**Original**

body{font-family:sans-serif;line-height:1.8} h1,h2,h3,h4,h5,h6{margin:0.6em 0} p{margin:0.6em 0} ul,ol{margin:0.6em 1.2em} blockquote{border-inline-start:3px solid #ccc;padding-inline-start:0.8em;color:#444}

**Page 1**

editors  
Seth G. Jones and Seamus P. Daniels  
A REPORT OF THE CSIS DEFENSE AND SECURITY DEPARTMENT  
War and the Modern Battlefield  
Insights from Ukraine and the Middle East  
SEPTEMBER 2025

**Page 2**

SEPTEMBER 2025  
contributors  
Kari A. Bingen  
Daniel Byman  
Mark Cancian  
Eliot A. Cohen  
Cynthia R. Cook  
Seamus P. Daniels  
Hannah Freeman  
Emily Harding  
Benjamin Jensen  
Seth G. Jones  
Tom Karako  
Elizabeth Kos  
Aosheng Pusztaszeri  
Joseph Rodgers   
Clayton Swope  
Sofia Triana  
Heather Williams  
A REPORT OF THE CSIS DEFENSE AND SECURITY DEPARTMENT  
War and the Modern Battlefield  
Insights from Ukraine and the Middle East  
New York • London • Oxford • New Delhi • Sydney

**Page 3**

II  
A Report of the CSIS Defense and Security Department  
About CSIS  
The Center for Strategic and International Studies (CSIS) is a bipartisan,   
nonprofit policy research organization dedicated to advancing practical   
ideas to address the world’s greatest challenges.   
Thomas J. Pritzker was named chairman of the CSIS Board of Trustees   
in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962,   
CSIS is led by John J. Hamre, who has served as president and chief executive   
officer since 2000.   
CSIS’s purpose is to define the future of national security. We are guided   
by a distinct set of values—nonpartisanship, independent thought, innova­  
tive thinking, cross-disciplinary scholarship, integrity and professionalism,   
and talent development. CSIS’s values work in concert toward the goal of   
making real-world impact.   
CSIS scholars bring their policy expertise, judgment, and robust net­  
works to their research, analysis, and recommendations. We organize   
conferences, publish, lecture, and make media appearances that aim to   
increase the knowledge, awareness, and salience of policy issues with rele­  
vant stakeholders and the interested public.   
CSIS has impact when our research helps to inform the decisionmaking   
of key policymakers and the thinking of key influencers. We work toward a   
vision of a safer and more prosperous world.   
CSIS does not take specific policy positions; accordingly, all views   
expressed herein should be understood to be solely those of the author(s).  
© 2025 by the Center for Strategic and International Studies.   
All rights reserved.  
Acknowledgments  
The editors would like to express their gratitude to Phillip Meylan, Hunter   
Hallman, William Taylor, Kelsey Hartman, Gina Kim, Shannon Yeung, Leena   
Marte, Julia Huh, and other members of the CSIS publication team and iLab   
for their invaluable contributions in the compilation, editing, and design   
of this report.   
This report is made possible by general support to CSIS. No direct spon­  
sorship contributed to this report.  
Center for Strategic and International Studies  
1616 Rhode Island Avenue, NW  
Washington, DC 20036  
202-887-0200 | www.csis.org

**Page 4**

III  
War and the Modern Battlefield  
Bloomsbury Academic  
Bloomsbury Publishing Inc, 1385 Broadway, New York, NY 10018, USA   
Bloomsbury Publishing Plc, 50 Bedford Square, London, WC1B 3DP, UK   
Bloomsbury Publishing Ireland, 29 Earlsfort Terrace, Dublin 2, D02 AY28,   
Ireland   
BLOOMSBURY, BLOOMSBURY ACADEMIC and the Diana logo are trade­  
marks of Bloomsbury Publishing Plc   
First published in the United States of America, 2025  
Copyright © Center for Strategic and International Studies, 2025   
Cover design: William H. Taylor/CSIS   
Cover image © : Dmytro Sheremeta/Getty Images   
All rights reserved. No part of this publication may be: i) reproduced or   
transmitted in any form, electronic or mechanical, including photocopy­  
ing, recording or by means of any information storage or retrieval system   
without prior permission in writing from the publishers; or ii) used or   
reproduced in any way for the training, development or operation of   
artificial intelligence (AI) technologies, including generative AI technol­  
ogies. The rights holders expressly reserve this publication from the text   
and data mining exception as per Article 4(3) of the Digital Single Market   
Directive (EU) 2019/790.   
Bloomsbury Publishing Inc does not have any control over, or responsi­  
bility for, any third-party websites referred to or in this book. All internet   
addresses given in this book were correct at the time of going to press.   
The author and publisher regret any inconvenience caused if addresses   
have changed or sites have ceased to exist, but can accept no responsibil­  
ity for any such changes.   
ISBN: PB:   
979-8-7651-9851-3  
   
ePDF: 979-8-7651-9852-0  
   
ePub: 979-8-7651-9853-7  
Printed and bound in the United States of America   
For product safety related questions contact productsafety@bloomsbury.  
com.   
To find out more about our authors and books visit www.bloomsbury.  
com and sign up for our newsletters.

**Page 5**

IV  
A Report of the CSIS Defense and Security Department  
Contents  
Introduction: How to Think About Modern Warfare   
1  
Eliot A. Cohen  
PART I: STRATEGY, POLITICS, AND SOCIETY  
01 | Adversaries and the Future of Competition   
8  
Seth G. Jones  
02 | Will, Cohesion, Resilience, and the Wars of the Future   
18  
Daniel Byman  
03 | Returning to an Era of Competition and Nuclear Risk   
24  
Heather Williams, Joseph Rodgers, and Elizabeth Kos  
PART II: OPERATIONS, TACTICS, AND TECHNOLOGY  
04 | Operational Art in the Age of Battle Networks   
33  
Benjamin Jensen  
05 | The Evolution of Landpower   
42  
Benjamin Jensen  
06 | The Enduring Role of Fires on the Modern Battlefield   
51  
Tom Karako and Hannah Freeman  
07 | Intelligence in a Transparent World   
60  
Emily Harding  
08 | Extending the Battlespace to Space   
69  
Kari A. Bingen  
09 | Technological Evolution on the Battlefield   
81  
Aosheng Pusztaszeri and Emily Harding  
10 | The Evolution of Airpower   
91  
Clayton Swope  
11 | The Future of Seapower   
99  
Mark Cancian  
12 | The Evolution of Irregular Warfare   
108  
Daniel Byman, Seth G. Jones, and Sofia Triana  
PART III: IMPLICATIONS FOR DEFENSE PLANNING AND INDUSTRY  
13 | Defense Budgets in an Uncertain Security Environment   
117  
Seamus P. Daniels  
14 | Industrial Roadblocks: Producing at Scale and Adopting New   
Technologies   
128  
Cynthia R. Cook   
15 | Power Projection and the Logistics of Modern War   
135  
Cynthia R. Cook  
CONCLUSION  
The Next Offset: Winning the Fight Before It Starts   
145  
Seth G. Jones

**Page 6**

V  
War and the Modern Battlefield  
About the Contributors   
154  
Endnotes   
161

**Page 7**

1  
Eliot A. Cohen  
INTRODUCTION  
How to Think About   
Modern Warfare  
By Eliot A. Cohen  
O  
ne of the great imponderables is what war will look like when all   
the dimensions, new and old, are woven together—information   
operations, irregular warfare, cyberattacks, space warfare, and   
even conceivably biological and nuclear warfare.  
It is a long-standing habit of military historians to describe changes in   
warfare in terms of two biological paradigms: more or less steady evolu­  
tion on the one hand and punctuated equilibrium on the other.1 The messy   
truth is in between. Sometimes the practice of war—its art and science, the   
sources of military strength and weakness—advances by fits and starts, and   
sometimes it evolves at a steady pace.   
It is reasonable to assert that the world is at a junction at which war is   
changing rapidly and that the pure evolutionary model no longer suffices. A   
confluence of political, social, and technological changes have collectively   
made war something very different than the practitioners and theorists of the   
Cold War expected and understood. That is why this collection of studies is so   
important: There are very large changes underway which have to be under­  
stood from multiple perspectives and which resist simple characterization.   
The Cold War saw different forms of conflict: irregular wars, which   
characterized the end of the European empires and their sequels (as in   
Vietnam), and short, sharp conventional conflicts (as in the 1967, 1973, and   
1982 Arab-Israeli wars, the 1971 India-Pakistan War, or the China-Vietnam   
war of 1979). These wars could be very costly, with casualties in the tens of   
thousands and possibly more, but by and large they were relatively brief   
and contained.  
The conflicts occurring today in Ukraine and the Middle East have   
changed that paradigm. These have been two large and protracted wars,   
lasting not weeks or months but years. They have involved enormous   
damage to civilian infrastructure and opposed not individual actors but   
large coalitions of states assisting proxies or clients. Whereas the wars of   
the late twentieth century involved one-sided dominance of the air, in these   
wars, missiles, drones, and occasionally aircraft are able to penetrate deep   
into enemy territory. These wars are different.  
Through them, the United States and its allies have rediscovered some   
old truths—chief among them the importance of industrial production of end

**Page 8**

2  
How to Think About Modern Warfare  
items and munitions. In 2022, the United States’ entire monthly production   
of 155 mm artillery rounds amounted to only somewhat more than what   
Ukraine expended every day—and considerably less than Russia’s daily rate   
of use. European allies were even worse off. Even Russia, which had retained   
an industrial mobilization model for war production, has not been able to   
meet the demands of the Ukraine war and depended on poorer but indus­  
trially deeper clients, like North Korea and Iran, to make up the shortfalls.   
Similarly, the West has rediscovered the phenomenon of irregular—  
or as we now prefer to call it, hybrid—warfare. All wars, including the   
World Wars, have included the extensive use of propaganda, subversion,   
and proxy and guerrilla warfare. In no case were these factors sufficient   
to change the fundamental balance of power, but they played their part   
nonetheless. However, these elements are playing an increasing role in   
contemporary warfare.  
The nuclear dimension of strategy has also reappeared after a hiatus   
of more than a generation. While fears of nuclear proliferation helped trig­  
ger the Second Gulf War in 2003 and concerns about the North Korean   
and Iranian nuclear programs have been important in U.S. foreign policy,   
nuclear weapons played only a minor role in the strategic thinking of the   
United States and other large powers from the end of the Cold War through   
the 2020s. That is no longer the case. The rise of China’s nuclear arsenal   
is one reason for this: China had doubled its number of nuclear warheads   
in the last decade, and it looks to double them again by 2030. As a result,   
the United States now faces two potential nuclear opponents that equal or   
may even overmatch it. Even more troubling, the disruption of the United   
States’ European alliances brought about by the Trump administration may   
very well launch a cascade of proliferation that will reshape geopolitics, for   
example, if countries like Poland and Finland feel they can no longer trust   
a U.S. deterrent.  
There are, however, genuinely new developments in the techne of war.   
The widespread use of unmanned systems in the Ukraine war is a notable   
example. Some of the first drones appeared at the end of World War I—most   
notably the Kettering Bug—and they sporadically reappeared during World   
War II and in Vietnam. The first major use came in the 1982 Israel-Lebanon   
war. But the Russia-Ukraine war (like the Azeri-Armenian war of 2020) saw   
a massive development in drone warfare: a change in quantity that became   
a change in quality.  
From a few hundred unmanned aircraft systems (UASs) at the beginning   
of the war, Ukraine began deploying thousands, then tens of thousands of   
drones, and is now manufacturing millions annually. Russia, of course, fol­  
lowed suit. The pattern of ground combat changed, as a UAS-saturated bat­  
tlefield paralyzed vehicular movement, while an entire fleet—Russia’s Black   
Sea Fleet—has suffered greater than 30 percent losses and was stopped in   
its tracks by the attacks of unmanned surface and subsurface systems.2

**Page 9**

3  
Eliot A. Cohen  
Unmanned ground-based systems have also begun to appear, which will   
no doubt evolve and proliferate as well.  
The deployment of various forms of AI in a military context is also a gen­  
uine innovation that has become pervasive. Automatic target recognition   
and the processing of vast quantities of data has enabled Israel to conduct   
orders of magnitude more strikes in its wars with Hamas in Gaza and Hez­  
bollah in Lebanon than it could have otherwise. Not only does AI enable   
the unmanned systems revolution, but it has increasingly transformed tac­  
tical- and even operational-level decisionmaking, with consequences for   
the degree of human control of combat in all of its domains.  
It is reasonable to expect that soon enough even terrorist organizations   
will be able to launch swarms of drones that cooperate with each other to   
attack targets. Indeed, such a capability probably already exists. The use   
of sophisticated facial recognition and other targeting software means that   
the barriers to extensive assassination campaigns, once the prerogative only   
of the United States, will lessen. The planning and execution of long-range   
attacks enabled by AI will not completely level the playing field for war, but   
it will go a long way toward it.  
War is changing in other respects as well. It has expanded to new   
realms, chiefly space and cyberspace. Space-based systems first played an   
important role in the 1991 Gulf War, but the consequences were one-sided   
and largely confined to reconnaissance, navigation, and communications.   
However, the recent explosion in satellite numbers is remarkable. In 2015,   
there were about 1,400 active satellites in orbit; in 2025, there are over   
10,000, and the next decade may see that number quintupling.3 Already,   
all countries can make some use of space for communications, navigation,   
and reconnaissance whether or not they possess their own satellites. Fur­  
ther, the potential now exists for actual warfare in and from space, includ­  
ing kinetic and non-kinetic attacks on satellite systems and the delivery of   
kinetic weapons from space to Earth. Compounding this spread of space-  
based capabilities is the increased (if murky) interest of great powers in the   
use of space as an area of combat; the temptation of blinding an opponent,   
or delivering unanswerable strikes from outer space, may be too much to   
resist in the next war.  
Meanwhile, conflict in cyberspace is now constant—albeit with spikes at   
particular moments, such as during the first months of Russia’s invasion of   
Ukraine in 2022 or in the Russian attack on Estonia in 2007. What remains to   
be seen (but will almost surely occur) is the use of cyberattacks to conduct   
lethal forms of sabotage.  
For the United States, all of these changes come at a time when its stra­  
tegic predicament has become more global and multifaceted. Three large   
geopolitical challenges have emerged. The first of these is a coalition of hos­  
tile powers—China, Russia, Iran, and North Korea—that collude in several   
respects and have a common objective of bringing U.S. predominance to

**Page 10**

4  
How to Think About Modern Warfare  
an end. Their collaboration across multiple domains—like the deployment   
of North Korean troops and Iranian drones to fight Ukraine, the sharing of   
advanced military technology and production, cooperation in disinforma­  
tion campaigns, and probably sabotage operations against the West—is a   
challenge unparalleled since the early days of the Cold War.  
The second challenge, which results from both geopolitics and technol­  
ogy, is the return of the threat of global war. Particularly after the Cold War,   
the U.S. military got into the habit of thinking about war as a regional matter,   
chiefly in the Middle East. Even as China rose, the United States continued to   
mostly conceptualize the challenge as a regional one in the Indo-Pacific. But   
because of the size of China’s economy, the expanding nature of its forces,   
and the evolution of technology—as well as the emergence of the coalition   
described above—it is likely that a war with China would be global. Hyper­  
sonic missiles, space-based weapons, and long-range naval forces coupled   
with sabotage and covert action mean that even the U.S. mainland would   
be vulnerable for the first time since the nineteenth century.  
Most troubling of all, the United States is no longer the dominant power   
it once was. To be sure, its relative decline has been exaggerated: Its military   
remains large and capable, and its share of global economic production   
(roughly one quarter) has been stable over a generation. Its research and   
development base remains unequalled, and its basic material ingredients   
of national power—geographical position, natural resources, and economic   
and financial strength—are substantial.  
But with China, in particular, the United States faces a rival unlike any   
since Nazi Germany—and that confrontation occurred in a world where the   
next two leading powers, Great Britain and the Soviet Union, were U.S. allies.   
The Chinese economy is smaller than that of the United States, but not by an   
order of magnitude; increasingly, China’s technological capabilities are com­  
parable, and its manufacturing and shipbuilding base considerably superior.   
In such a world, the United States, with the many vulnerabilities created by   
its main source of strength—its open society—may be liable to receiving shat­  
tering surprises of a kind that have not occurred since Pearl Harbor.  
One of the great imponderables is what war will look like when all the   
dimensions, new and old, are woven together—information operations,   
irregular warfare, cyberattacks, space warfare, and even conceivably bio­  
logical and nuclear warfare. It would be unlike anything experienced before   
in scope and scale, even World War II.  
In the essays that follow, CSIS scholars consider many dimensions of the   
changing character of war. Throughout, it is important to consider not just   
technology, which may evolve at tremendous speed, but also the relation­  
ship between the technical means of war, the politics that underly conflict,   
and the psychology of those who must direct it.   
For example, historically it has been assumed that a large population of   
young people—and specifically young men—was essential for the waging of

**Page 11**

5  
Eliot A. Cohen  
war. It is reasonable to ask whether the vast proliferation of unmanned weap­  
ons systems, and the reversion of humans to their direction and control,   
reduces the significance of demographic disadvantage. Or consider how old   
modes of warfare waged with new techniques have different efficacy because   
of new conditions. At one level, information warfare is as old as war itself.   
Propaganda and disinformation played their roles in the eighteenth century   
as much as the twentieth. But in an age of fragmented media, deepfakes, and   
bots, they may have a significantly different and possibly larger role to play.   
Finally, technology will affect how political and military leaders—whose   
essential human characteristics, after all, have not evolved—direct war.   
Since the middle of the nineteenth century, modern technology has made   
it ever easier for leaders to exercise direct supervision and control over   
forces on the battlefield. Yet the nature of war remains: chaos and confusion   
are generated (as Clausewitz pointed out) not by the physical smoke over   
the battlefield but by the pressures it generates. There is no guarantee that   
new technologies will improve the quality of wartime leadership. Indeed,   
they may actually serve to weaken it.  
In sum, the world of war that may emerge in the remaining three-quar­  
ters of the twenty-first century is more extensive, less comprehensible, and   
possibly even more devastating than anything humanity has ever known.   
That alone should be enough to compel its study with the utmost care—and   
to that end, these essays are an excellent beginning.  
Outline of the Report  
This report is divided into three primary sections. The first addresses the   
implications of the conflicts in Ukraine and the Middle East on war at the   
strategic, political, and societal levels. Chapter 1 argues that there is likely   
to be a deepening of relations going forward among U.S. competitors and   
adversaries. Chapter 2 demonstrates that societal resilience is a critical and   
integrated aspect of national security, which strategic planners should not   
relegate to a secondary consideration. And modern warfare for allies and   
adversaries alike will increasingly rely on nuclear weapons, as Chapter 3   
articulates.  
The second section of the report assesses the future of warfare in oper­  
ations, tactics, and technology, addressing the implications of the current   
wars on particular domains and capability areas. Chapter 4 provides an   
overview of the impact of battle networks on operations before Chapter 5   
highlights the continued significance of landpower in war. Chapter 6 argues   
that the experiences in Ukraine and the Middle East show that reigns of fire   
will endure, as offensive and defensive fires remain critical to combined   
operations. Technological advances, massive data analysis, and open-  
source intelligence have changed the world of intelligence and spycraft, as   
depicted in Chapter 7, but they have also contributed to a blurring of lines   
between state, industry, and academic actors.

**Page 12**

6  
How to Think About Modern Warfare  
Chapter 8 argues that the war in Ukraine has been a turning point in the   
role of space in warfare, demonstrating how space capabilities can create an   
advantage over a more capable military power. Other emerging technologies   
will push future conflicts into a competition of who can evolve and innovate   
more quickly, according to Chapter 9. This may be particularly true in the   
air domain, where Chapter 10 argues that AI-enabled decisionmaking will   
play an increasingly important role in a challenging environment shaped   
by increasingly sophisticated and diverse sensors. In the naval domain,   
Chapter 11 identifies that the Ukraine and Middle East wars, despite being   
predominantly land campaigns, yield some notable insights for current   
action, including expanding munitions inventories, accelerating uncrewed   
systems, and hedging on major surface combatants. Chapter 12 argues that   
the ongoing wars demonstrate that irregular warfare is not a relic of the past   
but a defining feature of contemporary conflict.  
The third section of the report addresses implications for defense bud­  
gets, logistics, and acquisition. Chapter 13 discusses the growth in global   
defense spending among allies and competitors and trends in procurement   
patterns. Chapter 14 argues that logistics is more critically important today   
than in the past, and Chapter 15 addresses how industry must evolve given   
the acquisition patterns in conflicts in Ukraine and the Middle East. The   
report concludes by discussing how prepared the United States is for com­  
petition, deterrence, and warfare in this new era of conflict.

