligent agent construction for national security. He has decades of experience leading interdisciplinary teams of scientists and engineers to creative solutions for pressing national security problems, including as the director, senior director, and program manager roles at Riverside Research, Scientific Systems Company, Inc., the Innovation Lab at Beyond Conflict, the Human Systems and Autonomy Lab at Lockheed Martin’s Advanced Technology Laboratories, and at the Defense Advanced Research Projects Agency as program manager in the Defense Sciences Office and Biological Technologies Office. Dr. Casebeer retired from active US Air Force duty as a lieutenant colonel and intelligence

analyst in August 2011 and is a graduate of the Air Force Academy, University of Arizona, Naval Postgraduate School, and University of California at San Diego.

Ben Connable

Dr. Ben Connable is an adjunct professor of security studies at Georgetown University, a principal research scientist at the nonprofit Center of Naval Analyses, senior research advisor to the nonprofit DT Institute, and principal owner of Battle Research Group. He recently served as a nonresident senior fellow at the Atlantic Council. Dr. Connable is a retired Marine Corps Middle East foreign area officer and intelligence officer. From 2009 through 2021, Dr. Connable was a senior political scientist at the RAND Corporation, where he led over twenty research projects for US government and allied sponsors. His most recent work focused on the analysis of the will to fight and methods for analyzing, modeling, gaming, and simulating human behavior in conflict. Dr. Connable co-led seven research projects on will to fight and co-authored *Will to Fight*, *National Will to Fight*, *NATO Will to Fight*, and other reports. He is the author of *Iraqi Army Will to Fight* and, most recently, *Ground Combat: Puncturing the Myths of Modern War*. Dr. Connable has published extensively, including with the *New York Times*, the *Washington Post*, and *Foreign Affairs*. At Georgetown University, he teaches a course on human behavior in war. Dr. Connable received his MA in national security affairs from the Naval Postgraduate School and his PhD in war studies from King's College London.

Aaron B. Frank

Dr. Aaron Frank is a senior information scientist at the RAND Corporation who specializes in the development of analytic tradecraft and decision support tools for analyzing complex national security issues. He is interested in problems associated with uncertainty, the philosophy and history of science, decision-making, and the way in which models mediate between data and theory to understand individual choices and collective action. He has employed agent-based models, war games, and other analytic tools to assess the benefits and limitations of historical and experimental data and generate missing information via simulation to analyze problems ranging from regional

conflicts between national governments, to military innovation and transformation, to the dynamics of social identities.

Dr. Frank's recent projects have primarily focused on two challenges, each of which seek to bring computation closer to national security decision-making. One area is in the field of computational social science, where he is working with advanced research agencies on the assessment, development, and use of social science theories, models, and simulations in support of incorporating assessments of individual and group behavior into national security decision-making. The second area is focused on assessing the quality, completeness, and analytic usability of data held within enterprise information technology systems and developing long-term visions for how data, analytics, machine learning, and artificial intelligence can assist senior executives and military leaders in decision-making by extracting more value from the data in their possession and developing new capabilities to improve data quality and completeness. Dr. Frank has a PhD in computational social science from George Mason University, a MA in national security studies from Georgetown University, and a BA in political science from Boston University.

Andrew D. Gainer

Andrew Gainer is an engineer with the Johns Hopkins University Applied Physics Laboratory (JHUAPL). Assigned as a field representative to the Naval Information Warfare Center (NIWC) Pacific in San Diego, California, he develops systems and operational concepts for complex, all-domain warfare. He attended Northwestern University in Evanston, Illinois, obtaining a bachelor of civil engineering degree and a commission in the United States Navy. His active duty career included fourteen years in the submarine force and sixteen years as an information warfare officer. During his final afloat tour, he served as information warfare commander aboard the USS *John C. Stennis* Carrier Strike Group. Returning to San Diego, he completed his naval career as commanding officer, NIWC Pacific, serving from 2020 to 2023. Mr. Gainer also holds a master of science degree in information technology management from the University of Maryland.