**Page 13**

PART I  
Strategy, Politics,   
and Society

**Page 14**

CHAPTER 01  
Adversaries and the   
Future of Competition  
Seth G. Jones

**Page 15**

9  
Seth G. Jones  
”  
“  
China, Russia, Iran, and North Korea are   
most likely headed toward deepening   
bilateral relations . . . which has significant   
implications for the future of warfare.  
T  
his chapter examines cooperation between   
China, Russia, Iran, and North Korea.1 It asks   
several questions: How has cooperation   
evolved between China, Russia, Iran, North Korea,   
and other actors, including during the Ukraine war?   
How might cooperation evolve over the next three   
to five years? What are the implications for modern   
warfare?   
This chapter outlines three possible security   
arrangements between China, Russia, Iran, and   
North Korea: (1) weakening engagement, (2) deepen­  
ing bilateral relations, or (3) a multilateral alliance.   
Under weakening engagement, cooperation between   
one or more of these axis members wanes because   
of divisions and diverging interests. There is greater   
infighting among countries and a decline in the over­  
all degree of cooperation. Under deepening bilateral   
relations, cooperation between the axis countries   
increases in such areas as the defense industrial   
base, though cooperation remains largely bilateral.   
Under a multilateral alliance, axis countries establish   
multilateral arrangements that include higher levels   
of cooperation, such as a multilateral treaty or other   
agreement that commits three or more signers to col­  
lective assistance in case of external attack.   
This chapter concludes that China, Russia, Iran,   
and North Korea are most likely headed toward deep­  
ening bilateral relations. This arrangement would   
involve axis countries increasing military and dual-use   
exports and imports, expanding the scale and scope   
of bilateral and, potentially, multilateral exercises and   
training, deepening defense industrial cooperation,   
establishing bilateral treaties or pacts that commit the   
signatories to greater military cooperation and even   
mutual defense in case of attack, and deploying sol­  
diers to fight in the wars of other axis countries.   
There are still likely to be areas of disagreement   
and tension between these countries, as well as limits   
to their cooperation. But the overall trend is likely to   
be greater cooperation, which has significant impli­  
cations for the future of warfare. For example, closer   
cooperation increases the possibility of inter-theater   
photo: sergei guneyev/pool/afp/getty images

**Page 16**

10  
Adversaries and the Future of Competition  
North Korea both seek to circumvent international   
sanctions, are desperate for outside investment, and   
desire both great power diplomatic protection and   
military aid in the event of a conflict with the United   
States or their pro-U.S. neighbors, such as Israel and   
South Korea, respectively.   
Beginning in 2022, China provided substantial   
aid to Russia’s full-scale war in Ukraine, including   
tooling machines, semiconductors, microelectron­  
ics for use in Russian weapons systems, spare parts,   
drones, gunpowder, and military contractors. Chi­  
nese companies such as Xiamen Limbach helped   
design and develop Russia’s Garpiya series long-range   
attack unmanned aircraft system, in collaboration   
with Russian defense firms like Joint Stock Company   
Aerospace Defense Concern Almaz-Antey.5 China also   
provided satellite imagery analysis and aid to improve   
Russian satellite and other space-based capabilities   
for use in Ukraine.6 Chinese companies even pro­  
vided cotton cellulose, nitrocellulose, and critical   
ingredients for nitrocellulose (such as cotton pulp),   
which are explosive precursors that the Russian mili­  
tary uses to produce gunpowder, rocket propellants,   
and other explosives.7  
This list of Chinese aid likely excludes many sys­  
tems and components that are shipped clandestinely   
and whose status is not reported. China has apparently   
used cargo ships, trains, trucks, and aircraft to send   
material to Russia.8 Several Chinese-based companies,   
such as Poly Technologies, Fujian Nanan Baofeng Elec­  
tronic Company, China Taly Aviation Technologies   
Corporation, Juhang Aviation Technology Shenzhen,   
Finder Technology Limited, Tulun International Hold­  
ing Limited, and many others, have likely exported   
material.9 Although vital to Russia, some of the Chi­  
nese material, such as chips, is of low quality com­  
pared with more advanced chips from the United   
States, Europe, Japan, South Korea, and Taiwan.  
Iran has exported drones to Russia, as well as artil­  
lery shells, ammunition, and short-range ballistic mis­  
siles.10 Russia and Iran have strengthened industrial   
base ties and set up production of Iranian drones—  
especially the Shahed-136—in Russia’s Tatarstan   
region.11 Russia has supplied Iran with Su-35 multi­  
role fighter jets and other weapons systems, as well   
military aid among axis countries in case of war and   
raises the prospect that two or more major wars could   
occur simultaneously in different theaters. It is pru­  
dent for such countries as the United States to be pre­  
pared to fight two wars at the same time, rather than   
focus on one region such as the Indo-Pacific.  
The rest of this chapter is divided into three sec­  
tions. The first provides an overview of lessons from   
Ukraine and the Middle East regarding axis coopera­  
tion. The second examines the possible evolution of   
the axis. And the third outlines possible indications   
and warnings to help gauge whether cooperation   
between axis countries is strengthening or weakening.  
Lessons from Ukraine   
and Other Wars  
Security cooperation between two or more powers is   
a routine occurrence in international politics. China,   
Russia, Iran, and North Korea see aspects of the West­  
ern-led liberal order as a set of rules designed to ben­  
efit the United States and its allies while forestalling   
potential rivals. In addition, these countries believe   
U.S. and allied efforts to promote democracy, support   
a free and independent press, maintain a free market,   
and encourage the free flow of ideas directly conflict   
with their goals of regime stability.2 All four powers   
are also revanchist. As the historian Philip Zelikow   
argued, they are “fundamentally revisionist powers.   
Their leaders regard themselves as men of destiny,   
with values and historical perspectives quite differ­  
ent from the consumerist or social metrics that suf­  
fuse much of the world.” He continued that they “all   
feel boxed in by extensions of American power they   
regard as fragile, though formidable in parts. All have   
long been preparing for a great reckoning.”3   
In addition, each country has its own reasons for   
pursuing cooperation. China likely wants partners to   
help achieve what Chinese leader Xi Jinping called   
the “great rejuvenation of the Chinese nation.”4 China   
needs access to critical minerals, bases, ports, and   
markets. Russia has needed assistance following its   
February 2022 full-scale invasion of Ukraine to keep   
its economy afloat, energize its defense industrial   
base, and ensure it can continue waging war. Iran and

**Page 17**

11  
Seth G. Jones  
Despite these examples of cooperation, there   
have been some limitations. Chinese leaders have   
expressed concern about Russia’s warming military   
relations with an erratic North Korea, including the   
strengthening of Pyongyang’s missile capabilities.15   
Beijing has generally been reluctant to help Pyong­  
yang with its nuclear program.16 Iranian leaders have   
expressed dismay with Russia and China for their   
diplomatic positions in a spat between Iran and the   
United Arab Emirates over the sovereignty of islands   
in the Persian Gulf—including Greater Tunb, Lesser   
Tunb, and Abu Musa—which dominate the approach   
to the strategic Strait of Hormuz.17 During Iran and   
Israel’s 12-day war in June 2025, China, Russia, and   
as aid to Iran’s space and missile programs.12 Finally,   
North Korea has provided artillery rounds (including   
152 mm and 122 mm), multiple launch rocket systems,   
KN-23 and KN-24 solid-propellant short-range ballis­  
tic missiles, soldiers, and other defense materiel to   
Russia.13 Table 1.1 provides an overview of some types   
of military cooperation between China, Russia, Iran,   
and North Korea.  
Not all cooperation has centered on the Ukraine   
war. Chinese and Russian companies and agencies   
have also provided weapons components and intel­  
ligence (including satellite imagery) to Iran and the   
Houthis, an ally of Iran that conducted strikes against   
U.S. warships in the Red Sea and Israel.14   
Table 1.1: Security Cooperation Between China, Russia, Iran, and North Korea  
Country  
Imports to Russia  
Exports from Russia  
China  
•   
Navigation equipment for M-17 military transport helicopters  
•   
Machine tools for ballistic missiles and other weapons systems  
•   
Parts for fighter jets  
•   
Antennae for military vehicles used for communication jamming  
•   
Drones, drone parts, and engines for drones and cruise missiles  
•   
Optical components for Russian tanks and armored vehicles  
•   
Military helmets and body armor  
•   
Global navigation satellite system boards for Russian attack drones  
•   
Electronic integrated circuits for Russian drones, infrared   
detectors, communications equipment, and pressure sensors and   
microcontrollers used in Russian missile systems and drones  
•   
Satellite imagery analysis and aid to improve Russian satellite and   
other space-based capabilities for use in Ukraine  
•   
Cotton cellulose, nitrocellulose, and critical ingredients for   
nitrocellulose (such as cotton pulp), which are used to produce   
gunpowder, rocket propellants, and other explosives  
•   
Aircraft engines   
•   
Helicopter systems   
•   
Space and   
counterspace cooperation  
Iran  
•   
Shahed-136 (Geran-2), Shahed-131 (Geran-1), Mohajer-6, and possibly   
Shahed-101 and Shahed-107 drones   
•   
Drone production facilities   
•   
Artillery shells   
•   
Ammunition   
•   
Fateh-110 short-range ballistic missiles  
•   
Fath-360 (BM-120) short-range ballistic missiles  
•   
Yak-130 pilot training aircraft   
•   
Su-35 multirole fighter jets   
•   
Mi-28 attack helicopters   
•   
Space cooperation   
North Korea  
•   
Artillery rounds (including 152 mm and 122 mm)   
•   
Rockets   
•   
KN-23 and KN-24 short-range ballistic missiles   
•   
Other munitions and components for munitions  
•   
Soldiers to fight in the Ukraine war  
•   
Technology for satellites   
•   
Technology for nuclear-  
powered submarines   
•   
Technology for ballistic   
missiles   
Source: CSIS analysis.

**Page 18**

12  
Adversaries and the Future of Competition  
saries likely pose a greater threat; and the assessed   
intentions of the adversary country or alliance, which   
could vary from benign to malign intentions.18 Second   
is the level of ideological solidarity, including shared   
political, cultural, or other traits or interests.19 The   
more interests countries share in common, the like­  
lier they are to want to cooperate.20 Third is domestic   
politics, including the preferences and decisions of   
leaders.21 Regime change—including the death of a   
leader—could impact the degree of cooperation and   
the type of security arrangement. Alternatively, lead­  
ers could develop stronger bonds that increase the   
prospect for cooperation.  
Table 1.2 provides an overview of the three possi­  
ble security arrangements: weakening engagement,   
deepening bilateral relations, and a multilateral alli­  
ance. These possibilities are not meant to be exhaus­  
North Korea did not provide substantial aid to Iran as   
Israel and the United States gained air dominance and   
struck targets across the country. China and Russia   
issued pro forma denunciations of U.S. actions, but   
they did not provide significant military assistance.  
Future Evolution of the Axis  
Several factors are likely to impact the type of security   
arrangement among the axis countries in the future.   
First is the degree of common threat. Since countries   
tend to increase cooperation to prevent stronger   
powers from dominating them, axis countries facing   
a growing external power or threat will likely increase   
security cooperation. The severity of the threat could   
be affected by the military power of an adversary   
country or alliance, including its offensive military   
capabilities; geographic proximity, since closer adver­  
Table 1.2: Overview of Axis Security Cooperation  
Security   
Arrangement  
Summary  
Type of   
Arrangement  
Examples of Security Cooperation  
Weakening   
engagement  
Security cooperation   
weakens between   
axis countries.  
Bilateral  
•   
Limited exports and imports of military and dual-use items  
•   
Joint exercises and training  
Deepening   
bilateral relations  
Cooperation   
deepens, though   
remains largely   
bilateral.  
Bilateral  
•   
Increase in exports and imports of military and dual-use   
items  
•   
Growth in the scale and scope of joint exercises and   
training  
•   
Rise in bilateral defense industrial cooperation, including   
codevelopment, coproduction, and co-sustainment of key   
weapons components and systems; joint ventures; and   
mergers and acquisitions  
•   
Creation or deepening of bilateral treaties or other   
agreements that commit signers to collective assistance   
in case of external attack  
•   
Deployment of soldiers to fight in wars with other axis   
members  
Multilateral   
alliance  
Cooperation deepens   
and becomes   
multilateral.  
Multilateral  
•   
Notable growth in multilateral joint exercises and training,   
especially for a joint or multifront war  
•   
Significant rise in defense industrial cooperation across   
three or more countries  
•   
Creation of a multilateral treaty or other agreement that   
commits signers to collective assistance in case of   
external attack  
•   
Establishment of a multilateral military structure that   
includes a military committee, develops joint war plans,   
and includes other committees to cooperate at the   
strategic, operational, and tactical levels  
Source: CSIS analysis.

**Page 19**

13  
Seth G. Jones  
military, economic, and technological power, though   
relations between Beijing and Moscow are likely the   
core of the axis. Overall, axis countries continue to   
develop closer bilateral ties in defense industrial pro­  
duction, including emerging technologies that have   
significant military capability, such as AI and quan­  
tum computing. A deepening coalition could include   
growing cooperation in several areas.  
Arms exports and imports among axis countries   
continue under deepening bilateral relations, but   
they increase in scale and scope. Axis countries also   
expand arms sales to the Global South, continuing   
recent trends. Between 2020 and 2024, for exam­  
ple, the main suppliers of arms to Africa were Russia   
(which accounted for 21 percent of total African   
imports of major arms) and China (18 percent).24  
Axis countries might broaden the scope, fre­  
quency, and geographic location of exercises and   
training missions to improve joint warfighting, intel­  
ligence sharing, command and control arrangements,   
and interoperability. Between January 2019 and July   
2025, China and Russia conducted nearly a dozen   
combined strategic aerial patrols, including with   
Russian Tu-95 and Chinese H-6N and H-6K bombers   
capable of carrying nuclear weapons.25 These patrols   
could increase in number and geographic scope,   
including in the western Pacific and off the U.S. coast.   
While many of these exercises and training missions   
could be bilateral, there might also be an increase in   
multilateral exercises and training missions. In March   
2025, for example, Iran, Russia, and China conducted   
a joint naval exercise—called Marine Security Belt   
2025—in the Gulf of Oman, marking the fifth year of   
joint drills.26 Several other countries, including Azer­  
tive but rather serve to illustrate plausible future   
security arrangements.   
Weakening Engagement  
In this scenario, bilateral relations between China,   
Russia, Iran, and North Korea become more tenuous,   
though axis countries might continue to cooperate   
in some form. This scenario assumes a weakening of   
bilateral security arrangements and declining levels   
of cooperation. Examples include decreasing exports   
and imports of military and dual-use items, as well   
as conducting joint exercises and training that are   
more symbolic than substantive. There are already   
periodic disagreements between the countries that   
could worsen over time.22   
In sum, weakening engagement would include a   
general fraying of military and security ties between   
axis countries. Several factors could lead to such an   
outcome. First is a declining threat environment,   
which would reduce the need for aggregating power.23   
The end of the war in Ukraine or between Israel and   
Iran (including Iranian-linked groups), a substan­  
tial weakening of NATO, or a significant decrease in   
defense spending among major powers in Europe   
or Asia could weaken the impetus for cooperation   
by decreasing the threat. A second factor is fraying   
common interests. Examples include growing divi­  
sions on such issues as territorial disputes (such as a   
flaring up of Sino-Soviet border disputes or the sov­  
ereignty of islands in the Persian Gulf), diplomatic   
détentes that create fissures, and even warming   
relations between some axis countries that threaten   
others (such as between Russia and North Korea,   
raising concerns in China). Third, domestic chal­  
lenges could weaken bilateral relations. The death   
or removal of a leader—including Xi Jinping, Russian   
President Vladimir Putin, Iranian Supreme Leader   
Ayatollah Ali Khamenei, or North Korean leader Kim   
Jong Un—could lead to a shift in foreign policy and a   
decision to decrease axis cooperation.   
Deepening Bilateral Relations  
Under deepening bilateral relations, cooperation   
between axis countries increases. The anchor of the   
relationship is likely Beijing because of its size and   
The anchor of the relationship is likely   
Beijing because of its size and military,   
economic, and technological power,   
though relations between Beijing and   
Moscow are likely the core of the axis.

**Page 20**

14  
Adversaries and the Future of Competition  
Finally, a deepening coalition could include   
increased combat assistance—including the deploy­  
ment of soldiers—to other axis members engaged in   
wars. There have already been several examples.   
China, Iran, and North Korea have provided military   
assistance to Russia for its war against Ukraine. In   
late 2024, North Korea sent approximately 12,000   
combat forces to Russia’s Kursk Oblast, where   
Ukraine seized Russian territory. In early 2025, North   
Korea deployed roughly 3,000 additional soldiers for   
combat against Ukrainian forces.32 Future examples   
could include growing Chinese and Russian security   
and intelligence assistance to Iran and its partner   
forces in the Middle East, Russian and Chinese aid   
to North Korea in a conflict on the Korean Peninsula,   
or Russian and North Korean assistance to China in   
a conflict in the Taiwan Strait, South China Sea, or   
East China Sea.  
Several factors could lead to deepening bilateral   
relations. First is an increased threat, such as an arms   
race with the United States, European countries, or   
Asian countries such as Australia, Japan, and South   
Korea. Significant increases in defense spending and   
potential offensive capabilities—such as fifth- and   
sixth-generation aircraft, nuclear weapons, bomb­  
ers, submarines, and ballistic, cruise, and hyper­  
sonic missiles by the United States, Europe, and   
Asian countries—could increase the threat percep­  
tion in Beijing, Moscow, Tehran, and Pyongyang. An   
escalating conflict in the Middle East, a protracted   
war in Ukraine, or an escalating crisis in the South   
China Sea, East China Sea, or Taiwan Strait could   
also increase the perception of threat among axis   
countries. A second factor is growing common inter­  
ests, including those against the West. As Stephen   
Hadley, President George W. Bush’s national security   
adviser, wrote, “There is a shared anti-Westernism,   
opposition to democracy, and embrace of authori­  
tarian alternatives. What truly binds the axis is not   
ideology but a common opposition to U.S. power and   
the international system it sustains.”33 Third is the   
persistence or deepening of strong ties between axis   
leaders. Most significant would be a deepening of   
ties between Xi and Putin, whose relationship could   
serve as the lynchpin of axis relations.  
baijan, Iraq, Kazakhstan, Oman, Pakistan, Qatar, Sri   
Lanka, South Africa, and the United Arab Emirates,   
observed the exercise.  
In addition, axis countries could deepen bilateral   
defense industrial base cooperation. A modern-day   
defense industrial base involves the production of   
defense and dual-use items by commercial compa­  
nies and state-owned enterprises across multiple   
domains. Key domains include maritime, air, ground,   
space, cyber, and nuclear. Axis countries could   
increase cooperation in areas such as unmanned   
and autonomous platforms, integrated air and mis­  
sile defense, space and counterspace, submarines,   
missiles, and emerging technologies such as AI and   
quantum.27 Cooperation could take several forms:   
the codevelopment, coproduction, and co-sustain­  
ment of weapons systems or components involving   
industrial firms from two or more axis countries, joint   
ventures, or transnational mergers and acquisitions.   
Next, axis countries could increase their commit­  
ment to defend each other in case of external attack   
through a deeper bilateral treaty or other agreement   
that commits signers to collective assistance. The   
most important relationship is likely between China   
and Russia, which agreed to a “no limits” friendship   
in February 2022 and reaffirmed it in February 2025.28   
Chinese-Russian relations could deepen if their lead­  
ership committed to collective assistance in the case of   
an armed attack. In addition, bilateral relations have   
strengthened between other axis countries, except   
Iran and North Korea, which do not have a formal   
alliance. In March 2021, for example, China and Iran   
agreed to a 25-year strategic partnership, which   
included Chinese investment in Iran and imports of   
discounted Iranian oil to China.29 In June 2024, Russia   
and North Korea signed the Treaty on Comprehensive   
Strategic Partnership, which commits the countries   
to mutual military and other assistance if the other   
is invaded.30 In January 2025, Russia and Iran signed   
a 20-year pact that formalized close ties between the   
two countries.31 However, the pact did not constitute   
a military alliance and required no direct obligations   
from either party. Overall, a future development that   
deepens bilateral relations would likely involve build­  
ing and expanding these commitments.

**Page 21**

15  
Seth G. Jones  
could push for greater multilateral collaboration to   
aggregate power among axis countries.  
Conclusion  
The most likely future security arrangement is deep­  
ening bilateral relations. Under this arrangement,   
axis countries might increase military and dual-use   
exports and imports, expand the scale and scope of   
bilateral and potentially multilateral exercises and   
training, integrate defense industrial cooperation,   
deepen bilateral treaties or pacts that commit the   
signatories to greater military cooperation and even   
mutual defense in case of attack, and deploy soldiers   
to fight in the wars of other axis countries. This sce­  
nario is likely for several reasons.  
First, the degree of common threat is likely to   
increase. European and Asian countries—such as   
France, Germany, Japan, and South Korea—are likely   
to raise defense spending and strengthen their defense   
industrial bases. Defense spending is rising among   
these countries and across the globe more broadly,   
with global defense spending increasing from $2.23   
trillion in 2023 to $2.46 trillion in 2024.37 Defense bud­  
gets across the European Union are likely to rise by as   
much as $84 billion by 2027, equivalent to approxi­  
mately 0.5 percent of GDP.38 In June 2025, NATO Sec­  
retary General Mark Rutte called for a 400 percent   
increase in Europe’s air and missile defense budget.39   
Defense budgets in Asia are also rising. As one analy­  
sis concluded, “strategic drivers—such as China’s mili­  
tary modernization and increasing assertiveness, and   
North Korea’s advancing nuclear weapons program—  
galvanize threat perceptions in the region.”40  
Consequently, an arms race is more likely than   
a détente. In addition, war involving Russia is likely   
to continue in Eastern Europe, and conflict is likely   
to persist between Israel and Iran (including Iranian   
partners) in the Middle East, with China and Russia   
providing some assistance to Iran and its partners.   
Further, there is a significant risk of conflict in the   
Taiwan Strait, South China Sea, and Korean Penin­  
sula. Consequently, security competition between   
axis countries and democratic countries in Europe,   
Asia, and the Middle East is likely to remain significant   
and could increase in intensity.   
Multilateral Alliance  
A final scenario is a multilateral alliance. In this case,   
axis countries begin to establish multilateral arrange­  
ments and include high levels of cooperation, such   
as an agreement that commits signers to collective   
assistance in case of external attack.34 A multilateral   
alliance would likely involve strengthened relations in   
several areas, such as multilateral joint exercises and   
training and integrated defense industrial coopera­  
tion across three or more countries. There would be   
several differences from previous scenarios.  
Axis countries could establish a multilateral   
arrangement—such as a treaty, defense pact, nonag­  
gression pact, entente, or other agreement—commit­  
ting signers to collective assistance in case of external   
attack or other types of arrangements. The agreement   
could be overt or covert. Historical examples include   
the Treaty of the Holy Alliance of 1815 between Austria,   
Prussia, and Russia; the Atlantic Charter of 1941, which   
established NATO; and the Warsaw Pact during the   
Cold War, which included the Soviet Union and Soviet   
satellite countries in Eastern Europe.35 Axis countries   
could also establish a multilateral military structure   
that includes a military committee, joint war plans,   
and other committees to cooperate at the strategic,   
operational, and tactical levels. The Warsaw Pact had   
a unified command under Soviet leadership. The com­  
mand structure included a Combined Armed Forces   
Command, located in Moscow, which comprised mil­  
itary officers from all the Warsaw Pact countries.36   
Several factors could lead to a multilateral alli­  
ance. The first is a major increase in the nature or   
scope of the threat, such as the outbreak of war   
between an axis member and the United States, Japan,   
Taiwan, South Korea, or one or more European coun­  
tries. Another cause could be nuclear proliferation   
to South Korea, Japan, Poland, or another country,   
which could increase the perception of threat in one   
or more axis members. A second factor is growing   
ideological solidarity or other common interests   
between axis countries. Third is domestic politics.   
Regime change in one or more axis countries could   
bring to power a leader who is willing to expand axis   
cooperation for their own interests. Strong, ambi­  
tious, and expansionist leaders in Beijing or Moscow

**Page 22**

16  
Adversaries and the Future of Competition  
•   
Arms Exports and Imports: Is there an   
increase or decrease in exports and imports   
of military and dual-use items between axis   
countries? Are axis countries shipping more or   
fewer military and dual-use items by ship, rail,   
truck, or air? Is the scope of trade expanding or   
shrinking, including in sensitive areas such as   
nuclear weapons, space, stealth, hypersonics,   
quantum, and emerging technology?  
•   
Joint Exercises and Training: Are exercises   
and training efforts primarily bilateral or mul­  
tilateral? Do exercises and training efforts pre­  
pare for large-scale combat against the United   
States and European and Asian countries,   
including across land, air, maritime, space, and   
cyber domains? Do they include closer com­  
mand and control arrangements and sensitive   
intelligence sharing?  
•   
Defense Industrial Base: Is there an increase   
or decrease in bilateral or multilateral defense   
industrial cooperation between axis companies   
and state-owned enterprises, including codevel­  
opment, coproduction, co-sustainment, joint   
ventures, and mergers and acquisitions? If there   
is greater cooperation, in what areas is it occur­  
ring? And what is the scope of cooperation?   
•   
Treaties and Defense Pacts: Do axis countries   
create or deepen bilateral or multilateral trea­  
ties or other agreements that commit signers to   
collective assistance in case of external attack?   
Or is there a weakening of commitments? Are   
agreements formal or informal? Are they overt   
or covert? Are there indications of warming or   
cooling relationships between the leaders of   
axis countries?  
•   
Military Aid During War: Do countries pro­  
vide military assistance—such as weapons,   
troops, and intelligence—to other axis countries   
during wars? Or do they refrain from providing   
aid, especially for short wars? What types of aid   
are they willing to provide? Are axis countries   
willing to shed blood for each other, including   
through combat deployments?  
•   
Military Structure: Do axis countries estab­  
lish a military organizational structure, develop   
Second, there is likely to be a deepening of   
common interests between axis countries, which   
aim to undermine democracy and increase their   
power and influence in multilateral institutions such   
as the United Nations and other international and   
regional institutions.41 A particular focus may be bal­  
ancing against what they view as U.S. imperialism or   
hegemony.   
Third, domestic factors will likely increase secu­  
rity cooperation among axis countries. Whereas   
Khamenei’s health has been the subject of specu­  
lation, Xi and Putin—the lynchpins of the axis—are   
unlikely to step down in the next three to five years,   
and their relationship has strengthened, not weak­  
ened.42 There is also little evidence that Putin will   
curb his revanchist interests in Ukraine or other   
areas, such as Eastern Europe, Central Asia, the   
Middle East, and Africa; that Iran will walk away   
from its partners and proxies in the Middle East; or   
that Xi will curb his expansionist ambitions in Asia   
and other areas.  
Growing collaboration between axis countries   
would have significant implications for the future of   
warfare. For example, cooperation could increase the   
possibility of multi-theater war. Would Russia take   
advantage of a U.S.-China war in the Taiwan Strait   
or South China Sea to move into the Baltics or other   
regions? Would China or Russia take advantage of a   
war in the Korean Peninsula that pulls in North Korea,   
South Korea, the United States, and other countries?   
Between World War II and 2012, the United States   
sized its military to fight two wars at the same time.43   
But that changed with the Defense Strategic Guidance,   
which altered the two-war standard to “secur[ing] ter­  
ritory and populations and facilitat[ing] a transition   
to stable governance” in one region, while “denying   
the objectives of––or imposing unacceptable costs   
on––an opportunistic aggressor in a second region.”44   
However, this force construct is likely inadequate for   
tomorrow’s challenges that could require fighting two   
wars simultaneously.  
Looking forward, there are several indications   
and warnings that could provide clues to the future   
evolution of the axis and the implications for the   
future of warfare:

**Page 23**

17  
Seth G. Jones  
countries? How serious are the differences and   
in what areas?  
Answers to these questions will provide useful   
and timely indicators of the strength or weakness of   
axis relations. They will also have significant implica­  
tions for the future of warfare, including the possibil­  
ity of multi-theater wars involving more than one axis   
country. Growing cooperation increases the possibil­  
ity that a war with one axis country could expand to   
multiple fronts, causing simultaneous demands for   
such countries as the United States.   
joint war plans, or create other types of coop­  
erative arrangements at the strategic, opera­  
tional, or tactical levels? Or is there insufficient   
trust or interest to establish a multilateral mil­  
itary structure?  
In addition, there are several indications and   
warnings that might cause axis relations to strengthen   
or weaken:  
•   
Arms Buildup: Is there an arms race, includ­  
ing a significant increase in defense spending,   
between axis countries and their competitors in   
Europe, Asia, and the United States? Are coun­  
tries building offensive military capabilities?  
•   
Nuclear Proliferation: Is there a proliferation   
of nuclear weapons, including in such coun­  
tries as South Korea, Japan, and even Iran? Or   
do potential nuclear states refrain from build­  
ing nuclear weapons?  
•   
War: Does war persist in Europe and the Middle   
East? Is there a new outbreak of war involving   
an axis country? Is there an end to a major   
war, such as a ceasefire or peace agreement in   
Ukraine? Is there a major decrease in the inten­  
sity of conflict, such as between Israel and Iran   
(including Iranian partners and proxies)?  
•   
Regime Change: Is there a change in leader­  
ship in one or more axis countries? Is a new   
leader more or less inclined to strengthen axis   
relations or to expand territory? Or is there   
continuity of leadership in core axis countries,   
especially China and Russia?  
•   
Domestic Instability: Is there significant   
domestic economic, social, or political insta­  
bility in one or more axis countries that could   
impact axis relations? Or is there relative stabil­  
ity within axis countries?  
•   
Future of Security Institutions: Does NATO   
grow stronger or weaker over the next three to   
five years? Is there a deepening of security ties—  
including a multilateral security institution—  
between the United States and countries in Asia   
such as Australia, Japan, and South Korea?  
•   
Divisions and Fissures: Are there increases   
or decreases in policy fissures between axis

**Page 24**

CHAPTER 02  
Will, Cohesion, Resilience,   
and the Wars of the Future  
Daniel Byman

**Page 25**

19  
Daniel Byman  
”  
“  
Societal resilience is vital for countries to   
stand up to aggression; when it is strong,   
it enhances deterrence. In future conflicts,   
aggressors such as China and Russia are   
likely to try to undermine resilience   
as an alternative or prelude to war.  
to war. Both Ukraine and Israel have proved resilient,   
drawing on their populations and civilian sectors to   
sustain long, grueling fights. Russia and Hamas have   
also proved resilient. Information campaigns have been   
vital for all these actors; some, notably Ukraine but also   
Hamas, have sold their narrative effectively. Hamas’s   
hostage taking, while not destroying Israeli resilience,   
has created significant fissures in Israeli society.  
This chapter first defines resilience and explains   
why it matters in both the Ukraine and Middle East   
wars. It then draws lessons from these two conflicts   
and details the implications for the future of war.  
What Is Resilience   
and Why Does It Matter?  
From a national security perspective, a country is   
resilient if it has both the will and ability to resist and   
recover from external pressure, ranging from influ­  
ence campaigns to an invasion. In practice, resilient   
societies can protect their civilians, ensure basic ser­  
vices like electricity and medical care continue, stand   
W  
ars involve not only a clash of forces but   
also a clash of national wills. The great   
theorist of war Carl von Clausewitz   
stressed the importance of “moral” factors in war,   
such as the people’s will to fight, levels of support   
for the cause, and national unity.1 Adversaries seek   
to shatter the cohesion and resilience of the United   
States and its allies through varied means. Russia   
uses disinformation to polarize U.S. and European   
societies and has supported extreme-right opposi­  
tion parties and even motorcycle gangs to increase   
violence and polarization.2 The Hamas attack on Is­  
rael on October 7, 2023, and various Russian attacks   
on Ukraine, including the 2022 all-out invasion, also   
sought to shatter resilience by killing and threatening   
civilians and imposing widespread suffering.  
This chapter argues that societal resilience is   
vital for countries to stand up to aggression; when it   
is strong, it enhances deterrence. In future conflicts,   
aggressors such as China and Russia are likely to try   
to undermine resilience as an alternative or prelude   
photo: les kasyanov/global images ukraine/getty images

**Page 26**

20  
Will, Cohesion, Resilience, and the Wars of the Future  
up to coercion, and build a will to resist and fight a   
foreign invader.  
Ukraine demonstrated resilience in February   
2022 when it rallied against a full-on invasion while   
facing Russian cyberattacks, a barrage of propaganda,   
leadership assassination attempts, the promotion of   
puppet governments, and other threats. Ukrainians   
signed up to fight Russia in droves, kept electricity   
and power plants going, and conducted assassi­  
nations and sabotage in Russian-occupied parts of   
Ukraine that made it hard for Russia to administer   
and stage from these areas. All of this bought valuable   
time for Ukraine’s allies, especially the United States,   
to pour billions of dollars of military aid into the coun­  
try, helping it survive multiple years of a grinding war   
against a much larger aggressor.  
Resilience is also vital to sustain forces in a   
conflict. The Ukraine conflict has been relentless,   
with Ukrainian leaders claiming they have lost over   
45,000 soldiers since 2022, with hundreds of thou­  
sands wounded. The former is almost certainly a   
gross understatement, with the real figure probably   
more than double.3 In addition, Ukraine has suffered   
over 10,000 civilian deaths and over 30,000 civilian   
injuries.4 Israel, for its part, lost more people on one   
day—almost 1,200—than any day in its history. In the   
months after October 7, it sustained a war on multi­  
ple fronts, drawing heavily on reservists despite the   
social strain and cost to the country’s economy.  
Resilience’s greatest benefit, however, often   
comes before a crisis occurs. Resilience is vital to   
deterrence. Countries that lack resilience may seem   
easy to invade, whereas those with resilience require   
more resources and are more difficult to occupy. As   
Finnish scholars argue, “Even the biggest bear will   
not eat a porcupine.”5  
Lessons from Ukraine   
and the Middle East  
Israel’s enemies—Iran, Hamas, Hezbollah, and the   
Houthis—and Russia have tried to undermine the   
resilience of Israeli and Ukrainian societies, respec­  
tively. Much of Russia’s conventional and irregular   
war effort, including cyber and missile attacks on   
power infrastructure and hospitals, assassination   
attempts, and propaganda, has sought to break the   
population’s will to resist and decrease support for   
Kyiv’s war effort. In addition, Moscow has created   
puppet governments in parts of Ukraine it has occu­  
pied and otherwise tried to undermine the legitimate   
government there. Meanwhile, Hamas sought to   
shatter Israeli morale at a time when the country was   
highly divided politically and believed that large-scale   
hostage taking would force the country to its knees.   
Hezbollah and Houthi leaders hoped their attacks in   
solidarity with Hamas would force Israel to stop oper­  
ations in Gaza, believing it could not sustain a long,   
draining war.  
Russia has also tried to use sabotage and eco­  
nomic pressure to coerce Ukraine’s European allies   
into withdrawing their support by targeting the resil­  
ience of their civilian populations. Russian sabotage   
attacks have primarily targeted critical infrastruc­  
ture such as pipelines, fiber-optic cables, and power   
cables, as well as rail lines and aviation, especially   
arms manufacturers and suppliers (a breakdown of   
categories is provided in Figure 2.1). Although such   
incidents are not new, Russia’s invasion of Ukraine   
in February 2022 accelerated the number of attacks:   
There were 3 in 2022, 12 in 2023, and 34 in 2024. These   
forms of attack, occurring in tandem with political   
interference and disinformation campaigns, amount   
to a hybrid warfare campaign.6  
To resist attacks intended to undermine domestic   
morale, both Israel and Ukraine have drawn on deep   
wells of resilience. Ukraine’s army had 196,000 sol­  
diers before the attacks; by early 2025, it maintained   
almost 900,000 soldiers, including reservists.7 In   
Israel, national security is normalized through com­  
pulsory military service at the age of 18; after this,   
individuals stay in the reserves until age 40 with   
continued training.8 The October 7 attacks brought   
the largest mobilization in Israel since the 1973 Yom   
Kippur War, and Israelis outside of the age range   
for reservists have still volunteered for military ser­  
vice.9 Many reservists have reported for duty before   
any official call-up, eager to volunteer when their   
country is under attack. Immediately after October   
7, Israel called up 360,000 reservists. As of January

**Page 27**

21  
Daniel Byman  
government ministries and financial institutions and   
worked with Ukrainian officials to combat it.20 Mic­  
rosoft has also allowed the Ukrainian government to   
utilize its cloud services for free.21  
Israel’s prewar preparedness has also served it   
well. Israeli residential and industrial buildings are   
required to have air defense shelters. Government   
funding is often allocated to building shelters in older   
buildings, addressing the 28 percent of Israelis who   
do not have close access.22 In addition, early warning   
systems provide civilians with notice to seek shelter.23   
As a result, the Israeli population has been well pro­  
tected and has not panicked in the face of Iranian and   
Houthi missile, rocket, and drone attacks.  
Information campaigns have been important   
parts of both conflicts, and Ukraine has fared better   
than Israel in this regard. Although Israel stressed   
Hamas’s aggression and hostage taking and has sought   
to justify its war as self-defense, much of the world   
has rejected the legitimacy of Israel’s ongoing oper­  
ations in Gaza, and the International Criminal Court   
has issued warrants for Prime Minister Benjamin   
Netanyahu and other Israeli leaders for war crimes.24   
Global opinion of Israel dropped by 18.5 percent from   
September to December 2023.25 In the United States,   
disapproval of Israeli military action increased from   
45 percent in November 2023 to 55 percent in March   
2024, with 33 percent of young Americans reporting   
they sympathized entirely or mostly with the Pales­  
tinian people.26 Around one-third of young Americans   
believe that Hamas’s reasons for fighting Israel are   
valid, indicating the challenges facing Israeli infor­  
mation campaigns.27  
2024, between 200,000 and 250,000 reservists were   
still mobilized.10 As of November 2024, 34 percent of   
reservists had served more than 150 days, and 54 per­  
cent had served more than 100 days.11  
Israel and Ukraine have also drawn heavily on   
their civilian sectors, which is vital for resilience.   
In 2022, Ukraine produced seven drone models. By   
2024, it was producing 67 models, with about 200   
domestic companies involved in the production.12 In   
an October 2024 speech, Ukrainian President Volo­  
dymyr Zelensky stated that Ukraine could produce 4   
million drones annually.13 With these drones, Ukraine   
has struck Russian energy facilities and other infra­  
structure deep inside Russia and has used drones to   
fight Russian military forces.14 After October 7, the   
Israeli Ministry of Defense worked with technology   
startups to deploy new capabilities.15 For example,   
50 percent of the anti-drone technology the Israeli   
military has used comes from startups.16 Between the   
start of the war and the end of 2024, Israel awarded   
orders to 101 startups or small companies to assist the   
war effort.17   
Civilian sectors, however, can easily become   
overtaxed, especially in longer wars. In Israel, 10   
to 15 percent of the technology workforce has been   
called to the reserves.18 The tech sector is critical   
for Israel’s economy, accounting for 16 percent of   
employment, half of the country’s exports, and 20   
percent of economic output.19 Much of Ukraine’s   
ability to defend itself against Russia’s cyberattacks   
has similarly been due to support from the private   
sector. Following the invasion, Microsoft alerted   
Ukrainian authorities of malware designed to target   
Figure 2.1: Targets of Russian Attacks in Europe, 2022–25  
Number of incidents  
Transportation  
Government  
Critical infrastructure  
Industry  
Other  
14  
14  
11  
11  
2  
Source: CSIS analysis.

**Page 28**

22  
Will, Cohesion, Resilience, and the Wars of the Future  
Measuring resilience within authoritarian states   
is difficult. Opinion polls, media criticism, political   
disagreements, and other standard ways to measure   
popular will and support for fighting all are inaccu­  
rate or muted in authoritarian states, and accuracy is   
usually even more skewed regarding support for sub­  
state groups. A month after the Ukraine war began in   
2022, Pentagon Press Secretary John F. Kirby claimed,   
“We certainly have indications that morale is a grow­  
ing problem inside the Russian forces that are fighting   
in Ukraine.”36 A 2023 Cambridge study reported that   
“levels of Russian financial and life satisfaction may   
be near their lowest levels in a decade, while levels of   
online dissent have spiked in response to failures in the   
prosecution of the war.”37 Russia still faces shortages of   
soldiers and, despite having a much larger population   
than Ukraine, has been forced to draft large numbers   
of convicts, offer large bonuses to recruits, and bring in   
North Korean forces to bolster its ranks. Nevertheless,   
despite sustaining staggering losses on the battlefield   
as well as Ukrainian attacks on Russian energy and mil­  
itary infrastructure, Russia has stayed in the fight.  
Measuring Hamas’s morale is even more difficult.   
It is reasonable to conclude that the devastation of   
Gaza, the loss of many fighters, and the decimation   
of Hamas’s leadership hindered morale, but the orga­  
nization has not collapsed. Even after the ceasefire,   
Hamas remains the strongest Palestinian power and   
does not seem to face significant popular unrest.38  
Conclusion  
In both Ukraine and Israel, the story of resilience   
is not only about battlefield endurance but also the   
mobilization of society—military, civilian, techno­  
logical, and psychological—to resist aggression and   
maintain national cohesion. Their experiences under­  
score the critical importance of preparing societies   
for long-term conflict, including safeguarding infra­  
structure, cultivating civilian readiness, and main­  
taining the credibility of national narratives in the   
global information space. Resilience in this broader   
sense serves both defensive and deterrent functions:   
It helps nations absorb shocks without collapse and   
signals to adversaries that occupation or coercion will   
not yield easy gains.  
Ukraine has not face similar informational   
challenges, as it has the support of NATO countries   
and Russia is widely seen as the aggressor, partic­  
ularly after U.S. intelligence detected the invasion   
in advance and “prebunked” Russian propaganda.   
The Ukrainian government has advanced its cause   
effectively, largely via social media, focusing on the   
resilience of Ukrainian citizens and giving thanks to   
international supporters.28 Ukraine also appealed to   
the United Nations following the outbreak of war,   
with the UN General Assembly holding an emergency   
special session in February 2022 and overwhelmingly   
supporting a resolution demanding that Russia stop   
its invasion.29   
However, Russia has scored many propaganda   
victories, which are especially impressive given the   
overt nature of its aggression and the brutal behav­  
ior of its forces. Russian narratives in Africa capital­  
ize on European colonial history, with over 178,000   
Russia-linked tweets in the first two weeks of Russia’s   
invasion accusing Ukrainians and Europeans of rac­  
ism.30 According to the Africa Center for Strategic   
Studies, Russia has also sought to increase its general   
support of the continent, sponsoring 80 documented   
campaigns in over 22 countries.31 Russian propaganda   
has often been successful, with 84 percent of the pop­  
ulation in Mali reporting positive opinions of Russia.32   
Russia has also used propaganda within Europe. Ger­  
many, Ukraine’s second-largest weapons supplier, has   
reported an increase in Russian disinformation in an   
attempt to decrease support for Ukraine.33   
Hamas’s taking of hostages has proved a chal­  
lenge for Israeli resilience. The question of whether   
to continue the fight against Hamas or to seek a   
ceasefire as part of a hostage release divided Israel   
for many months. In January 2024, the war cabinet   
largely supported a ceasefire, but lawmakers in the   
governing Likud party supported continued military   
operations.34 On June 2, 2024, two far-right minis­  
ters threatened to quit if Prime Minister Netanyahu   
agreed to the ceasefire proposal, a move that would   
have collapsed the governing coalition.35 Israel has at   
times pursued negotiations but in other cases pur­  
sued aggressive military operations that have made a   
ceasefire and negotiated end to the conflict less likely.