Jim Giordano

James Giordano, PhD, DPhil, is the director of the Center for Disruptive Technology and Future Warfare of the Institute for National

Strategic Studies at the National Defense University, Washington, DC. He is Professor Emeritus in the Departments of Neurology and Biochemistry at Georgetown University Medical Center, Washington, DC; and served as the senior bioethicist of the Defense Medical Ethics Center and professor of psychiatry at the Uniformed Services University, Bethesda, Maryland; senior science advisory fellow of the Strategic Multilayer Assessment Branch of the Joint Staff, Pentagon; and the Distinguished Stockdale Fellow in Science, Technology, and Ethics at the United States Naval Academy. He previously served as the Donovan Group Senior Fellow, US Special Operations Command; fellow of the Simon Center for the Military Ethic, US Military Academy, West Point; founding member of the Neuroethics, Legal, and Social Issues Advisory Panel of the Defense Advanced Research Projects Agency (DARPA); task leader of the Working Group on Dual-Use of the EU-Human Brain Project; and was an appointed member of the Department of Health and Human Services' Secretary's Advisory Committee for Human Research Protection (HHS-SACHRP). Professor Giordano is the author of over 350 peer-reviewed publications, nine books, and fifty governmental reports on science, technology, and biosecurity and is an elected fellow of the Hastings Center for Ethics, an elected member of the European Academy of Science and Arts, a fellow of the Royal Society of Medicine (UK), and a Fulbright Professorial Fellow. A former US naval officer, he was a designated aerospace physiologist and research psychologist and served with the US Navy and Marine Corps.

Timothy Grayson

Dr. Timothy Grayson is senior vice president, chief architect, Defense Systems Sector, Leidos Corporation. Formerly, he was a special assistant to the Secretary of the Air Force with the primary responsibility to coordinate concept development, analysis, and implementation of the secretary's Operational Imperatives, the critical operational air and space capabilities needed to deter, and if necessary, defeat our pacing challenges.

Prior to this role, Dr. Grayson was the director of the Strategic Technology Office (STO) at the Defense Advanced Research Projects Agency (DARPA). He led the office in developing breakthrough technologies to enable warfighters to field, operate, and adapt distributed, joint, all-domain combat capabilities at continuous speed. Dr. Grayson came to the STO in 2018 from a varied career in government and

industry. Immediately prior to DARPA, he was the founder and president of Fortitude Mission Research LLC, a consulting company specializing in strategy and technology analysis related to defense and intelligence. Dr. Grayson has extensive government experience. He spent several years as a senior intelligence officer with the Central Intelligence Agency (CIA) in the Directorate of Science and Technology and culminating in a tour at the Office of the Director of National Intelligence. Prior to the CIA, Dr. Grayson was a program manager and senior scientist at DARPA and a research fellow at Air Force Wright Laboratory (now part of Air Force Research Laboratory). Dr. Grayson holds a PhD. in physics from University of Rochester, where he specialized in quantum optics, and a BS in physics from the University of Dayton with minors in mathematics and computer science.

Michael Groen

Lt. Gen. (Ret.) Michael Groen served over 36 years in the Marine Corps, culminating his career as the director of the Joint Artificial Intelligence Center and the senior executive for AI in the Department of Defense. He previously served at the National Security Agency, overseeing computer network operations, and as the director of Joint Staff Intelligence (JSJ2), working closely with the chairman of the Joint Chiefs. Groen is an experienced Marine commander and multi-tour combat veteran. He has earned master's degrees in electrical engineering and applied physics. He is the author of *With the First Marine Division in Iraq, 2003: No Greater Friend, No Worse Enemy*.

David Huberdeau

Dr. David Huberdeau is an AI/ML engineer at Riverside Research Institute (RRI) and principal investigator for RRI under the NGA's GEOCOG program. Dr. Huberdeau leads a team of engineers and scientists focused on innovation for more effective human machine synergy, including novel methods in cognitive state estimation and human-aware autonomous planning. He and his team have published in leading journals on measuring human performance and learning and using gaming environments, virtual reality, and humanoid robots to develop and evaluate human-machine synergy solutions. Prior to joining RRI, Dr. Huberdeau completed a postdoctoral fellowship at Yale University where he studied cognitive impairments of neurodegenerative conditions like Alzheimer's disease. He acquired his PhD

in biomedical engineering from Johns Hopkins University and has over ten years of experience in the development and use of technology to monitor, assess, predict, and interpret human behavior.