**Page 29**

23  
Daniel Byman  
tion and social change. Political leaders can worsen   
or ameliorate these divisions through their rhetoric   
and policies, and they must recognize that playing up   
divisions provides openings for adversaries.  
Strategic planners must view societal resilience   
as an integrated element of national security, not a   
secondary consideration. The wars in Ukraine and   
the Middle East illustrate that the contest over will   
and cohesion is not merely an adjunct to military con­  
flict—it is central to victory or defeat.  
Mobilizing the population is necessary to resist   
foreign efforts to undermine resilience. Both the   
Ukraine and Gaza wars have been long and have   
required Ukraine and Israel to mobilize reservists and   
parts of their population outside the military. It is dif­  
ficult to know how long a conflict between the United   
States and China or another major war would last,   
but it is plausible that such a conflict would require   
a sustained effort in which success would depend, in   
part, on which side could best mobilize its population   
for the long term.  
Authoritarian states can use coercion and propa­  
ganda to suppress dissent. Like other regimes, they   
can also draw on nationalism and antiforeign senti­  
ment to stay in power. Nevertheless, their resilience   
can be undermined, and it is often more brittle than it   
appears. Indeed, as the December 2024 fall of Bashar   
al-Assad’s Syrian regime suggests, seemingly solid   
authoritarian regimes can collapse quickly. Offensive   
information operations against authoritarian states   
could focus on unpopular regime policies, human   
rights abuses, economic problems, corruption, or   
domestic political and societal divisions.  
Future conflicts could see large-scale hostage   
taking, forced assimilation of captured populations,   
and other illegal, but nonetheless quite real, anti-ci­  
vilian actions that might divide popular opinion.   
Countering this requires developing an information   
strategy for domestic and foreign audiences, develop­  
ing communications with occupied parts of a country,   
and ensuring special operations forces are well pre­  
pared for hostage rescue missions.  
Ensuring cohesion and resilience depends,   
in part, on defending civilian infrastructure and   
national security assets controlled by private sector   
companies, many of which do not focus on national   
security or regularly interact with the government   
in peacetime. Much of this activity will occur in the   
cyber realm, requiring close cooperation with a range   
of private technology companies.  
Societal divisions undermine resilience, and   
adversary propaganda tries to play on these. Such   
divisions are difficult to overcome, often stemming   
from broader societal problems due to discrimina­  
Resilience . . . serves both defensive and   
deterrent functions: It helps nations   
absorb shocks without collapse and   
signals to adversaries that occupation   
or coercion will not yield easy gains.

**Page 30**

CHAPTER 03  
Returning to an Era   
of Competition and   
Nuclear Risk  
Heather Williams, Joseph Rodgers, and Elizabeth Kos

**Page 31**

25  
Heather Williams, Joseph Rodgers, and Elizabeth Kos  
”  
“  
The erosion of the global nuclear   
order—fueled by adversarial nuclear   
expansionism, the proliferation of theater-  
range nuclear forces, growing adversary   
collusion, and the weakening of U.S.   
alliance credibility—demands change.  
spheres, including with respect to nuclear issues.   
Adversary nuclear collusion has included joint exer­  
cises, transfers of fissile material, and mutual support   
in international diplomatic forums.3 In July 2024,   
Russia and China carried out a joint bomber patrol   
exercise near Alaska using dual-capable bombers and   
approaching U.S. sovereign airspace.  
U.S. global leadership in the defense arena is also   
facing growing skepticism from key allies. In March   
2025, French President Emmanuel Macron declared   
that Europe may need to adopt a defense posture less   
reliant on the United States, potentially signaling a   
shift away from the long-standing NATO framework.4   
France is even considering extending its nuclear   
deterrent to cover the defense of Europe, a signifi­  
cant departure from its traditional focus on national   
defense. This development, coupled with growing   
calls within the Trump administration to reduce   
European dependence on U.S. security guarantees,   
highlights changes in transatlantic relations and the   
potential for a reconfiguration of the global security   
U  
.S. strategic thinking in the Cold War was   
dominated at various points by fears of ad­  
versarial collusion, the erosion of U.S. alli­  
ances, and the collapse of U.S. global leadership. To­  
day, all three of those fears are simultaneously coming   
to fruition.   
Russia, China, and North Korea have all ramped   
up their nuclear threats, with the goal of gaining   
territory in Europe, the Indo-Pacific, and East Asia,   
respectively. In October 2022, for example, Krem­  
lin officials initiated large-scale nuclear exercises   
and threatened nuclear use to further Putin’s goal   
of illegally annexing Ukraine.1 Meanwhile, all three   
countries have worked to rapidly upgrade, expand,   
and diversify their nuclear arsenals. The Department   
of Defense (DOD)’s 2024 report on China’s military   
power warns that Beijing is accelerating its buildup of   
nuclear weapons, including those with theater-range   
dual-capable delivery systems.2 In the past few years,   
Russia, China, Iran, and North Korea have expanded   
cooperation in military, economic, and political   
photo: keystone/hulton archive/getty images

**Page 32**

26  
Returning to an Era of Competition and Nuclear Risk  
expansionist objectives, (2) the proliferation of the­  
ater-range nuclear forces, (3) increased cooperation   
among adversaries, and (4) the erosion of U.S. credi­  
bility with allies.   
These trends are underpinned by major invest­  
ments in nuclear modernization by all nuclear-armed   
states. The United States is currently undertaking a   
$1.7 trillion nuclear modernization effort to upgrade   
all three legs of its nuclear triad—land-based inter­  
continental ballistic missiles, submarine-launched   
ballistic missiles, and strategic bombers.8 This pro­  
gram, initiated by the Obama administration, seeks   
to ensure the continued credibility and effectiveness   
of the U.S. nuclear deterrent. Simultaneously, U.S.   
adversaries are rapidly expanding and modernizing   
their nuclear arsenals, posing a direct challenge to   
U.S. strategic dominance. The DOD’s 2024 report on   
China’s military power estimates that China may pos­  
sess as many as 1,000 nuclear warheads by 2030, a   
significant increase from its current arsenal.9 Mean­  
while, Russia is fielding advanced weapons such   
as hypersonics capable of countering U.S. missile   
defenses, and North Korea is developing tactical   
nuclear weapons designed for battlefield use.  
Nuclear Expansionism by Adversaries  
Nuclear-armed states are leveraging their arsenals   
to pursue territorial ambitions and redraw interna­  
tional borders. Following Russia’s illegal invasion of   
Ukraine in February 2022, Moscow has used a variety   
of nuclear threats and signals in apparent attempts   
to deter Western intervention in the war.10 Recently,   
President Trump announced on social media that the   
United States would order two nuclear submarines   
“to be positioned in the appropriate regions” after   
former Russian President Dmitry Medvedev mocked   
what he termed U.S. “ultimatums” for Russia to end   
the war in Ukraine.11 Similarly, North Korea continues   
to issue nuclear threats against South Korea, aiming   
for reunification on its own terms. For example, in   
October 2024, North Korean leader Kim Jong-un   
threatened to destroy South Korea with “all the offen­  
sive forces it [possesses], including nuclear weapons,”   
if provoked.12 Furthermore, U.S. defense experts have   
expressed concern that China might employ similar   
architecture. Coinciding with these threats, U.S. allies   
are increasingly anxious about the credibility of U.S.   
nuclear commitments. In April 2024, Polish President   
Andrzej Duda urged NATO to deploy nuclear weap­  
ons to Poland in response to Russia’s deployment   
of nuclear weapons in Belarus.5 Additionally, a Feb­  
ruary 2024 poll by the Chey Institute for Advanced   
Studies revealed that over 70 percent of the South   
Korean public supports the development of an indige­  
nous nuclear weapons program to counter the threat   
posed by North Korea.6  
This chapter argues that the future of modern   
warfare will feature increased reliance on nuclear   
weapons by adversaries and allies alike. During the   
Cold War, the United States responded to adversary   
nuclear coercion by making judgments about Soviet   
red lines and signaling resolve to defend allies in the   
face of crisis. The United States addressed threats to   
regional deterrence from expanding Soviet nuclear   
capabilities and possible collusion with other adver­  
saries by strengthening its own nuclear capabilities   
and alliance networks. Doubling down on U.S. alli­  
ances through demonstrations of resolve and nuclear   
sharing arrangements had the additional effects of   
reassuring U.S. allies and stemming incentives for   
nuclear proliferation. For example, during the Cold   
War, the United States stored nuclear weapons in   
Europe as part of a broader effort to quell fears of   
allied proliferation.7   
The rest of this chapter is divided into three main   
sections. The first outlines nuclear risks that have   
emerged from the wars in Ukraine and the Middle   
East. The second analyzes new challenges and impli­  
cations, such as the need for nuclear moderniza­  
tion. The third concludes by highlighting the need to   
develop a strategically nuanced approach to prevent   
miscalculation and maintain stability in an era of   
heightened competition and nuclear risk.  
The Resurgence of Nuclear Risks  
Conflicts in Ukraine and the Middle East, alongside   
escalating tensions across the globe, point to trends   
in the evolving role of nuclear weapons in interna­  
tional politics. Four related trends stand out: (1)   
adversaries relying on nuclear weapons to support

**Page 33**

27  
Heather Williams, Joseph Rodgers, and Elizabeth Kos  
developed and deployed intermediate-range nuclear   
weapons that could reach U.S. allies overseas. In   
1976, the Soviet Union deployed its new SS-20 inter­  
mediate-range ballistic missiles to Europe.17 This   
move allowed Moscow to hold European capitals   
at risk of nuclear attack and undermined Washing­  
ton’s extended deterrence guarantees in the region.   
To resolve this dilemma and strengthen regional   
deterrence, NATO decided to modernize and deploy   
its intermediate-range nuclear forces to Europe,   
holding the Soviet Union at risk with a parallel set of   
capabilities.18 The United States also began deploying   
nuclear-armed sea-launched cruise missiles, known   
as TLAM-Ns, on naval vessels to strengthen regional   
deterrence in both Europe and the Asia Pacific.  
The proliferation of theater-range nuclear weap­  
ons is particularly concerning today, however, as   
the bulk of the U.S. nuclear arsenal consists of stra­  
tegic systems designed to deter large-scale nuclear   
attacks, not battlefield use. In 1987, the United States   
and Soviet Union agreed to remove all intermedi­  
ate-range ground-launched ballistic and cruise mis­  
siles from the arsenals of both sides through the   
Intermediate-Range Nuclear Forces (INF) Treaty.19   
Additionally, the United States removed TLAM-Ns   
from its surface combat ships and submarines in   
1991 and officially retired the capability in 2010.20 In   
2014, however, Russia moved beyond limits set by the   
INF Treaty by developing a ground-launched cruise   
missile in violation of the agreement’s parameters.21   
While the United States is seeking to close the gap   
by developing a nuclear-tipped sea-launched cruise   
missile (SLCM-N), this capability will be difficult to   
field before 2034.22  
Increased Adversary Collusion  
The current security environment is also marked   
by growing collusion between Russia, China, North   
Korea, and Iran. Russia is exporting nuclear reactors   
to China, which DOD assesses will play a vital role   
in Chinese plutonium production for nuclear weap­  
ons.23 Similarly, China and Russia are conducting joint   
strategic bomber drills. For example, in November   
2024, China flew an H6-N nuclear-capable bomber in   
a joint drill with Russia.24 In January 2025, Secretary of   
tactics in a future Taiwan Strait crisis, threatening   
nuclear escalation to compel concessions.13   
While the United States faced similar nuclear   
threats from the Soviet Union during the Cold War,   
the addition of China’s and North Korea’s nuclear   
expansionism multiplies these risks and demands that   
the United States divide its attention among multiple   
adversaries at once. In the past, Washington helped   
thwart nuclear expansionism by making judgments   
about Soviet red lines and signaling resolve to defend   
allies in the face of crisis. Today, however, the United   
States must provide these judgments for multiple   
adversaries, each of whom has unique nuclear doc­  
trines and attitudes surrounding nuclear weapons.   
At the same time, adversaries, to calculate activities   
in their own regions, observe the actions the United   
States has taken (or not taken) to signal resolve in   
other theaters. Moreover, Russia, China, and North   
Korea are far less transparent than the United States   
in their doctrines and attitudes and the makeup of   
their nuclear forces. These new challenges of antic­  
ipating adversary red lines and signaling resolve to   
multiple adversaries at the same time raise the overall   
risks of nuclear use.  
Proliferation of Theater-Range Nuclear Forces  
Russia, China, and North Korea are all working to   
upgrade, expand, and diversify their nuclear arse­  
nals, including with theater-range nuclear capabili­  
ties. The 2023 Annual Threat Assessment of the U.S.   
Intelligence Community, produced by the Office of   
the Director of National Intelligence (ODNI), claimed   
that Russia is developing nonstrategic nuclear forces   
“because Moscow believes such systems offer options   
to deter adversaries, control the escalation of poten­  
tial hostilities, and counter U.S. and allied conven­  
tional forces.”14 China is also rapidly expanding its   
theater-range nuclear capabilities, exemplified by   
the DF-21 dual-capable “carrier killer” missile and   
the H6-N nuclear-capable bomber.15 North Korea,   
as acknowledged by the ODNI threat assessment,   
has explicitly stated its intention to develop tactical   
nuclear weapons for battlefield operations.16  
In the late 1970s and early 1980s, the United   
States faced similar challenges as the Soviet Union

**Page 34**

28  
Returning to an Era of Competition and Nuclear Risk  
deterrence commitments. As adversaries increasingly   
rely on nuclear weapons to achieve their expansionist   
goals, allies have sought greater nuclear assurances   
for themselves. According to recent reports by news   
sources and think tanks, some allies, such as Poland,   
have pushed for greater roles in U.S. nuclear shar­  
ing arrangements.31 Others, such as South Korea,   
have faced public pressure to consider developing   
indigenous nuclear weapons capabilities.32 Citing   
the possibility that the United States will not “remain   
by [Europe’s] side,” President Macron has suggested   
that France could step in to provide extended nuclear   
deterrence guarantees.33  
In the late 1950s, concerns over growing Soviet   
capabilities and doubts over U.S. commitments to   
European defense also caused several allies to con­  
sider developing nuclear weapons.34 In response, U.S.   
President Dwight D. Eisenhower proposed a plan to   
establish a NATO nuclear stockpile, whereby allies   
would operate nuclear delivery systems but the United   
States would retain primary control over nuclear war­  
heads.35 Through engaging allies in nuclear sharing   
arrangements, the United States bridged its nuclear   
force commitments to Europe while reducing risks of   
allied proliferation.36 The United States also facilitated   
the negotiation of several arms control agreements,   
such as the Limited Test Ban Treaty and the Nuclear   
Non-Proliferation Treaty, that helped restrict further   
proliferation.37 These agreements established global   
norms around nuclear nonproliferation and provided   
incentives, such as access to peaceful uses of nuclear   
technology, for countries to refrain from developing   
their nuclear weapons capabilities.   
Today, the future of arms control is increasingly   
precarious. The last remaining bilateral arms control   
agreement between the United States and Russia,   
the New START Treaty, will expire in February 2026.   
The demise of other crucial agreements, such as the   
Intermediate-Range Nuclear Forces Treaty, the Open   
Skies Treaty, and the Anti-Ballistic Missile Treaty,   
further underscores the erosion of the arms control   
architecture. Russia’s recent de-ratification of the   
Comprehensive Nuclear Test Ban Treaty has further   
eroded the heel of the global nonproliferation regime.   
Compounding these challenges, the United States is   
State Antony Blinken stated there is “reason to believe   
that Moscow intends to share advanced space and sat­  
ellite technology with Pyongyang.”25 Advanced space   
and satellite technologies are often dual-use, and   
advances in space technology contribute to advances   
in long-range ballistic missile programs. Similarly, in   
September 2024, Secretary Blinken claimed, “Russia   
is sharing technology that Iran seeks—this is a two-  
way street—including on nuclear issues as well as   
some space information.”26  
During the Cold War, U.S. officials feared the   
Soviet Union could work with other powers, such as   
China and North Korea, to achieve its expansionist   
aims. In March 1950, Secretary of State Dean Acheson   
testified to Congress that the United States must   
ensure “that whoever runs China, even if the devil   
himself runs China, that he is an independent devil.   
That is infinitely better than if he is a stooge of Moscow   
or China comes under Russia.”27 These fears became   
acute, as Chinese intervention in the Korean War   
in October 1950 yielded speculation over collusion   
among communist leadership in Beijing, Pyongyang,   
and Moscow.28 The Truman administration developed   
a robust response by building up conventional and   
nuclear forces in the United States.29 In later years,   
National Security Advisor Henry Kissinger tried to   
drive a wedge between the Soviet Union and China   
with a diplomatic strategy that enabled the United   
States to “maintain closer relations with each side   
than they did with each other.”30 This historical lesson   
underscores the enduring imperative for the United   
States to prevent the formation of a unified bloc of   
nuclear-armed adversaries and highlights the strate­  
gic value of fostering divisions among them. In today’s   
multipolar landscape, characterized by increasingly   
intertwined yet distinct national interests, the United   
States must proactively seek to discourage deeper,   
irreversible security alignments between Russia,   
China, North Korea, and Iran.  
Erosion of U.S. Alliance Credibility  
Threats from adversary nuclear expansionism, the­  
ater-range nuclear forces, and adversary collusion   
have produced doubts among U.S. allies over the   
ability of the United States to maintain its extended

**Page 35**

29  
Heather Williams, Joseph Rodgers, and Elizabeth Kos  
acute awareness of possible escalatory ladders and   
adversary red lines.  
This dynamic inherently alters the calculus of   
future conventional wars between nuclear-armed   
states, where the specter of nuclear weapons could   
be placed over each decision. It implies that future   
opponents may use nuclear threats not only as a last   
resort but as a part of their early coercive campaigns   
to extract concessions, discourage third-party inter­  
vention, or even cover conventional aggression. This   
openness to such high-risk action naturally elevates   
the danger of miscalculation and accidental escala­  
tion, making conflict management much more com­  
plicated and risky for the United States and its allies.  
Lack of Escalation Management Tools   
Could Exacerbate Crises   
The evolving nature of warfare, characterized by the   
blurring of lines between conventional and nuclear   
conflict, necessitates the development of robust   
escalation management tools. Russia’s increasing   
reliance on hostile rhetoric and nuclear saber-rat­  
tling in Ukraine demonstrates a willingness to employ   
nuclear coercion to achieve its objectives.38 Moscow’s   
use of nuclear threats to seize territory and redraw   
borders in Europe represents a dangerous escalation   
that challenges fundamental norms of international   
security. Furthermore, the development of tactical   
nuclear weapons by U.S. adversaries poses a chal­  
lenge to escalation control. These weapons, designed   
for battlefield use against a limited number of targets,   
lower the threshold for nuclear use and complicate   
traditional notions of deterrence.  
This asymmetry creates a potential “deterrence   
gap” and necessitates the development of a more   
flexible and nuanced approach to escalation man­  
agement. The United States needs a broader array of   
capabilities to deter—and, if necessary, respond to—  
limited nuclear use by adversaries. This could include   
developing conventional weapons with enhanced   
precision and destructive power, modernizing   
existing nuclear capabilities to provide more flexi­  
ble options, and exploring non-kinetic tools such as   
cyber warfare and electronic warfare to disrupt and   
degrade an adversary’s ability to escalate conflict.  
now demanding more from its allies while seeming   
to scale back its own commitments. Taking a more   
transactional approach, Washington seeks increased   
financial and security contributions from its partners.   
The prospects for achieving meaningful progress on   
arms control and strengthening alliance cohesion   
appear increasingly dim.  
New Challenges and Implications  
These converging challenges—renewed threats of ter­  
ritorial expansion backed by nuclear threats, theater   
nuclear forces, adversary collusion, and degrading   
U.S. alliance credibility—have several implications   
for the future of warfare and competition. It is likely   
that there will be an increase in nuclear threats and   
risk-taking in future regional conflicts, a lack of esca­  
lation management tools during crises, and a greater   
need for increased knowledge of nuclear issues at   
every echelon of military command. These trends   
demand a reassessment of nuclear strategy and chal­  
lenge some key prevailing deterrence assumptions of   
the past eight decades.   
Increased Risk-Taking in Regional Conflicts   
Other nuclear possessors are likely watching Rus­  
sia’s actions in Ukraine. If they draw the conclusion   
that nuclear bullying delayed Western intervention,   
they may be more prone toward risk-taking and risk   
manipulation in future regional conflicts. Adversar­  
ies may come to believe that the United States and   
its allies have less at stake in distant theaters, thus   
validating the utility of nuclear coercion as a tool to   
achieve strategic objectives.   
This trend may result in the perceived reduction   
of the nuclear threshold, altering the way conflicts   
are initiated and controlled. Opponents may increas­  
ingly try to take advantage of this perceived change,   
blending nuclear threats and coercive signaling into   
different stages of conflict, ranging from pre-cri­  
sis intimidation to bids for escalation control in the   
course of a conflict. The purpose of nuclear threats   
would be to achieve asymmetric benefit or nullify   
superior conventional capabilities. This sets up a sit­  
uation where conventional actions are continuously   
overshadowed by nuclear potential, requiring an