Lauren Kahn

Ms. Lauren Kahn is a Senior Research Analyst at Georgetown's Center for Security and Emerging Technology (CSET), focused on national security applications of artificial intelligence. Prior to CSET, she was a research fellow at the Council on Foreign Relations (CFR) within the National Security and Defense and Digital and Cyberspace Policy programs, where she worked on defense innovation and the impact of emerging technologies on international security, with a particular emphasis on AI. Prior to joining CFR, she worked as a research fellow at Perry World House, the University of Pennsylvania's global policy think tank, where she helped launch its project on emerging technologies and global politics. Her work has appeared in outlets including *Foreign Affairs*, *Lawfare*, *War on the Rocks*, the *Journal of Conflict Resolution*, and *AI & Society* and has been featured in *The Economist*.

Jamie R. Lukos

Dr. Jamie Lukos is the senior technologist (ST) for cognitive and decision science at the Naval Information Warfare Center (NIWC) Pacific. Her research primarily focuses on dynamic measurements of operators during human-autonomy interactions and mobile brain imaging during demanding physical and cognitive tasks. Her work leads to a better understanding of the neurological basis of human decision-making in operationally relevant environments and informs algorithm development for future physiological monitoring devices, human-machine teaming bidirectional communication, and fieldable brain computer interfaces.

She received her PhD from Arizona State University, where she worked in the Neural Control of Movement laboratory studying anticipatory grasp control and human decision-making in unpredictable settings and her BS from the University of Michigan, where she worked in the Human Neuromechanics Laboratory. She also received her MA from the US Naval War College in defense and strategic Studies in 2022 and has a Human Systems Integration Certificate from the Naval Postgraduate School.

In 2021 the Office of the Secretary of Defense selected Dr. Lukos for the Percy Hobart Fellowship with the UK Royal Navy and as the ASN(RD&A) Dr. Delores M. Etter Top Scientist. She has been recognized with several individual and team awards, including a 2019 NAVWAR Lightning Bolt Team Award (DAISEY Team) and a 2018 Publication of the Year Award (“Advancing Autonomy while Building Trust in Unmanned and Autonomous Systems”).

Sir David Omand

Sir David Omand GCB is Visiting Professor in the Department of War Studies, King’s College London. His posts in British government service include UK security and intelligence coordinator in the Cabinet Office, permanent secretary of the home office, director of the Government Communications Headquarters (GCHQ), and deputy under-secretary of state for policy in the Ministry of Defence. He served for seven years as a member of the Joint Intelligence Committee (JIC). He is a member of the Senior Advisory Board of Paladin Capital, and until 2021, he was the senior independent director of Babcock International Group. He has published the books *How to Survive a Crisis: Lessons in Resilience and Avoiding Disaster* (Penguin, 2024), *Securing the State* (Hurst, 2010) and (with Prof. Mark Phythian) *Principled Spying: The Ethics of Secret Intelligence* (Oxford 2018). His book *How Spies Think: 10 Lessons from Intelligence* is now published in paperback by Penguin (July 2021).

Lt. Gen. Jack Shanahan, US Air Force (Ret.)

General Shanahan retired in 2020 after a thirty-six-year military career in the US Air Force. In his final assignment, he served as the inaugural director of the US Department of Defense (DOD) Joint Artificial Center (JAIC). General Shanahan served in a variety of operational and staff positions in various fields, including flying, intelligence, policy, and command and control. He commanded at the squadron, group, wing, agency, and numbered Air Force levels. As the first director of the Algorithmic Warfare Cross-Functional Team (Project Maven), he established and led the DOD’s pathfinder AI fielding program charged with bringing AI capabilities to intelligence collection and analysis.