**Page 36**

30  
Returning to an Era of Competition and Nuclear Risk  
operational concepts, and a renewed focus on   
nuclear literacy within the armed forces.  
Conclusion  
The resurgence of great power competition, coupled   
with the evolving nature of nuclear threats, pres­  
ents a complex challenge to the role that nuclear   
weapons play in the future of modern warfare. The   
erosion of the global nuclear order—fueled by adver­  
sarial nuclear expansionism, the proliferation of   
theater-range nuclear forces, growing adversary col­  
lusion, and the weakening of U.S. alliance credibility—  
demands change. All nine nuclear-armed states are   
currently modernizing their nuclear forces, under­  
scoring the increasing role that nuclear weapons will   
play in future conflicts.   
The challenges facing the security environment   
today bear some similarities to those of the Cold War,   
but in many ways the current threats are different   
and more diverse. The contemporary security envi­  
ronment presents unique complexities requiring   
innovative solutions and a willingness to adapt to   
new realities.   
By examining the confluence of rising nuclear   
threats, eroding alliance credibility, and increasing   
adversarial collusion, this chapter paints a concern­  
ing picture of the future of modern warfare. The   
demonstrated willingness of nuclear-armed states to   
employ coercive nuclear signaling in pursuit of terri­  
torial gains, coupled with the proliferation of more   
usable theater-range nuclear weapons, suggests a   
lowering of the nuclear threshold in future conflicts.   
Furthermore, growing security cooperation among   
Unfamiliar Deterrence Challenges,   
Learning Delays   
While some underlying aspects of the new nuclear   
landscape are similar to the Cold War era—such as   
the dynamics of great power rivalry, high-stakes   
games of chicken, the balance between offense and   
defense, and the nuances of alliance management—  
the modern environment also features a plethora of   
new challenges. These include unprecedented tech­  
nological change, the growing frequency and inten­  
sity of nuclear-backed crises in regional contexts, and   
an expanding network of proliferation threats that go   
well beyond traditional state actors.   
Along with the implications of a deterrence gap,   
wherein U.S. capabilities and the range of adversary   
threats may not be perfectly matched, there may   
also be an acute knowledge gap in twenty-first-cen­  
tury warfare. Modern military strategists must know   
how various technologies and complex technologi­  
cal systems interact in warfare, be aware of how to   
deter effectively in regional crises, and understand   
how the United States should contend with the com­  
plexity of deterring two peer competitors—China   
and Russia—simultaneously across separate theaters.   
Future warfighters will need to closely calibrate man­  
aging escalation and signaling resolve in a multipolar   
nuclear landscape where intentions and doctrines are   
less openly advertised.  
Filling this knowledge gap and elevating over­  
all “deterrence IQ” will be a long-term and multi­  
faceted endeavor, requiring intellectual effort well   
beyond the traditional nuclear policy community.   
There needs to be an increase in nuclear knowledge   
across the entire defense establishment. Warfight­  
ers, even those who work almost exclusively in   
the conventional sphere, will need to gain a much   
deeper appreciation of the prospective effects of   
nuclear weapons on conventional conflict. This   
means coming to terms with the psychological and   
physical effects of nuclear employment, appreciat­  
ing adversary escalation ladders, and developing   
the skills and procedures needed to fight and win   
in a nuclear-contaminated battlefield environment.   
Warfighters will need new training regimens, revised   
Future warfighters will need   
to closely calibrate managing   
escalation and signaling resolve in   
a multipolar nuclear landscape,   
where intentions and doctrines   
are less openly advertised.

**Page 37**

31  
Heather Williams, Joseph Rodgers, and Elizabeth Kos  
U.S. adversaries creates a complex web of threats,   
demanding new and sophisticated approaches to   
deterrence and conflict management.   
The erosion of U.S. alliance credibility risks fur­  
ther destabilizing the international order and poten­  
tially incentivizing proliferation among concerned   
partners. These trends collectively point to a future   
where nuclear considerations will be more present   
and the risks of escalation more acute in the manage­  
ment of modern warfare. Ultimately, navigating this   
era of heightened competition and nuclear risk will   
require a strategically nuanced approach to prevent   
miscalculation and maintain stability in an increas­  
ingly dangerous world.

**Page 38**

PART II  
Operations, Tactics,   
and Technology

**Page 39**

CHAPTER 04  
Operational Art in the   
Age of Battle Networks  
Benjamin Jensen

**Page 40**

34  
Operational Art in the Age of Battle Networks  
”  
“  
Combat power is increasingly defined by   
the ability to fuse intelligence, orchestrate   
synchronized actions, and generate   
affordable mass through dynamic kill webs.  
and the government research and development infra­  
structure that created nuclear weapons. However,   
today, well into the age of information, bytes cross   
global networks and increasingly integrate the private   
sector to change the character of war and, through it,   
operational art.6   
New technologies generate new ideas about war,   
a cycle of discovery and experimentation often com­  
pressed by the demands of battle. That pattern is on   
display from the vast steppes of Ukraine to the deserts   
of the Middle East.   
This chapter explores what these battles say   
about the future of war. Through examining crucial   
case studies in Ukraine and conflicts in the Middle   
East, it charts how operational art is changing based   
on the rapid advancement of networked sensors,   
data-driven command and control, and precision   
fires, including information effects in the electromag­  
netic spectrum and cyberspace. These developments   
realize the visions of future war imagined in the 1990s   
by army leaders like General Gordon Sullivan in Force   
O  
n the morning of October 29, 2022, a swarm   
of Ukrainian naval drones, controlled re­  
motely and connected via a shared targeting   
network, struck Russia’s Black Sea Fleet at Sevastopol.1   
While the concept of swarming is an old one, the at­  
tack represented something new—a demonstration of   
modern operational art, where distributed platforms,   
intelligence fusion, and autonomous systems create   
asymmetric effects against a conventionally superior   
adversary.2 The battle turned emerging ideas of war,   
often associated with terms like “replicator” and “mo­  
saic warfare,” into a reality.3 The strike forced Russia   
to reconsider its naval posture, highlighting that suc­  
cessful operational art in the age of battle networks is   
contingent on integrating effects across domains while   
leveraging information as a force multiplier.4  
War is a continuation of politics by other means,   
but its form and manifestation on the battlefield are   
directly linked to the intersection of ideas and chang­  
ing material conditions.5 In the past, materials for   
wartime economies focused on iron, gunpowder,   
photo: u.s. marine corps photo by lance cpl. colton brownlee

**Page 41**

35  
Benjamin Jensen  
both harbingers of the new ways of combat: (1) the   
Ukrainian campaign in Kursk and (2) Israeli retalia­  
tory air strikes against Iran’s air defense network in   
October 2024. While additional cases—such as the   
2020 Second Nagorno-Karabakh War, the May 2025   
India-Pakistan standoff, and Israel-Iran clashes in   
June 2025—further illustrate the trend, this chapter   
focuses on these crucial air and ground cases in order   
to link observed operational behavior to foundational   
military theory. The chapter concludes with reading   
across these cases to catalogue how the emergence of   
modern battle networks and long-range effects alter   
the character of warfare.   
Charting Change in Operational   
Art: The Principles of War  
There is a long history across cultures of using law­  
like principles to guide the design of military cam­  
paigns. Both Sun Tzu (ca. 400–301 BCE) in The Art   
of War and the Indian philosopher Kautilya (ca.   
300 BCE) in the Arthashastra outlined key factors   
associated with mobilizing and deploying combat   
power.14 In the fourth century CE, Flavius Vegetius   
Renatus wrote De re militari for Emperor Valentinian   
II, including a section on maxims (i.e., principles) of   
war. This work proved influential for over a thousand   
years and shaped Niccolò Machiavelli’s ideas in books   
like The Art of War.15 The concept of principles and   
guides to war extended from the Renaissance into   
early modern Europe through key works by Henri,   
duke de Rohan, and Marquis de Silva’s 1778 work   
Principles, which, alongside ideas by English thinker   
Henry Lloyd, became the foundation of Napoleonic   
warfare.16 The modern usage of the concept draws   
from both Lloyd’s work and The Art of War by Henri,   
baron de Jomini, through British military officer and   
theorist J. F. C. Fuller.17  
The enduring concept is that military practi­  
tioners use these principles to help analyze and plan   
campaigns. The principles provide the underlying   
logic in the search for a theory of victory, guiding   
commanders and staff as they confront the dual pres­  
sures of allocating resources and translating intent   
into schemes of maneuver. Current U.S. joint doctrine   
lists 12 principles (Table 4.1).18  
XXI and even earlier by Soviet theorists dreaming of   
precision strike complexes.7 The resulting networked   
formations represent the defining trend in modern   
war. These scalable networks invert the relationship   
between fire and maneuver to create entire cam­  
paigns predicated on moving sensors into place to   
deny adversary courses of action through a mix of   
long-range strikes, information effects, and drone   
swarms along the forward line of troops. This trans­  
parent battlefield is unforgiving.8 To use an old army   
phrase from General William DePuy, “What can be   
seen can be hit, what can be hit can be destroyed.”9  
There is a new character of combined arms where   
information is more than a combat multiplier.10 The   
ability to collect, fuse, and disseminate information is   
a defining feature of military power and calls for new   
ways of thinking about the correlation of forces and   
means in modern war.11   
Combat power is increasingly defined by the   
ability to fuse intelligence, orchestrate synchro­  
nized actions, and generate affordable mass through   
dynamic kill webs.12 The formations that master this   
approach generate operational tempo, imposing   
dilemmas on adversaries and forcing self-defeating   
decisions. This evolution marks a movement away   
from traditional linear strategies focused on mass   
and objectives (i.e., decisive points) toward a more   
dynamic hunt for asymmetries, exploiting weak   
points and overloading adversary decision cycles.   
Operational art becomes the ability to disrupt, dis­  
orient, and out-cycle the adversary by designing ways   
to integrate domains and sequence tactical actions.  
Technology drives change but only through the   
people who use it and imagine new ways of war. The   
underlying assumption is that there are transnational   
learning communities at play in the transmission of   
military art across national boundaries. Profession­  
als including career officers, civilian appointees,   
entrepreneurs, and scientists learn from each other   
through a process of emulation and adaptation.13  
This chapter proceeds by establishing an analyt­  
ical framework for analyzing how the emergence of   
information-centric battle networks is changing oper­  
ational art using the concept of the principles of war.   
Next it applies this framework to two case studies,

**Page 42**

36  
Operational Art in the Age of Battle Networks  
resources becomes. This effect, in turn, allows states   
with robust C5ISRT networks, like Ukraine, to fight   
outnumbered by vectoring in small drones, such   
as first-person view (FPV) drones, and artillery fire   
to attrit assaults and even spoil attacks before they   
begin. This logic is also why the U.S. Department of   
Defense, despite ongoing struggles, has prioritized   
both combined joint all-domain command and con­  
trol (CJADC2) and software-driven approaches to   
acquisition.20   
The concept of kill chains, increasingly called   
“webs,” reflects the lethal application of fused data   
from a battle network.21 The term “webs” identifies the   
importance of more scalable and resilient networks   
consistent with earlier Defense Advanced Research   
Projects Agency (DARPA) concepts of mosaic war­  
fare.22 This idea has diffused rapidly through the inter­  
national system, including references in the People’s   
Liberation Army (PLA) Science of Military Strategy and   
Russian doctrine before the war in Ukraine.23 This   
concept, in turn, reflects the maturation of an earlier   
idea of reconnaissance-strike complexes, which has   
dominated Russian military thought for decades.24 Kill   
The central idea is that these principles help   
assess crucial cases in recent wars and, in the process,   
illustrate the emerging importance of information   
effects and battle networks to modern operational   
art. A battle network is the fusion of sensors, shooters,   
and decisionmakers into a dynamic system capable   
of synchronizing effects across domains.19 These net­  
works aim to shorten kill chains, increase survivability   
through dispersal, and maximize cross-domain fires.   
Unlike traditional force structures that emphasize   
mass formations, battle networks prioritize speed,   
precision, and adaptability, shifting from a plat­  
form-centric to a data-centric approach to warfare.  
Battle networks encompass two key comple­  
mentary concepts: (1) command, control, commu­  
nications, computers, combat systems, intelligence,   
surveillance, and targeting (C5ISRT) and (2) kill   
chains/webs. C5ISRT networks are the backbone of   
modern operations, enabling real-time data fusion   
to match weapons with targets faster than the enemy   
can react. The core concept is that the faster a side   
can fuse data and allocate resources, the higher   
the tempo and more prudent the expenditure of   
Table 4.1: Twelve Principles of War  
Principle  
Definition  
Objective  
Direct military action toward a clearly defined and achievable goal.  
Offensive  
Seize, retain, and exploit the initiative.  
Mass  
Concentrate the effects of combat power at the most advantageous place and time to produce results.  
Maneuver  
Place an adversary or enemy in a position of disadvantage.  
Economy of force  
Expend minimum essential combat power (lethal and nonlethal) on secondary efforts to allocate the   
maximum possible combat power on primary efforts.  
Unity of command  
Ensure unity of effort under one responsible commander for every objective.  
Security  
Prevent the enemy from acquiring an unexpected advantage.  
Surprise  
Strike at a time or place where the enemy is unprepared.  
Simplicity  
Increase the probability of success in execution by preparing clear, uncomplicated plans and concise   
orders.  
Restraint  
Prevent the excessive use of force.  
Resilience  
Withstand and recover from disruptions from internal and external factors.  
Legitimacy  
Maintain legal and moral authority.  
Source: U.S. Department of the Army, ADP 3-0: Operations (Washington, DC: Department of the Army, July 2019), https://armypubs.  
army.mil/epubs/DR\_pubs/DR\_a/ARN18010-ADP\_3-0-000-WEB-2.pdf.

**Page 43**

37  
Benjamin Jensen  
not supporting fires but central to the correlation of   
forces and means in twenty-first-century conflict.  
Maneuver on a Transparent Battlefield:   
The 2024 Kursk Offensive  
One of the core challenges of modern war is how to   
conduct large-scale maneuvers—whether by ground,   
air, or sea—when the adversary has access to constant   
intelligence feeds fusing commercial satellite imagery   
with classified signals and human intelligence. This   
dynamic has been characterized elsewhere as a “trans­  
parent battlefield,” implying that massing forces has   
diminishing marginal returns, essentially a self-defeat­  
ing proposition.27 The first challenge of modern opera­  
tional art is therefore how to align surprise, maneuver,   
mass, and objective on a transparent battlefield.   
Ukraine’s initial push into Kursk offers a crucial case.  
In the late summer of 2024, Ukraine launched its   
largest cross-border assault into Russia since the start of   
the 2022 war in an effort to point Moscow on the horns   
of a dilemma. A mix of Ukrainian special operations   
and elements of the 80th Air Assault Brigade infiltrated   
the front line, conducting special reconnaissance that   
complemented larger intelligence operations and com­  
bined a mix of commercial satellite imagery analysis,   
signals intelligence, and extensive human intelligence   
networks. These infiltration operations made exten­  
sive use of drones and electronic warfare—both attack   
and collection—to map adversary battle networks and   
weak points along the front line.   
Combined, these operations created a new opera­  
tional picture that maneuver commanders could use to   
visualize the battlespace and identify when and where   
to launch their initial assault. This assault consisted   
of mobile groups conducting armed reconnaissance   
designed to identify and exploit gaps in the Russian line   
based on intelligence reporting. Once a mobile group   
had attacked in depth, Ukrainian forces could commit   
entire brigades to exploit the advantage. The case was   
a textbook example of maneuver warfare but was con­  
ducted in a manner consistent with emerging trends in   
drone and electromagnetic spectrum warfare.   
Turning to the principles of war, the campaign   
highlighted key features of modern conflict: rapid   
mechanized thrusts, electronic warfare, and deliber­  
webs support operational targeting through concepts   
like kill boxes, which define geographic areas where   
forces have deconflict engagement authority. This   
accelerates tempo, including rapidly shifting author­  
ities and attack guidance based on feedback loops   
analyzed at machine speed. In other words, increas­  
ing tempo requires a robust network, structured data,   
and analysis—including AI-driven analysis—to create   
advantage, a dynamic on display in Ukrainian inno­  
vations like the Delta common operating picture and   
multiple fires applications.25 It also speaks to the logic   
of pulsed operations and other core concepts in the   
U.S. Joint Warfighting Concept.26  
Information, Operational Art, and   
the Changing Character of War  
Modern warfare is undergoing a transformation in   
which information is no longer just a combat mul­  
tiplier—it is the battle space. The ability to collect,   
fuse, and disseminate information now defines mil­  
itary power, shaping how forces mass, maneuver,   
and achieve surprise. On increasingly transparent   
battlefields where commercial satellites, drones,   
signals intelligence, and human networks operate in   
real time, the traditional calculus of force ratios and   
firepower must be reimagined.   
Two recent campaigns illustrate this shift. In   
July and August 2024, Ukraine launched its boldest   
cross-border operation of the war, penetrating deep   
into Russia’s Kursk region using a combination of   
reconnaissance-strike networks, mobile brigades,   
and electronic warfare to fracture Russian battle net­  
works. Months later, Israel executed a meticulously   
sequenced campaign against Iran’s missile infrastruc­  
ture and regional proxies, blending airpower, cyber   
operations, and psychological warfare to target not   
just enemy systems but also enemy perception. In   
both cases, operational success depended not on   
overwhelming force alone but on the ability to shape   
the information environment, degrade adversary   
coherence, and achieve tempo through decision   
dominance. Together, these cases point to a new   
theory of combined arms—one in which intelligence,   
surveillance, and reconnaissance (ISR), cyber, elec­  
tromagnetic operations, and influence campaigns are