General Shanahan is a graduate of the North Carolina State University (NCSU) Master of International Studies program and serves

on the NCSU School of Public and International Affairs Advisory Council. He is an adjunct senior fellow with the Center for a New American Security (CNAS) Technology and National Security Program and a member of the CNAS Defense Technology Task Force. He is also an advisor to the Special Competitive Studies Project (SCSP) Defense Panel. He serves on a variety of AI-related committees, boards, and advisory groups and as a consultant on the use of AI-enabled technologies for national security.

Karl F. Van Orden

Dr. Van Orden recently retired as a member of the scientific and technical cadre of the Senior Executive Service specialized in advanced user interfaces and optimizing decision-making at the Naval Information Warfare Center (NIWC) Pacific in San Diego. He led or worked on projects related to improving operational planning, command and control, air and missile defense tactical systems, and tactical employment of robotic craft by Marines. From 2006 to 2015 he was the director of research and development at the Naval Health Research Center. Dr. Van Orden also served as a uniformed Navy research psychologist from 1986 to 2006 and conducted studies in visual perception, stress and performance, psychophysiological measures of fatigue and workload, and improving the training of Fleet Marine Force corpsmen by using highly realistic and stressful training strategies. He has held several additional duty appointments at the Office of Naval Research supporting research program management. Dr. Van Orden received his BS in psychology at Syracuse University and earned his PhD in biological psychology (visual perception and psychophysics) at Syracuse.

David Vernal

David Vernal is a retired Air Force colonel whose last assignment was director of intelligence for Sixteenth Air Force (Air Forces Cyber), the service's operational arm of US Cyber Command. In his twenty-seven-year career, he also co-led interagency development of cyber operations policy for the Obama administration as a director on the National Security Council staff and studied as an Olmsted Scholar in Taipei, Taiwan. He holds degrees from Harvard University, Air War College, and Stanford's Graduate School of Business, where he is researching generative AI applications for national security as an affiliate of Stanford's Gordian Knot Center for National Security Innovation.

Acknowledgments

We owe a huge debt to the authors who contributed to this volume. Their scholarship and ideas changed the way we think about these momentous issues: They asked insightful questions and gave thoughtful answers. The contributors also kindly persevered from their initial talks and discussions with us all the way through to final publication—thank you.

Many other people also helped make this volume a reality, and we would like to highlight the wonderful support of two key individuals who really went above and beyond. Mariah Yager in the Strategic Multilayer Assessment (SMA) office not only corralled many of the speakers in the Mind-Tech Nexus speaker series but also provided timely intellectual insights, as well as energetic administrative support. Jeanne Shamburger was our editor at Air University Press (AUP), where she was diligent and hard-working and brought a really helpful problem-solving attitude to all the inevitable wrinkles we faced.

We would like to extend thanks to Nicole Omundson at SMA who helped with the speaker series. We also thank all those scholars and practitioners who gave talks on the Mind-Tech Nexus panel at the 2023 SMA conference at Joint Base Andrews and in the speaker series more broadly, who included the then DARPA director, Dr. Stefanie Tompkins; Rear Adm. Douglas Small; Maj. Gen. Matthew Dinmore (Sixteenth Air Force); and David Kilcullen. We also thank the team at AUP, including Paul Hoffman, who led administratively at the Press, and those who did a great job producing the book, including Jonathan Marks (typesetter), Catherine Smith (illustrator/cover), and Donna Budjenska (draft and final quality reviews). We also thank our wonderful SMA community of interest and audience at our speaker events who ensured that so many of the ideas in this volume were probed, interrogated, and improved.

Index

- Aegis, 83, 85
- air battle manager (ABM), 98, 104, 106–7, 356
- artificial intelligence (AI)
 - as a human replacement, viii, 7, 29, 31, 36, 154, 171, 340–41
 - as augmenting the human, 8, 29, 31, 86, 95, 98, 117, 125, 173, 186, 202, 215–16, 218, 234, 245, 335, 341, 346, 356
 - assistant, 7, 98, 154, 169
 - governance, 44, 50, 122, 344
- automation bias, 17, 29, 32–35, 37, 134, 144n29, 174, 341, 345, 347
- autonomous, 10, 31–33, 35, 89, 99, 130, 139, 169–70, 187, 211, 217, 325, 349, 357
- aviation accidents, 18, 34, 83–85