**Page 44**

38  
Operational Art in the Age of Battle Networks  
tance, a coordinated multi-wave strike on Iranian   
military targets across the country.29 The operation,   
unprecedented in scale and precision, hit over 20   
high-value sites, including solid-fuel missile produc­  
tion facilities, long-range radar systems, and key com­  
ponents of Iran’s integrated air defense network.30   
Although framed publicly as retaliation for Iran’s   
massive October 1 missile and drone salvo, the strikes   
were far more than a proportional response. Rather,   
these complex attacks were the visible climax of a   
meticulously sequenced campaign—months in the   
making—that fused airpower, cyber operations, elec­  
tronic warfare, and covert action into an integrated   
operational design. Israel did not just strike infrastruc­  
ture; it targeted the logic of Iran’s battle networks,   
disrupted proxy coordination, and used information   
as a weapon to generate psychological shock across   
the enemy system. What looked like an air strike was,   
in reality, a campaign to undermine Tehran’s con­  
fidence in its ability to withstand future strikes and   
launch retaliatory strikes, a reality brought to fruition   
in Israeli’s punishing 12-day campaign in June 2025. In   
other words, the campaign targeted the enemy’s sense   
of coherence and leaders’ perception of survivability   
while setting conditions for follow-on operations.  
Israel’s 2024 campaign against Iran and its proxy   
network was not a single air strike or even a week   
of bombardment. It was the culmination of a phased   
multidomain operation that fused conventional pre­  
cision, unconventional disruption, and psychological   
warfare into a coherent effort to degrade Iran’s capac­  
ity to project power and force its leaders to question   
their networks, decisions, and security.  
At its core, this was a campaign against battle   
networks, which for Tehran consist of command and   
control systems, sensor architectures, and proxy   
infrastructure that allow Iran and its regional allies   
to operate as a distributed but connected strike com­  
plex. Israel took an indirect, sequential approach,   
opting to generate effects over time as opposed to   
seeking one decisive knockout blow that was almost   
certain to draw it into a larger war. By conducting a   
series of shaping activities targeting Iranian networks   
over months, striking them with precision and sowing   
cognitive dislocation among their operators, Israel   
ate surprise against a more numerous but potentially   
slower-to-adapt adversary. In terms of the principles   
of offense and mass, Ukraine transitioned from a   
largely defensive posture to a fast, deep penetration   
based on infiltration that exposed gaps. The high   
tempo of mechanized thrusts and the swift capture   
of Russian territory reflect a desire to stun the Rus­  
sian command structure—what military theorist John   
Antal calls “battleshock.”28 Instead of using brute-  
force numbers, Ukraine is using “affordable mass”   
via FPVs and other drones to support mechanized   
brigades maneuvering based on real-time intelli­  
gence and electronic warfare. By synchronizing mul­  
tiple brigades in at least two axes of advance, Ukraine   
seeks to overload Russian response efforts rather than   
simply present a large, static force.  
In terms of the principles of maneuver and secu­  
rity, the Kursk campaign demonstrated how to place   
the enemy in a position of disadvantage through the   
flexible application of combat power. Ukraine’s deep   
incursion—potentially tens of kilometers into Russian   
territory in the opening stages—enabled them to keep   
Russian forces off-balance. Maneuver encompassed   
not only physical envelopment but also electromag­  
netic and cyber elements. Ukraine jammed Russian   
communications and integrated intelligence from   
multiple sources to target Russia’s weak points. This   
ability to rapidly identify and exploit gaps in the Rus­  
sian line was related to Ukrainian operational secu­  
rity measures. Ukraine’s success underscored how   
effective security in planning can achieve operational   
surprise. By masking intent, ensuring tight operations   
security, and possibly feeding deceptive indicators to   
Russian intelligence, Ukraine prevented Russia from   
reinforcing Kursk quickly. In withdrawing from Kursk,   
Ukraine also demonstrated the impost of securing its   
long supply lines and flanks within Russian territo­  
ry—a key tactical vulnerability.   
Battle Shock and Broken Networks:   
How Israel Fused Conventional and   
Unconventional Operations to Rewire   
Deterrence  
In the early hours of October 25, 2024, over 100   
Israeli aircraft launched Operation Days of Repen­

**Page 45**

39  
Benjamin Jensen  
of war by and through battle networks. First, consider   
the principle of objective and the need to ensure every   
military action is directed toward a clearly defined   
and achievable end. In the campaign, the objective   
appeared to be eroding Iran’s ability to mass and launch   
precision missiles at Israel. By degrading missile pro­  
duction nodes and battle network infrastructure, Israel   
reduced near-term threats without widening the war.  
Two additional principles help frame the cam­  
paign: offensive and maneuver. Israel seized and   
retained the initiative through a three-wave strike   
campaign, using air-launched standoff munitions   
to force Iran into a reactive posture.34 And this strat­  
egy was not just geographic. Israel maneuvered in   
the electromagnetic spectrum—jamming, spoofing,   
and disabling radar systems—and in cognitive space   
by compelling Iranian leaders to question the integ­  
rity of their command networks and the accuracy of   
their information picture. Rather than strike sym­  
bolic or escalatory targets (e.g., oil infrastructure,   
nuclear sites, or regime leadership), Israel concen­  
trated advanced munitions and assets in the October   
campaign on key enablers of Iran’s strike complex,   
essentially reducing its viability and signaling its abil­  
ity to hold other targets at risk. This preserved mis­  
sile defense reserves, ensured strategic restraint, and   
sustained readiness for follow-on operations. Perhaps   
the most profound aspect is that Israel did not just   
protect its forces, it made Iranian commanders feel   
insecure. By striking deep targets without warning,   
disrupting early warning networks, and demonstrat­  
ing the ability to kill leaders in the heart of Tehran,   
Israel demonstrated its ability to impose costs.  
Taken as a whole, Israel’s campaign demonstrates   
that modern battle networks exist not just in servers,   
satellites, or sensor arrays but also in the minds of their   
operators. Israeli planners understood that disrupting   
data links and radar systems would go only so far. The   
real target was perception, which is why Israel likely   
integrated cyber operations to delay enemy reaction   
time, degrade command coordination, and injected   
doubt into decision chains. Israeli Air Force F-35Is,   
with their suite of passive sensors and electronic war­  
fare capabilities, likely mapped and disrupted Iranian   
air defense systems in real time. Paired with standoff   
demonstrated how information is no longer just about   
passing data across systems; it is about how leaders   
perceive the world around them—and whether they still   
believe their systems will hold.  
This campaign began not with a missile, but with   
a message. In late July 2024, a senior Hamas official   
was assassinated in central Tehran—one of the most   
secure areas in the Islamic republic.31 The strike was   
not random; it was symbolic and surgical. It punc­  
tured the idea that Iran could protect key nodes in its   
regional proxy network, and it forced senior officials   
in Tehran to ask a dangerous question: If they got him,   
who is next?  
This covert action was followed by escalating   
strikes in southern Lebanon, including a September   
attack on a Hezbollah command site and a sabotage   
campaign that took thousands of fighters off the bat­  
tlefield by blowing up their communications devices   
(i.e., pagers, radios).32 These operations reflected a   
deliberate focus on battle networks—degrading not   
just shooters or missiles but also the communication   
and coordination layers that allow Iranian and proxy   
forces to act as a system.  
This shaping phase—covert, psychological, and   
electromagnetic—laid the foundation for what came   
next. And it was not just about killing leaders or   
destroying assets; it was about fragmenting adver­  
sary situational awareness. In modern war, battle   
networks are the central nervous system. Israel was   
not trying to defeat a massed army; it was disabling a   
distributed brain to gain a position of advantage over   
its much larger rival, Iran.  
When Israeli aircraft launched a multi-wave strike   
on October 25, 2024, targeting 20 Iranian military   
sites across the country, it was the kinetic crescendo   
of a campaign designed to change Iran’s decision   
calculus. The targets included missile production   
facilities essential to Iran’s solid-fuel ballistic missile   
arsenal and high-end radar systems like the S-300.33   
This shaping would prove critical in the June 2025   
campaign in which Israel demonstrated its ability to   
attack targets across Iran.   
From an operational perspective, the campaign   
aligned with key principles of war, adapted to an area

**Page 46**

40  
Operational Art in the Age of Battle Networks  
is about generating converging dilemmas at speed   
across domains and denying adversaries the ability   
to process what is happening until it is too late. The   
campaigns examined here reflect more than adapta­  
tion in real time; they offer blueprints for the future   
of warfare.  
Implication 1: Future campaigns will be built   
around adaptive kill webs.  
Ukraine’s battlefield innovation demonstrates   
that modern campaigns will be increasingly defined   
by software-defined kill webs that can be rapidly   
reconfigured under fire. In Kursk, Ukraine combined   
drone reconnaissance, open-source targeting, and   
decentralized command nodes to fracture Russian   
battle networks. These operations were not linear.   
They were modular, pulsed, and responsive to real-  
time intelligence. Future military formations, partic­  
ularly for smaller or outnumbered states, will need to   
emulate this model by fusing civilian and military ISR,   
applying real-time analytics, and pushing decision   
authority down to frontline echelons. In this world,   
survivability is not just about armor; it is about adap­  
tation at the speed of relevance.  
Implication 2: Strategic effects will come   
from information-driven shock.  
Israel’s 2024 air campaign revealed that the most   
powerful strike is not always kinetic. It is the one that   
fractures an adversary’s perception of control. From   
the assassination in Tehran to coordinated cyber and   
electronic warfare attacks, Israel targeted not just   
radar sites and missile factories but also the cogni­  
tive coherence of Iran’s battle network. The lesson   
jamming platforms and coordinated decoy opera­  
tions, these actions rendered Iran’s most advanced   
radar systems functionally blind.  
But even more important, the campaign created   
informational fog for Iran’s leadership. In a regime   
where trust is already precarious and decisionmaking   
centralized, the sudden loss of awareness—combined   
with fear of further targeted assassinations—frayed   
coherence across Tehran’s national security appara­  
tus. This is the modern adaptation of battle shock: not   
just sudden violence but calculated disorientation;   
a break in trust, not just a break in infrastructure; a   
feeling that no network is safe, no command center   
secure, no bunker deep enough.  
As a result, Israel’s 2024 campaign was more than   
a response to missile salvos. It was a case study in how   
operational art adapts to an age of systems warfare   
and cognitive contestation. By attacking the connec­  
tive tissue of Iran’s battle networks, Israel degraded   
not only strike capabilities but also the belief that   
those capabilities could function under fire. These   
effects set the conditions for the deeper campaign   
Israel launched in June 2025 that significantly set back   
Iran’s missile inventory, nuclear sites, air defenses,   
and even military leadership.  
This is the essence of modern deterrence: not just   
the ability to retaliate but also the ability to create per­  
sistent uncertainty—a psychological edge that makes   
adversaries hesitate. In this campaign, Israel did not   
just pass data faster or fire further. It weaponized per­  
ception, shattered battle networks, and rewrote the   
strategic calculus in Tehran—not through occupation   
but by eroding confidence from the inside out.  
Conclusion  
From the campaign in Kursk and the skies of Tehran,   
contemporary military operations reveal a world in   
which the decisive terrain is not just geographic—it   
is digital, electromagnetic, and psychological. The   
integration of sensors, shooters, and decisionmak­  
ers into fused battle networks is redefining how   
states generate combat power. These cases show   
that operational art in the twenty-first century is no   
longer about massing forces at a decisive point. It   
From the campaign in Kursk and   
the skies of Tehran, contemporary   
military operations reveal a world   
in which the decisive terrain is   
not just geographic—it is digital,   
electromagnetic, and psychological.

**Page 47**

41  
Benjamin Jensen  
for future deterrence and coercion campaigns is clear.   
The side that can inject uncertainty into decisionmak­  
ing loops, fracture trust in systems, and make leaders   
feel personally vulnerable will shape strategic out­  
comes long before a single brigade deploys. Informa­  
tion is not just a force multiplier; it is a weapon of war.  
Implication 3: Multidomain operations will   
prioritize tempo.   
Israel’s multidomain campaign—synchronizing   
F-35 sensor fusion, cyber operations, decoys, and   
standoff munitions—demonstrates that the future of   
operational art is about shaping time more than ter­  
rain. Maneuver now happens across the electromag­  
netic spectrum, cyberspace, and strategic narrative,   
all while creating tempo that overloads adversary   
systems. In this vision, “seizing the initiative” means   
disrupting adversary kill chains, fragmenting their   
information picture, and making their battle rhythm   
irrelevant. Tomorrow’s campaigns will succeed by   
making adversaries hesitate, misallocate resources,   
and react to illusions until their networks and confi­  
dence collapse.

**Page 48**

Benjamin Jensen  
CHAPTER 05  
The Evolution of   
Landpower

**Page 49**

43  
Benjamin Jensen  
”  
“  
Landpower remains indispensable as the hub   
that sustains and integrates operations across   
air, sea, space, and cyber domains. There is   
no airpower without airports. There is no   
seapower with major ports. There is no cyber   
or space power without digital infrastructure,   
ground stations, and launch platforms.  
hinged on the value of territory in the land domain.   
Great battles remain fought by people over land, and   
the domain plays a central role at every level of war.  
But land is not just the object of campaigns, it is   
the medium through which adversaries access other   
domains. In a world of satellites, precision munitions,   
and networked warfare, the initial campaign of the   
war in Ukraine underscored an enduring reality:   
Landpower remains indispensable as the hub that   
sustains and integrates operations across air, sea,   
space, and cyber domains. There is no airpower with­  
out airports. There is no seapower with major ports.   
There is no cyber or space power without digital infra­  
structure, ground stations, and launch platforms.   
Landpower in the twenty-first century is neither   
eclipsed by technology nor rendered obsolete by   
distant-strike capabilities and the increasing impor­  
tance of other domains. It evolves with new doc­  
trines, and technology, such as artificial intelligence   
and machine learning (AI/ML) and cyber integration.   
Yet it endures in its fundamental role. Cyberspace   
I  
n late February 2022, Russian forces launched   
a full-scale invasion of Ukraine. Within hours,   
columns of tanks rolled across borders, missiles   
launched from the air and sea struck airfields, and   
cyberattacks targeted communication systems. Yet   
amid these varied assault vectors, the defining strug­  
gle in the war’s early phase—Russia’s attempt to encir­  
cle Kyiv and seize critical lodgments like the Hostomel   
airport—was for land.1   
Despite Russia’s initial multidomain salvo, com­  
prising long-range fires, cyberattacks, and electronic   
warfare, the Ukrainian defense hinged on organized   
ground resistance. Soldiers and territorial volunteers   
held the capital’s outskirts and prevented Russian   
paratroopers from establishing a key air bridge at   
Hostomel. A mix of former tech executives turned   
drone operators and special forces teams launched   
ambushes along Russian armored columns reminis­  
cent of Finnish motti tactics from the Winter War.2   
These activities at the tactical level denied Moscow’s   
operational objective of rapidly seizing Kyiv in a   
lightning 10-day campaign. In other words, strategy   
photo: leon neal/getty images

**Page 50**

44  
The Evolution of Landpower  
works complicate massing forces.6 This condition has   
become increasingly acute with the rise of the trans­  
parent battlefield, where even small or medium-sized   
countries can network drones to deny maneuver.7   
Modern multidomain operations seek to use long-  
range fires to change battlefield conditions and enable   
maneuver. Multidomain operations revolve around   
penetrating layered defenses, such as anti-access/  
area denial (A2/AD) networks, to disrupt an adver­  
sary’s depth and create exploitable corridors.8 The   
concept is consistent with the “pulse attacks” envi­  
sioned by the Joint Warfighting Concept, which will   
increasingly rely on coordinated effects across space,   
cyberspace, and more traditional land, air, and mari­  
time domains.9 At the same time, modern landpower   
has to increasingly contend with how information   
changes politics and puts a premium on understand­  
ing human terrain.10 Long-range strikes happen along­  
side computational propaganda campaigns, creating   
a new form of political warfare.11 Seen in this light,   
Isserson’s key insight—that changes in technology   
(e.g., mechanization, long-range fires) drive doctrinal   
evolution but never negate the human requirement   
to seize ground—continues to inform contemporary   
landpower debates.   
The political utility of landpower remains its role   
in adding credibility to strategic deterrence through   
forward-deployed forces ranging from trip wires to   
large coalition formations designed to prevent a con­  
ventional fait accompli attack and provide options to   
seize key terrain.12 Traditionally, the seat of power has   
been on land, defined by both political and economic   
points. These hubs—such as capital cities, mountain   
passes, and ports located on critical sea lines of com­  
munication—provided the aimpoints for campaigns   
for centuries.   
Yet, increasingly, there is a new logic to land­  
power. Hubs on land anchor how militaries connect   
their forces to project combat power across multi­  
ple domains. In other words, landpower anchors   
the entire warfighting architecture.13 As highlighted   
above, ports supply navies, runways host and main­  
tain airpower, ground stations control satellites, and   
fiber-optic cables house the internet’s spine. Absent   
secure territorial footholds, domain capabilities   
relies on servers and fiber-optic cables housed on the   
ground. Ultimately, political and strategic outcomes   
still hinge on who holds which territory, for how   
long, and at what cost.  
The chapter proceeds by adapting naval theory   
to reconceptualize twenty-first-century landpower.   
Using Sir Julian Corbett’s ideas as a guide, it proposes   
seeing land as a hub connecting other domains.   
This perspective is then illustrated through a series   
of vignettes analyzing how Ukraine, China, and the   
United States are using land-based forces to generate   
effects in other domains. The chapter concludes by   
drawing three implications about the future of war.   
First, future campaigns will need to focus on securing   
strategic ground-based infrastructure that includes   
not just air and naval ports but space-based hubs and   
data infrastructure. Second, combined arms now   
means combined domains where land serves as a   
gateway to effects in air, sea, cyberspace, and space.   
Last, there is a larger competition over critical infra­  
structure likely to define both competition and warf­  
ighting in the coming decades.   
What Has Changed:   
Depth and Domains  
A persistent theme in the evolution of modern land   
warfare is disrupting adversaries across the depth of   
battlespace to enable maneuver. If a force can move,   
it can threaten adversary centers of gravity, thus   
compelling surrender or inviting destruction. Early   
twentieth-century Soviet theorist Georgii Isserson   
charted the changing character of war in relation to   
how politics and technology create new epochs.3 His   
notion of successive “epochs of warfare” predicted   
that once continuous fronts became the norm (as in   
World War I), future battles would require deep opera­  
tions to bypass linear defenses. This thinking inspired   
Soviet deep battle doctrine, which remains relevant   
in the twenty-first century.4 It also provides a larger   
conceptual foundation for modern combined arms   
maneuver and writings from Liddell Hart and Mikhail   
Tukhachevsky about how to break static fronts.5 And   
since the late Cold War, concerns about combined   
arms maneuver have had to grapple with the challenge   
of how precision weapons and modern battle net­

**Page 51**

45  
Benjamin Jensen  
from intelligence updates to positioning, navigation,   
and timing (PNT) support to targeting. Even space and   
cyberspace depend on land-based infrastructure rang­  
ing from downlink stations and fiber-optic cables to   
data centers and launch platforms. Corbett’s land-sea   
integration model should be expanded into a land-cen­  
tric model for multidomain operations, where control   
of ports, airports, cyber hubs, and space infrastruc­  
ture determines the ability to conduct effective mili­  
tary operations across all domains.   
How Land Hubs Shape Modern   
Military Competition and   
Campaigns   
Corbett’s concept of “disputed command”—the idea   
that no force can achieve total dominance at sea and   
must instead focus on controlling key areas—applies   
directly to modern multidomain operations. In this   
framework, seizing and holding at risk key land-based   
infrastructure such as ports, space launch sites, and   
data centers determines the flow of effects across   
domains. Three cases, laid out in the sections below,   
demonstrate this logic.   
China’s Infrastructure Strategy  
Contrary to much of the scholarship, China’s mili­  
tarization of artificial islands in the South China Sea   
is not just a maritime gray zone tactic.22 Rather, it   
reflects an enduring truth about war: Land remains   
the hub through which great powers generate and   
sustain cross-domain advantage. Drawing from Cor­  
bett’s theory of limited maritime command, Beijing’s   
strategy is not singularly about coercion beneath   
the threshold of war. Instead, these activities shape   
the theater and set conditions by extending Beijing’s   
A2/AD bubble and creating opportunities for power   
projection. Seen in this light, beyond coercion, mili­  
tarized islands help Beijing generate the air and mar­  
itime power required to support future sea control   
operations that complicate U.S. and allied planning.23   
These artificial island hubs serve as forward oper­  
ating bases, sensor nodes, and logistics platforms—  
critical nodes in China’s evolving battle network.   
They enable the People’s Liberation Army (PLA) to   
extend surveillance and strike reach far beyond the   
wither. Joint all-domain warfare and the “symphony   
of capabilities” called for in the Joint Warfighting Con­  
cept require fusing effects across multiple domains.   
This logic suggests a need to revisit how soldiers, pol­  
icymakers, and analysts conceptualize the utility of   
landpower.   
The Land-Sea Interaction as a   
Model for Multidomain Warfare  
Sir Julian Corbett (1854–1922) is remembered as a   
leading naval theorist, but his ideas help understand   
the centrality of land as a gateway to joint all-domain   
operations. His seminal work, Some Principles of Mar­  
itime Strategy (1911), challenged conventional naval   
thought by emphasizing that maritime power is inher­  
ently tied to operations on land.14 Unlike American   
naval theorist Alfred Thayer Mahan (1840–1914), who   
championed decisive naval engagements and total   
sea control, Corbett argued that true strategic suc­  
cess required the integration of sea and landpower.15   
Over the last generation, scholars and practi­  
tioners have applied this insight to new domains,   
including space and cyberspace.16 This chapter   
expands Corbett’s original insight even further.17 The   
land is no longer just a strategic objective, with naval   
forces serving as a supporting element. It becomes a   
hub for connecting domains and waging joint all-do­  
main operations.18   
Just as Corbett emphasized that naval forces must   
influence events on land to be strategically decisive,   
modern joint forces must integrate land, sea, air,   
space, and cyber capabilities to achieve operational   
success. At the operational level, landpower serves   
as a means of both generating and denying effects in   
other domains in support of a larger campaign. Cor­  
bett’s logic dictates that airpower, like naval power, is   
fundamentally dependent on ground-based logistical   
support, radar stations, and air defense systems.19   
Modern naval forces cannot operate effectively   
without land-based resupply.20 Furthermore, modern   
naval campaigns operate as part of a network of   
coastal sensors and missile batteries central to modern   
concepts of sea denial.21 They also rely on satellites   
launched from ground sites to provide everything

**Page 52**

46  
The Evolution of Landpower  
In the maritime domain, the BRI has enabled   
China to construct a web of dual-use logistics nodes   
that support the evolution of the People’s Liberation   
Army Navy (PLAN) into a blue-water force. China’s   
first overseas base in Djibouti and key BRI-linked ports   
like Gwadar (Pakistan), Hambantota (Sri Lanka), and   
Doraleh (Djibouti) offer refueling, surveillance, and   
maintenance infrastructure for PLAN deployments   
in the Indian Ocean and Red Sea. These ports are   
not simply commercial. They are “strategic strong­  
points” designed to extend the reach of Chinese sea­  
power while providing platforms for intelligence,   
surveillance, and reconnaissance (ISR) collection   
and coercive diplomacy in times of crisis. During a   
Taiwan contingency, these positions could support   
PLAN surface action groups or submarines imposing   
a distant blockade, placing pressure on U.S. and allied   
resupply routes.  
Equally important is China’s Digital Silk Road   
(DSR), a pillar of the BRI aimed at exporting Chinese   
telecommunications technology, including 5G infra­  
structure, fiber-optic networks, smart-city surveil­  
lance systems, and undersea cables.27 Companies like   
Huawei and ZTE dominate many of these projects,   
often bundled with surveillance and facial recogni­  
tion systems that mirror China’s domestic “digital   
authoritarianism” model.28 Elements of this tech­  
nology are already installed in more than 80 coun­  
tries, providing China with not only soft power but   
also potential access to foreign data and signals intel­  
ligence. In strategic terms, China is creating digital   
terrain dependencies that allow Beijing to shape or   
even disrupt the information environment through   
technical infrastructure and software backdoors.  
The export of Chinese telecommunications sys­  
tems dovetails with the rise of the Space Silk Road.29   
Under the larger “Space Information Corridor”   
initiative, China is building and operating satellite   
ground stations and launch facilities in key partner   
countries, such as Argentina, Namibia, and Pakistan.   
These facilities support China’s growing satellite con­  
stellations, including the Beidou navigation system   
and remote-sensing platforms capable of supporting   
PLA C4ISR and precision strike operations. Beidou   
now offers global PNT services and is marketed as a   
mainland, fusing land-based radar, ship-borne sen­  
sors, and airborne early warning into an integrated   
architecture for command, control, communica­  
tions, computers, cyber, intelligence, surveillance,   
and reconnaissance (C5ISR).24 From these positions,   
China can deploy drones, patrol aircraft, naval militia   
vessels, and coast guard cutters in coordinated mari­  
time domain operations. This forward basing enables   
the PLA to sustain presence, monitor traffic, and hold   
at risk key chokepoints like the Bashi Channel and   
the Strait of Malacca—contested sea lines of commu­  
nication vital to both global commerce and regional   
military mobility.   
At the strategic level, these land hubs function   
as platforms for power projection and political war­  
fare. They support not only A2/AD operations but also   
economic and legal gray zone tactics—enabling Bei­  
jing to expand illegal fishing operations, intimidate   
rival claimants, and lay de facto claim to undersea   
resources, including hydrocarbons, gas fields, and   
mineral deposits beneath the South China Sea.25   
These actions mirror a broader trend: the use of land-  
based infrastructure to enable multidomain opera­  
tions that blur the line between conventional force   
projection and peacetime coercion. China’s artificial   
islands are not just concrete symbols of sovereignty—  
they are multidomain launchpads from which Beijing   
contests both physical access and legal norms in the   
Indo-Pacific. In this context, landpower becomes not   
just the foundation of military operations, but the   
platform for strategic influence.  
Second, China’s Belt and Road Initiative (BRI) is   
not just about trade routes or economic corridors. It   
is a global strategy to reshape the physical and digital   
terrain through which power is projected. BRI reflects   
a modern understanding of landpower as the con­  
nective tissue for multidomain influence. By build­  
ing, financing, or leasing key infrastructure around   
the globe—from ports and railways to data centers   
and satellite ground stations—Beijing is establishing   
positional advantage to shape maritime access, cyber­  
space architecture, and space operations.26 The stra­  
tegic logic mirrors Corbett’s foundational claim that   
the sea alone does not win wars; control over land is   
required to influence outcomes at sea and beyond.

**Page 53**

47  
Benjamin Jensen  
anchor point, from which forces can shape air, sea,   
space, and cyber operations. Whether striking stra­  
tegic bomber bases deep inside Russia, sinking the   
Moskva, or disabling satellite communications links in   
Crimea, Ukraine has exposed how control of terrain   
and infrastructure enables the projection of power   
across all domains. This is a war fought not only over   
territory, but over the systems that connect, sense,   
and strike across that territory.  
On February 25, 2022, Ukraine launched a Toch­  
ka-U ballistic missile strike on Russia’s Millerovo air   
base in Rostov Oblast, about 20 km from the border.30 ​  
The attack set hangars ablaze and destroyed at least   
one Russian Su-30SM fighter on the ground​. This early   
cross-border strike signaled Kyiv’s willingness and   
capability to target Russian military infrastructure   
from the outset. The surprise attack forced Russia to   
recognize its vulnerability at home, complicating Rus­  
sian air operations near the front and foreshadowing   
a broader Ukrainian strategy of hitting deep targets to   
disrupt Russian multidomain operations.   
On August 9, 2022, explosions rocked the   
Saky (Novofedorivka) airbase in Russian-occu­  
pied Crimea.31 ​The blasts, which Ukraine later   
implied were its doing, obliterated ammo depots   
and wrecked multiple Russian warplanes. Western   
intelligence assessed that over half of the Black Sea   
Fleet’s naval aviation combat jets were put out of   
use by the Saky strike.​ In its aftermath, Russia had   
to disperse or relocate remaining aircraft, degrading   
its ability to project airpower over the Black Sea and   
southern Ukraine.  
In another unprecedented long-range attack,   
Ukraine targeted the Dyagilevo airfield (over 450 km   
from Ukraine) on December 5, 2022, using modified   
Soviet-era drones.32​ The strike, aimed at disabling   
Russia’s strategic bombers, caused a fuel truck explo­  
sion that killed three personnel and injured others,   
and it reportedly damaged a Tu-22M3 nuclear-capable   
bomber. ​The ability of Ukraine to hit an airbase so   
deep in Russian territory underscored gaps in Russia’s   
air defenses and threatened its multidomain opera­  
tions by potentially limiting the sortie rate of strategic   
bombers used for cruise missile attacks on Ukraine.  
GPS alternative. By extending space infrastructure   
abroad, China ensures redundancy and global cover­  
age for its space assets, giving the PLA an advantage   
in a future blockade or counter-intervention scenario.  
The larger family of BRI initiatives thus provides   
China with a global network of land-based infrastruc­  
ture nodes that connect sensors, shooters, and deci­  
sionmakers—the essence of a modern battle network.   
In a Taiwan contingency, China may never need to   
encircle Taiwan directly. Instead, it can leverage this   
infrastructure to isolate the island digitally and eco­  
nomically. PLA doctrine, including exercises like Joint   
Sword-2024, points to the use of cyberattacks, elec­  
tronic warfare, and space-based ISR to sever Taiwan’s   
communications and raise the costs of U.S. interven­  
tion. Ground stations in the Middle East or Africa can   
relay data in support of operations in East Asia, while   
telecommunications dependencies can be used to   
shape the decisionmaking of foreign governments   
hesitant to side with Washington in a crisis.  
Ultimately, the BRI is not a traditional military alli­  
ance or a treaty network. It is a system of territorial   
dependencies through infrastructure. China is build­  
ing a multidomain campaign plan through roads,   
cables, ports, and satellites, all anchored on land. In   
this new logic of combined arms, land is not just the   
objective. It is the access point, the enabler, and the   
global amplifier of Chinese influence. Understand­  
ing how larger strategic initiatives like BRI generate   
“land power in being” in the age of battle networks   
is essential for U.S. strategists thinking about denial,   
disruption, and resilience in long-term competition.  
Killing Planes, Ships, and Satellites   
with Ground-Launched Effects   
One of the defining features of Ukraine’s evolving   
campaign is its ability to use land-based strikes to   
fracture Russian multidomain operations. From the   
outset of the war, Ukraine has demonstrated that   
long-range fires—whether delivered by ballistic mis­  
siles, drones, or cruise missile systems—can create   
strategic effects when precisely targeted at key air­  
fields, naval ports, and satellite communications   
centers. These operations reveal how land serves not   
merely as a battlespace, but as a hub, essentially an

**Page 54**

48  
The Evolution of Landpower  
denial operations. In the early weeks of the war,   
Ukraine targeted Russian naval forces using occu­  
pied ports as forward bases. On March 24, 2022, a   
Ukrainian Tochka-U ballistic missile struck a port on   
Ukraine’s Sea of Azov coast, where Russian Black Sea   
Fleet landing ships were unloading supplies.36​ The   
strike caused a massive explosion and fire, sinking the   
Alligator-class landing ship Saratov and heavily dam­  
aging two other Russian amphibious vessels docked   
nearby​. This attack eliminated a key asset for Russia’s   
planned amphibious operations and forced an abrupt   
withdrawal of the remaining landing ships from Berd­  
iansk. In effect, Ukraine’s missile strikes foiled Russia’s   
seaborne resupply efforts on that front and demon­  
strated that port facilities under Russian control were   
not safe from attack, disrupting Russia’s joint land-sea   
logistical operations in southern Ukraine.  
On April 13, 2022, Ukraine achieved a landmark   
naval victory by striking Russia’s Black Sea Fleet flag­  
ship, the cruiser Moskva.37 Ukrainian Neptune antiship   
cruise missiles hit the Moskva off the Ukrainian coast,   
igniting a fire and eventually sinking the 12,000-ton   
warship​. The loss of the Moskva—the largest Russian   
warship sunk in combat since World War II—was a   
major symbolic and operational blow to Russia’s navy​  
. As the fleet’s primary air defense ship, its sinking left   
Russian naval forces at greater risk from Ukrainian   
aircraft and missiles. After this incident, Russian war­  
ships pulled farther away from Ukraine’s coast​.   
Last, Ukraine attacked Russian targets on land to   
try and degrade Moscow’s access to space. In Decem­  
ber 2023, Ukrainian forces targeted a Russian satellite   
communication hub in Yevpatoriya, Crimea. Of note,   
this site was associated with coordinating GLONASS   
(i.e., Russian GPS) and a wide range of orbital activi­  
ties.38 The attack involved a mix of drones and cruise   
missiles. In June 2024, Ukrainian forces hit the facility   
again. Ukrainian sources identified the attack as the   
“second Ukrainian strike on [Russia’s] space warfare   
infrastructure” in Crimea.39 The attack likely com­  
pounded the damage to satellite dishes and commu­  
nication equipment from the first strike. Each of these   
blows further degrades Russia’s ability to use Crimea   
as a secure node for command and control via sat­  
ellite. By targeting ground-based satellite links and   
On August 19, 2023, a Ukrainian drone strike hit   
Soltsy-2 air base in northwestern Russia (about 650   
km from Ukraine), which hosts Tu-22M3 “Backfire”   
bombers​.33 This strike again highlighted Russia’s   
struggles to protect strategic assets deep inside its   
territory—a vulnerability that undermines its air   
domain supremacy. Following the strike, Russia hur­  
riedly relocated the remaining Tu-22M3 fleet to more   
remote airfields, revealing how Ukrainian deep strikes   
were steadily eroding Russia’s freedom of action in   
the air. The attack also served as a harbinger for even   
bolder attacks that would occur in 2025 like Opera­  
tion Spider Web and using special forces and drones   
to attack long-range bombers deep inside Russia.34  
In addition to using ground-launched, long-range   
drones, Ukraine has used U.S.-supplied ATACMS mis­  
siles to strike Russian airfields. On October 17, 2023,   
Ukrainian missiles struck the helicopters staged in   
Berdyansk and Luhansk.35 The twin strikes forced   
Russia to temporarily relocate surviving helicopters   
farther from the front,​ blunting its ability to support   
ground troops. Collectively, the ATACMS strikes   
demonstrated a significant evolution in Ukraine’s   
multidomain operations, combining precision mis­  
siles and special forces targeting to neutralize key Rus­  
sian aviation assets in one coordinated blow​.   
While the use of naval drones and air-launched   
cruise missiles have captured the headlines, Ukraine   
has also illustrated how to integrate ground-launched   
ballistic and antiship cruise missile strikes into sea   
Whether striking strategic bomber   
bases deep inside Russia, sinking   
the Moskva, or disabling satellite   
communications links in Crimea,   
Ukraine has exposed how control   
of terrain and infrastructure   
enables the projection of   
power across all domains.

**Page 55**

49  
Benjamin Jensen  
domains. This integration enables the MDTF to con­  
duct operations that combine kinetic strikes with   
cyber and electronic attacks, effectively targeting   
adversary command and control systems and creat­  
ing opportunities for joint force exploitation.​   
The MLR is designed as a stand-in force capable   
of conducting sea denial operations, particularly   
in contested maritime environments. It leverages   
Expeditionary Advanced Base Operations (EABO)   
to establish temporary, low-signature positions that   
can launch antiship missiles, conduct air defense, and   
support maritime domain awareness.45 The integra­  
tion of systems like the Navy/Marine Corps Expedi­  
tionary Ship Interdiction System (NMESIS) enhances   
the MLR’s ability to target enemy vessels effectively.   
The formation also includes more organic infantry   
than the MDTF and high-end mobile radar that allows   
it to coordinate surface and air search missions that   
support naval strike and sector air defense.46​   
Additionally, the MLR’s coordination with the   
Marine Expeditionary Force Information Group   
(MIG) allows for synchronized operations across   
the electromagnetic spectrum, cyber, and space   
domains.47 The group provides capabilities such as   
electronic warfare, signals intelligence, and informa­  
tion operations, ensuring that the MLR can operate   
effectively in the information environment and sup­  
port joint force objectives.  
Both the MDTF and MLR exemplify the U.S. mil­  
itary’s shift toward integrated, multi-domain opera­  
tions. By serving as agile hubs that coordinate effects   
across land, sea, air, space, cyber, and the electromag­  
netic spectrum, these units enhance the joint force’s   
ability to respond to complex threats and maintain   
strategic advantages in contested environments.  
Conclusions  
Landpower is not vanishing in the age of long-range   
fires and precision-guided munitions. Rather, it is   
transforming. As this chapter has shown, land remains   
the essential hub that links, sustains, and amplifies   
effects across domains. From the defense of Kyiv to   
drone strikes on strategic airfields, ports, and satellite   
arrays, Ukraine has illustrated that territorial control   
over-the-horizon radars, Ukraine is directly contest­  
ing Russia’s space and electronic dominance. These   
operations have implications beyond immediate bat­  
tlefield effects. They challenge Russia’s strategic situ­  
ational awareness and precision warfare capabilities   
(which rely on satellite guidance), thereby influencing   
the multidomain balance (land, air, sea, and space) in   
favor of Ukraine.  
Occupying Key Maritime Terrain   
Emerging littoral rotational forces like the U.S. Army’s   
Multi-Domain Task Force (MDTF) and the U.S. Marine   
Corps’ Marine Littoral Regiment (MLR) represent a   
significant shift in operational art. These formations   
emphasize the integration of capabilities across mul­  
tiple domains—land, sea, air, space, cyber, and the   
electromagnetic spectrum projected from littoral bat­  
tlespace.40 The units are designed to operate as agile,   
forward-deployed hubs, capable of coordinating and   
executing complex operations that challenge adver­  
saries across all domains of warfare.​ Neither the MDTF   
nor MLR is decisive in any one domain. Rather, the   
theory of victory is that they can generate effects in   
multiple domains to place the adversary on the horns   
of a dilemma, thus disrupting freedom of action.  
The MDTF is a brigade-sized formation tailored to   
penetrate and disintegrate adversary A2/AD systems.   
It integrates long-range precision fires—including a   
mix of land and sea cruise missiles—with non-kinetic   
capabilities, including cyber and electronic war­  
fare, to create multiple dilemmas for adversaries.41   
The formation also has organic air and counter–  
unmanned aircraft system (UAS) defense.42 Central   
to the MDTF’s effectiveness is the Multi-Domain   
Effects Battalion (MDEB), which synchronizes target­  
ing across domains, leveraging space-based sensors   
for real-time intelligence and coordinating cyber   
and electromagnetic spectrum operations to disrupt   
enemy networks.​43 These are coordinated with novel   
low-cost sensors, including long-endurance UASs and   
high-altitude balloons.44   
The MDTF’s structure includes components   
such as the Intelligence, Information, Cyber, Elec­  
tronic Warfare, and Space (I2CEWS) battalion, which   
ensures seamless integration of operations across

**Page 56**

50  
The Evolution of Landpower  
converging dilemmas for adversaries. The MDTF’s   
Multi-Domain Effects Battalion and the MLR’s coor­  
dination with the MIG show that command nodes   
must now integrate not just fires and maneuver, but   
sensing, spoofing, jamming, and even narrative con­  
trol. In effect, multidomain formations are emerging   
as the new combined arms teams—agile, integrated,   
and capable of commanding terrain in both the phys­  
ical and information space.  
Implication 3: Strategic competition is a   
battle of infrastructure.  
Finally, the broader logic of China’s BRI—includ­  
ing its extension into digital and space infrastructure—  
alongside its militarized island strategy highlights   
that the future of great power competition will hinge   
less on massed formations and more on positional   
advantage. China is building the physical scaffolding   
for a global battle network—ports, data centers, and   
ground stations—that can project power and support   
coercion at a distance. In this context, strategic com­  
petition becomes a race to build, access, and pro­  
tect key infrastructure nodes across the globe. Like   
the United Kingdom building coaling stations and   
laying undersea cables in the past, Beijing is laying   
the foundations for global reach in the age of sensors,   
satellites, and digital terrain. For U.S. strategists, this   
means deterrence and campaigning must account not   
just for military postures, but for the infrastructure   
ecosystems that allow domain integration. In the age   
of multidomain operations, holding the high ground   
often begins with holding the right hub.  
and infrastructure access remain central to projecting   
power in modern warfare. Likewise, China’s milita­  
rized islands and BRI infrastructure demonstrate how   
states use physical footholds to enable distributed   
operations in cyberspace and space and across the   
electromagnetic spectrum. Modern landpower does   
not just seize ground. It shapes the strategic environ­  
ment across domains. In short, land is no longer just   
where wars are fought. It is the platform from which   
they are connected, contested, and won.  
Implication 1: Secure terrain is strategic   
infrastructure.  
The first implication is that future campaigns will   
hinge on the ability to secure and deny access to key   
land-based infrastructure—airfields, ports, ground   
stations, fiber-optic hubs, and satellite uplinks. As   
seen in Ukraine’s ATACMS strikes on the Berdiansk   
and Luhansk airfields and its attack on the Yevpa­  
toriya space communications hub, controlling or   
disrupting critical ground nodes can dismantle an   
adversary’s multidomain battle network. For oper­  
ational planners, this means the geography of future   
conflict will expand beyond front lines to include   
“strategic terrain” tied to logistics, sensing, and   
information flows. The side that can hold or disrupt   
these land-based hubs will set the tempo across all   
domains. As Ukraine’s campaign demonstrates, even   
a nation under invasion can impose strategic effects if   
it understands and targets the warfighting infrastruc­  
ture that enables adversary operations.  
Implication 2: Combined arms now means   
combined domains.  
Second, the evolution of the U.S. Army’s MDTF   
and the Marine Corps’ MLR underscores that modern   
combined arms no longer simply means integrating   
tanks, artillery, and infantry—it means synchroniz­  
ing effects across land, sea, air, space, cyber, and   
the electromagnetic spectrum. This concept is at   
the core of the new Joint Warfighting Concept and   
Joint All-Domain Operations, as well as part of Army   
doctrine.48 Hence, the future is likely to resemble the   
present but with greater ability for land-based units   
to generate effects in multiple domains. These units   
act as forward-deployed hubs capable of generating

**Page 57**

Tom Karako and Hannah Freeman  
CHAPTER 06  
The Enduring Role of Fires   
on the Modern Battlefield