- big data, 40, 43, 305–6
- brain-computer interface (BCI), 8, 19, 151, 155, 161–63, 218, 224, 236–37, 247, 254, 256–57, 330, 356

- cognitive defense, 348, 351
- Cold War, xiii, 13, 62, 64, 68, 71, 165, 295, 299, 302, 305, 314, 326
- Collaborative Combat Aircraft (CCA), 33, 37, 99
- command and control (C2), viii, xi, 18–19, 30, 32, xi, 77, 82, 87, 89, 104, 113, 119, 124, 128, 130, 132, 233, 329
- competitive advantage, 44, 117–20, 327, 345
- complexity, xi, 77–78, 80, 82, 85, 89–91, 93, 95–96, 100–104, 106–14, 119, 132, 200, 262–63, 266, 284
- convergence, vii, ix, xi, xiv, 1–3, 5–7, 16, 19, 23, 93, 151–52, 163–64, 167–72, 175, 323, 326–28, 330
- crisis, 47, 128, 132, 363
- CRISPR, 41, 174–75
- cryptography, 62, 66–67
- cybersecurity, 169, 354
- data, information, knowledge, wisdom, 11–12, 173
- decision-making
 - AI role in, xiv, 4, 21, 32, 36, 93, 98, 100, 117, 120–21, 132–33, 174, 211–12, 339–40, 357
 - process, 11–12, 173
 - data, 11–12, 18, 173
 - information, 11–12, 18, 173
 - knowledge, 11–12, 18, 173
 - wisdom, 11–12, 18, 173
- deep brain stimulation (DBS), 42
- deepfakes, 22, 156, 291, 300–306, 308–9, 336
- Defense Advanced Research Project Agency (DARPA), 10, 42, 53, 72, 107, 162, 165–66, 170, 186, 247, 309, 356
- disinformation, 74n12, 131, 295, 297, 299, 301–2, 304, 308, 317n34, 334
- dogfight, 94, 96–97, 99
- drones, xi, 2, 9–10, 20, 24, 30, 68, 123, 170, 213–17, 220, 237, 244, 247, 325, 357
- dual use, 8, 20, 45, 50, 53, 68–69, 72–73, 129, 132, 141n5, 171, 301, 330

- ethical, legal, and social implications (ELSI), 51–53, 181, 188–90
- ethics, ix, 17, 27, 43, 45–46, 48–50, 53, 55–57, 71, 74–75, 82, 126, 138, 192, 315, 324, 347
- evolution
 - of humans, 5–6, 62, 131, 152, 263–64
 - of Mind-Tech, 124–25, 163, 340
 - of warfare, ix, xiv, 8, 15–16, 81, 85–90, 117–18, 125, 127, 211, 219, 269, 340–41, 350
- experimentation, 20, 31, 70, 136–37, 181, 183–84, 189, 216, 219, 254, 256, 282–83, 327, 337

- first-person view (FPV) drones, 9–10, 20
- Fitts' Law, 181–82, 188
- fog of war, 4, 18, 29, 132, 238

- generative artificial intelligence (GenAI),
7–8, 12, 19, 22, 151, 153, 155–56,
158–61, 166–67, 169–70, 173–74,
228–29, 234, 236, 291, 293, 300–302,
306, 327, 331
- genomics, 13, 40
- human-machine
interface, ii, ix, xi, 1–3, 6–8, 10, 16,
19, 21, 23, 35, 61, 72, 127, 135,
151–55, 157–59, 161, 163, 171,
175, 182, 216, 218–19, 223–24,
236–37, 247, 281, 323, 326–27,
330, 356, 368
symbiosis/team, vii–viii, xi, 6–7, 9,
12–13, 29, 32–36, 82, 84–85, 91,
95, 99–100, 103–4, 107, 113–14,
117, 123, 134–37, 140, 144n36,
146n46, 153, 161–62, 211–12,
228–29, 243–44, 269, 357
- imagination in innovation, 117, 121–23,
329, 334–35
- information operations, 22, 88, 292–96,
301, 303, 305, 309–10, 312–15, 328,
346, 351
- intelligence, surveillance, and recon-
naissance (ISR), 30, 87, 211–12
- “intelligentized” warfare, 32, 133
- interface (see under human-machine
interface)
- Internet, 6, 61–62, 70–71, 84, 88, 168,
173, 228–30, 306, 336
- Internet of Things, 70, 170, 306
- investment(s), 17, 22, 69, 184, 205, 229,
243–45, 247–48, 250, 255–56, 262,
268–70, 282–85, 329, 334, 346, 348
- Joint All-Domain Command and Con-
trol (JADC2), 7, 10, 33, 326–27
- large language model (LLM), 96, 99,
156, 159–60, 173–75, 334–37, 339
- leader(s), vii–viii, 3, 7, 17, 31, 62, 65,
78–79, 92, 101, 103, 106, 121, 130,
181, 187, 189, 238, 247, 252, 255–57,
328
- machine learning (ML), 33, 40–43, 71,
133, 188, 190, 193–94, 204, 228, 306,
334–35
- malinformation, 67, 74n12
- mass personalization, 19, 22, 291, 305
- misinformation, 74n12, 83, 132, 237,
299, 308, 317n34
- Mosaic warfare, 10, 107–8, 110–11
- nanoengineering, 41
- narrow AI, 120–22, 138, 345
- neuroethics, 39, 43–45, 49, 53
- neuroscience, 2–3, 5, 17, 20, 22, 39, 42,
72, 261–62, 265, 267–69, 281–85
- OODA loop, 73, 91–94, 96, 99–100,
103–4, 106–7, 109–12, 128, 132, 138,
147, 234, 327
- pandemic, 43, 297, 313
- physiologic intelligence (PHYSIOINT),
20, 181–84, 186–90
- physiology sensors, 19–20, 183, 187–90,
197, 204
arousal, 157, 183
cognitive burden, 91–92, 99, 101,
103–4, 106, 120, 183–84
fatigue, 183–84, 267–68, 370
situational awareness, 10, 30, 65,
183–84, 200–202, 234–36
- politics, vii–viii, xiv, 4, 12, 32, 43–44,
47–48, 50–52, 65, 77–79, 87, 90, 130,
264, 292, 294–95, 303–4, 309–10,
312, 314, 324
- quantum
computing, 2–3, 13, 17–18, 61, 70,
81, 134, 140
revolution, 69–70
- sandboxes, 72–73, 166, 327–28
- substitution myth, 31
- technological readiness level (TRL), 51,
166, 326
- timeliness, xi, 51, 62, 64, 66, 353

- transcranial magnetic stimulation, 42
- trust
 - of new technology, xi–xiii, 9, 35, 71, 83, 88–89, 98–100, 146n46, 282–83
 - of team members, 262, 265–66, 268, 269–70, 283, 294
- uncertainty, 29, 93–94, 96–98, 100, 104, 110–12, 132, 134, 224, 229, 244, 246
- wearable sensing, 20, 181–83, 187, 189, 193–94, 197–99, 202–5, 224, 232, 245, 247
- will to fight, 243–44, 246–47, 250, 252–56, 262–65, 283–85, 323, 330
- World Wide Web, 62, 70

HUMAN, MACHINE, WAR

How the Mind-Tech Nexus Will
Win Future Wars

Military and strategic success depends not on minds or technology but on the combination of minds plus technology. We call this combination the *Mind-Tech Nexus*, which we define as how human factors (e.g., will to fight, skill, daring, perception) will interface and converge with the technologies of our time (e.g., digital, artificial intelligence, quantum computing, neuroscience) to help shape the character and the outcomes of competition.

This volume brings together world-leading scholars and practitioners to explore how minds and technology are being—and can be—harnessed for military and geostrategic power.

Forewords by

General James E. Rainey
*Commander, US Army
Futures Command*

Sir Lawrence Freedman
*Emeritus Professor of War
Studies, King's College London*



ISBN 9781585663347