**Page 58**

52  
The Enduring Role of Fires on the Modern Battlefield  
”  
“  
The future of warfare will likely be   
characterized by an increased demand   
signal for offensive and defensive fires.  
Trends affecting the demand for fires include the   
diffusion of precision guidance and its marriage with   
pervasive surveillance and targeting abilities. In a   
transparent battlefield, anything can be targeted, and   
in a world full of precision-guided munitions, every­  
thing will be. Weapon systems development likewise   
reflects these trends. Today, virtually all rockets are   
equipped with guidance of some kind, and almost all   
gravity bombs are smart bombs.   
The reign of fires, both offensive and defensive, is   
at little risk of being toppled. Today’s new missile age   
is defined by a surge in the global supply and demand   
for a spectrum of standoff strike capability and the   
means to counter it. Air defenses and long-range mis­  
siles have consistently been the Ukrainian govern­  
ment’s top two requests for aid. The United States   
has significantly increased spending on long-range   
strike since Russia’s 2014 invasion and occupation of   
Crimea, and this trend is unlikely to change anytime   
soon (Figure 6.1). Air and missile defense (AMD) and   
long-range precision fires are likewise the top-two   
F  
rom time to time, commentators opine that   
emerging technology will make some tradi­  
tional features of war obsolete. These pre­  
dictions are almost invariably premature. The use of   
antitank weapons in Ukraine was initially received   
as signaling the death of armor.1 The arrival of mass   
unmanned platforms on land, sea, and air, likewise,   
has been accompanied by predictions of the death   
of platforms such as advanced tactical aircraft and   
ships.2 The advent of numerous means of non-kinetic   
and electronic warfare has been occasioned by pre­  
dictions that they will render traditional kinetic fires,   
if not a thing of the past, at least less important than   
they have been.   
Artillery has long been known as the “king of   
battle,” and for good reason. In virtually every major   
land conflict for centuries, artillery and missilery have   
accounted for the vast majority of casualties. Instead   
of becoming less relevant, the future of warfare will   
likely be characterized by an increased demand signal   
for offensive and defensive fires.  
photo: official u.s. army photo

**Page 59**

53  
Tom Karako and Hannah Freeman  
dispatch, cause to go, let go, release, discharge.”4   
A missilis is something “that may be hurled or cast,   
that is thrown or hurled.”5 The words “mission” and   
“emissary” share this etymology—thus the old saw in   
diplomatic circles that an ambassador is “an honest   
man sent to lie abroad for the good of his country.”6   
In the early days of the first missile age, distinc­  
tions were made between the terms “rocket” and   
“missile,” with the latter usually reserved for projec­  
tiles that are guided rather than unguided. Thus, a   
simple Katyusha rocket was distinguished from an   
Atlas missile, though the distinction was somewhat   
artificial. At bottom, a missile is simply a thing that   
is sent. When the 2019 Marine Corps commandant   
declared in his guidance document that the opera­  
tional environment had become “an era of missile   
warfare,” it was a way of saying that there is a high   
supply and demand for standoff capability.7   
In today’s jargon, Iranian Shaheds are often   
referred to as one-way attack drones, loitering muni­  
tions, remotely piloted aircraft, Group 3 unmanned   
aircraft systems (UASs), or some other turn of phrase.8   
Fundamentally, however, they are missiles: physical,   
kinetic delivery systems sent to accomplish some   
mission. In the past, air defenders had several basic   
categories to contend with, such as fixed wing (FW),   
modernization priorities for allied countries such as   
Australia and Japan.3  
Defensive fires have also assumed a newfound   
salience and reputation. Over the past four years,   
nearly every AMD system the United States or Israel   
operates has had successful engagements against mis­  
siles fired in anger, especially in Ukraine, the Red Sea,   
and in the defense of Israel. Only the Ground-based   
Midcourse Defense system, the system designed to   
intercept ICBMs, has not been operationally employed.  
The rest of this chapter is divided into six sec­  
tions. The first outlines the nature and character of   
missiles. The second, third, and fourth sections exam­  
ine lessons from Ukraine, the Red Sea, and Israel,   
respectively. The fifth assesses implications for the   
future, especially the salience of fires, and the sixth   
provides brief conclusions.  
What Is a Missile, Anyway?   
To understand the character of this new missile age, it   
is helpful to consider the nature and character of mis­  
silery. Given that the defense world has a penchant for   
jargon, word definitions and origins are one way to   
seek clarity amid confusion. In this case, it is helpful   
to recall the etymology of the word “missile,” which   
derives from the Latin verb mittere, meaning “to send,   
Figure 6.1: Conventional Strike Modernization, 2009–2026  
$0B  
$4B  
$8B  
$12B  
FY 2010  
FY 2012  
FY 2014  
FY 2016  
FY 2018  
FY 2020  
FY 2022  
FY 2024  
FY 2026  
Anti-armor/personnel  
Bombs  
Rockets, artillery, and mortars  
Standoﬀ  
Torpedoes  
Total Obligational Authority (in FY 2026 dollars)  
Source: DOD Comptroller data and CSIS analysis.

**Page 60**

54  
The Enduring Role of Fires on the Modern Battlefield  
as well as focus on the physical characteristics of sys­  
tems. A Shahed is, after all, a fixed-wing air-breathing   
threat not unlike the V-1 missiles of yesteryear.  
Lessons from Ukraine  
The last three years of the Ukraine conflict have   
yielded considerable case studies of the role of stand­  
off capability in the future of warfare. Hundreds of   
thousands of drones, cruise missiles, ballistic mis­  
siles, and even some hypersonic systems have been   
employed to great effect. As in wars past, the vast   
majority of casualties on both sides of the Ukraine   
war have resulted from artillery and missile attacks.   
Russia has made advances through its use of long-  
range strikes, but the effects have been insufficient to   
produce a decisive victory.   
At the outset of the war, Russian forces attempted   
to attack too many targets with too few missiles, a   
result of their underestimation of the scale of effort   
needed to accomplish their objectives.11 Analysts   
rotary wing (RW), tactical ballistic missile (TBM), and   
air-breathing threats (ABTs) such as cruise missiles   
(Table 6.1). The diffusion and increased reliability of   
guidance, propulsion, and targeting have led to the   
massive blurring of these categories.   
For this reason, it was entirely appropriate that   
the 2022 Missile Defense Review included UASs as   
part of its mandate.9 Countering UASs is such a prev­  
alent need that the mission is now part of U.S. Army   
basic training.10 Rather than creating a new threat   
category, however, it might be better to think about   
countering UASs as simply a new chapter of air and   
missile defense.   
For this reason, a new taxonomy will be needed   
to better explain the spectrum of objects sent in and   
through the air. With the ubiquitous availability of   
remotely piloted or autonomous systems, the char­  
acteristic of being unmanned will likely come to be   
taken for granted. A future taxonomy might deprior­  
itize the distinction between unmanned and manned   
Table 6.1: Traditional Air and Missile Defense Taxonomy  
   
Target  
Ballistic   
missile  
Cruise   
missile  
Rotary   
wing  
Fixed   
wing  
UAS   
groups   
1–3  
UAS   
groups   
4–5  
Rockets,   
artillery,   
and   
mortars  
System  
Terminal High Altitude Area   
Defense (THAAD)  
   
   
   
   
    
   
   
Patriot  
   
   
   
   
   
   
   
Indirect Fire Protection   
Capability (IFPC)  
   
   
   
   
   
   
   
Stinger  
   
   
   
   
   
   
   
Mobile-Low, Slow, Small   
Unmanned Aircraft   
Integrated Defeat System   
(M-LIDS)  
   
   
   
   
   
   
   
Counter-Rocket, Artillery,   
and Mortar (C-RAM)  
   
   
   
   
   
   
   
Directed Energy (DE), High-  
Power Microwave (HPM),   
and High-Energy Laser (HEL)  
   
   
   
   
   
   
   
Source: U.S. Department of the Army, U.S. Army Air and Missile Defense Operations (Washington, DC: U.S. Department of the Army,   
2020), https://irp.fas.org/doddir/army/fm3\_01.pdf.

**Page 61**

55  
Tom Karako and Hannah Freeman  
6.3). The overall neutralization rate of Russian mis­  
siles since the beginning of the conflict remains   
high, estimated at around 84 percent.13 Ukrainian   
air defenses have struggled the most with intercept­  
ing faster missiles, with Russian short-range ballistic   
missiles having the lowest successful intercept rate.14   
Even with a diminished frequency and a high inter­  
cept rate, sustained air attacks against Ukraine’s elec­  
trical grid increase the risk of exhausting Ukraine’s   
capacity to repair it, highlighting the importance of   
passive defense and the capacity to quickly reconsti­  
tute capabilities and infrastructure.15 In addition to   
degrading Ukraine’s electrical grid, the composition   
of Russian missile salvos since October 2022 suggests   
a secondary Russian goal of depleting Ukrainian air   
defense capacity.  
A combined arms approach remains critical to   
contending with Russian long-range fires. Opera­  
tional art will require incorporating new aerial assets   
into traditional formations and capabilities, which,   
in many cases, has not been done well by either side.   
Across domains, Ukrainian forces must use different   
combat arms simultaneously and effectively, includ­  
ing mechanized infantry, tanks, artillery, air defense,   
and antitank systems.16   
have noted a slow over-the-horizon targeting cycle,   
frequent shifts in targeting priorities, and irregular   
availability of precision-guided munitions (PGMs)   
on the Russian side. Russian failures after the initial   
period are attributable to Ukrainian defense tactics   
and poor Russian strategic planning. In this respect,   
the decisive edge may go to the side with the better   
surveillance and the ability to accelerate their tar­  
geting cycle. Conversely, new forms of countering   
missile threats may emerge from electromagnetic   
warfare: camouflage, concealment, and deception   
(CCD) and other means to thwart the intelligence, sur­  
veillance, and targeting that underlie an adversary’s   
standoff strike. The missiles or drones may always get   
through, but they may not get to the right place at the   
right time.   
Since the fall of 2022, Russia’s long-range air and   
missile attacks against Ukraine have become larger   
but less frequent as Russia has attempted to over­  
come the growing efficiency of Ukrainian air defenses   
(Figure 6.2).12   
Although Ukrainian air defenses have proved   
effective, especially since the influx of Western air   
defense systems in October and November 2022, no   
weapon system or operation is perfect (see Figure   
Figure 6.2: Russian Air and Missile Attacks on Ukrainian Civilian Infrastructure, 2022–2025  
0  
100  
50  
150  
Major attack (≥20 projectiles)   
Minor attack (<20 projectiles)  
Number of Attacks, Monthly  
2025  
2024  
2023  
Source: CSIS analysis of data from Air Force Command of Ukraine and General Staff of the Armed Forces of Ukraine.

**Page 62**

56  
The Enduring Role of Fires on the Modern Battlefield  
high-necessity systems or interceptors. An increase in   
short-range, low-cost intercept options means a cor­  
responding decrease in the number of longer-range,   
high-value interceptor vessels needed to defend   
larger areas. The U.S. Navy is reportedly looking at   
a Maritime PAC-3 MSE, which the Army produces in   
greater quantities than the SM-6.18 It seems likely that   
navies will look to supplement maritime counter-UAS   
capacity as well, even if resources must be taken from   
land-based systems.19  
The USS Carney has thus far set the standard for   
successful air defense engagements at sea—a standard   
that has been replicated many times since October   
2023. Recently, the Navy detailed the types and quan­  
tities of intercept methods used in engagements with   
more than 400 Houthi-launched aerial threats (Table   
6.2). The wide variety of Standard and Evolved Sea   
Sparrow missiles used highlights the cost-exchange   
fallacy: A commander is sure to decide that a grave   
threat to the safety of the crew is worth the cost of an   
interception.   
The challenges and successes of the U.S. Navy   
in the Red Sea have demonstrated the effectiveness   
of missile defense technology in an active weapons   
Lessons from Red Sea Operations  
Another critical case study is the protracted conflict   
with the Houthis in the Red Sea, which has been   
marked by numerous tactical successes for U.S. AMD   
forces. A frequent refrain in popular commentary on   
the engagement has been the cost-exchange ratio,   
measuring the cost of a threat missile against the cost   
of a defensive interceptor. While lower-cost intercep­  
tors exist, they come with greater operational risk due   
to their limited range and capabilities.17 When a $2   
billion warship is at risk, the cost trade-off of shooting   
down a cheaply manufactured threat with a sophisti­  
cated interceptor is no longer so unfavorable. While   
the cost ratio of an offensive missile to a defensive   
interceptor is a valid one to consider, it also reflects   
a partial perspective. A more complete assessment   
would consider other factors, including the value of   
the defended asset, the operational cost of failing to   
defend, and the ratio of combined arms activity by   
both sides.  
For ship-based air defenses, inventory limitations   
have proved a restrictive factor. With only so much   
capacity on board, equipping a ship with numer­  
ous low-cost options limits the space available for   
Figure 6.3: Intercept Rates of Russian Air and Missile Attacks on Ukrainian Civilian Infra­  
structure, 2022–2025  
All attacks  
100%  
80%  
60%  
40%  
Percent Intercepted, Monthly  
Major attack (≥20 projectiles)   
Minor attack (<20 projectiles)  
2023  
2024  
2025  
Source: CSIS analysis of data from Air Force Command of Ukraine and General Staff of the Armed Forces of Ukraine.

**Page 63**

57  
Tom Karako and Hannah Freeman  
and structured air and missile attack. It also repre­  
sented the single largest number of same-day AMD   
engagements in history. Another attack in October   
2024 included a wave of approximately 200 ballistic   
missiles launched from Iran.23 In both cases, a rela­  
tively small number of missiles reached their targets.  
The importance of effective AMD capabilities was   
once again made clear in the Israel-Iran conflict in   
June 2025.24 Over the course of the 12-day conflict, Iran   
launched a series of missile attacks at Israel. Accord­  
ing to reports of Israel Defense Forces estimates, these   
included approximately 550 ballistic missiles and   
1,000 drones.25 While Israel’s layered missile defense   
systems were largely successful in responding to the   
incoming strikes, their efficacy was increasingly chal­  
lenged as the conflict progressed, and Israel and the   
United States expended large numbers of intercep­  
tors, forcing difficult choices about which assets to   
defend, and potentially changing shot doctrine.26   
In addition, U.S. air defenders reportedly fired   
more than 150 Terminal High-Altitude Area Defense   
(THAAD) missiles, almost a quarter of the total number   
the United States military has purchased in its history.   
The number expended will likely take years to replace.27   
Israeli officials reported concern about the ability of   
their interceptor stockpiles to outlast successive Ira­  
nian missile attacks, with one former official saying   
that interceptor stocks are not infinite, and another   
explaining that “we can make it, but it’s a challenge.”28   
These defensive successes highlights the importance of   
magazine depth, defended asset prioritization to con­  
serve interceptor expenditure in protracted conflicts,   
and accurate sensors that can inform defenders about   
the end target of a threat. Following the Iranian attack   
on the Al Udeid air base in Qatar, U.S. soldiers fired a   
considerable number of PAC-3 interceptors, and only 1   
of the 14 missiles fired reportedly got through.29  
Israel’s development philosophy has been   
informed by the urgency and proximity of its threat   
environment. “Cheap enough” and “good enough”   
are more attractive technology descriptions in times   
of conflict than they would be in times of stability. This   
approach is not necessarily applicable to the United   
States or other actors. Nevertheless, Israel’s historical   
integration of disparate and multinational AMD ele­  
engagement. At a CSIS event, Rear Admiral Fred Pyle,   
former director of surface warfare, observed that U.S.   
Naval forces have not seen this level of action since   
World War II.20 The near-immediate response time   
required, combined with an imperative to “get it   
right” 100 percent of the time, suggests that defensive   
interceptors warrant a high degree of trust.   
Pyle additionally highlighted several possible   
routes for minimizing the perceived inefficiency of   
the cost-exchange ratio.21 Whether improving the   
recertification process for older munitions or increas­  
ing scalability, options exist to reduce the spending   
burden for defense without sacrificing operational   
integrity. Developing technologies in directed energy   
(DE), such as lasers or high-powered microwaves,   
could also contribute to a more attractive cost per   
shot, though development and maintenance costs   
will be substantial.  
Lessons from the Defense of Israel  
A third case study of recent air and missile warfare   
comes from the defense of Israel against missile   
attacks. On April 13, 2024, Iran launched a large salvo   
of missiles and drones at Israel. A retaliation for a fatal   
Israeli air strike against an Iranian diplomatic base in   
Damascus, Syria, Operation True Promise included   
approximately 170 drones, 120 surface-to-surface   
ballistic missiles, and 30 cruise missiles.22 The attack   
was the single largest instance to date of a complex   
Table 6.2: U.S. Navy Intercept Usage in   
the Red Sea Through Early 2025  
Type  
Number of engagements  
SM-2  
120  
SM-6  
80  
5-inch rounds  
160  
ESSM/SM-3  
20  
Source: Vice Admiral Brendan McLane in Geoff Ziezulewicz,   
“Navy Just Revealed Tally of Surface-to-Air Missiles Fired in   
Ongoing Red Sea Fight,” The War Zone, January 14, 2025,   
https://www.twz.com/news-features/navy-just-disclosed-  
how-many-of-each-of-its-surface-to-air-missiles-it-fired-  
during-red-sea-fight.

**Page 64**

58  
The Enduring Role of Fires on the Modern Battlefield  
Frying the Sky  
The first such area is only partly a technological one,   
namely the continued development of DE systems.   
The ability to “fry the sky” will be an important offset   
to the capacity problem posed by air and missile   
swarms and salvos. Although the United States is   
making significant investments in DE technologies,   
hurdles remain to transition DE capabilities from   
research and development to programs of record.33   
Operationalizing DE capability is by no means   
just a technological problem. Doctrine, organiza­  
tion, logistics, and sustainment are among the many   
aspects of DE that must be considered. Moreover, DE   
is not as inexpensive as marketing brochures might   
suggest.34 The real cost is not measured in the “cup   
of coffee” worth of electricity for a single shot but   
rather across the life cycle—what it takes to build,   
maintain, and operate the system continuously.   
Increasing the role of DE weapons in responding to   
aerial and missile threats will increase the advantage   
of the defender. Future investment in high-powered   
microwave weapons, high-powered radio frequency   
weapons, lasers, various forms of jammers, and   
other forms of electronic attack will be pivotal to   
effective AMD operations.35  
Building Up  
A second category meriting attention is the need to   
build up offensive and defensive munitions. U.S. and   
allied defense industries have been structured to be   
lean, with limited stockpiles for peacetime, which has   
left a number of countries woefully underprepared   
for conflict scenarios.36 The expenditure of THAAD,   
PAC-3, and Standard Missile variants in the Red Sea   
operations and in the defense of Israel now presents   
the United States with a considerable shortfall of   
AMD interceptors. It seems likely that supplemental   
appropriations will likely be applied to replenish and   
expand the inventory.   
Limited munitions stockpiles have hindered U.S.   
assistance to Ukraine throughout the conflict. Both the   
Trump and Biden administrations delivered far fewer   
missiles to Ukraine than were necessary to deter Rus­  
sia.37 The conflict between Israel and Iran highlighted   
the same issue of high intercept expenditure rates   
ments has proven critical in weathering major attacks   
from Iran over the past two years.   
One of the features of Israel’s defense is multi­  
national cooperation.30 Moshe Patel, the director of   
the Israeli Missile Defense Organization, highlighted   
the importance of the interoperability and integra­  
tion that the United States provides, expressing a   
newfound appreciation that “sharing the sky pic­  
ture and the full engagement cooperation capabil­  
ity” is “very, very important.”31 Patel highlighted a   
series of landmark missile defense moments from   
the conflict, from the “first outer space, exoatmo­  
spheric kind of operational interception of a ballistic   
missile” in November 2023 to the April 2024 coor­  
dinated defense that “built a huge confidence about   
[the Israeli] capability and . . . system.”32 While these   
successes are worth celebrating, they also provide a   
blueprint for continued development. The attacks   
launched on Israel demonstrate the potential com­  
position of future attacks and once again highlight   
the need to scale up current capabilities.  
Implications for the Future   
Each of these case studies confirm the salience of fires   
in this new missile age. Missiles coming and going,   
offensive and defensive, will be in high supply and   
demand for the foreseeable future. The United States   
and its allies have already begun to reckon with the   
implications of this new environment for operational   
doctrine and force planning. The forthcoming U.S.   
Army Warfighting Concept, for instance, is expected   
to emphasize that maneuver forces should support   
fires, rather than the other way around. To contend   
with this new environment, at least four areas of tech­  
nological and operational innovation merit special   
attention: frying the sky, hunkering down, building   
up, and the advent of space fires.   
Missiles coming and going, offensive   
and defensive, will be in high supply   
and demand for the foreseeable future.

**Page 65**

59  
Tom Karako and Hannah Freeman  
ture over a much shorter time horizon than it can   
develop and scale production of components like DE   
weapons.41 These strategies will be force multipliers in   
future conflicts, ensuring mission success in the face of   
increasingly complex air and missile threats.   
As space becomes an increasingly pivotal warf­  
ighting domain, both offensive and defensive “space   
fires” will assume a new salience, including space-  
based interceptors. The Trump administration’s Jan­  
uary 2025 executive order calling for the creation of   
a homeland missile defense shield references a provi­  
sion for space-based interceptors. Boost-phase inter­  
cept is becoming an increasingly attractive option as   
missile technology matures, as these interceptors   
strike missiles before they maneuver, reach high   
speeds, or release decoys or multiple warheads.42   
While creating these capabilities is still costly   
and technologically challenging, it is a much more   
realistic objective than it was 20 years ago.43 The cost   
of launching a satellite into orbit has also fallen by   
orders of magnitude, and the emergence of counter­  
space capability may well yield spinoff capability for   
countering missiles of various kinds.44   
Conclusion  
The reign of fires will long endure, and its kingdom   
spans from mud to space. Combined operations will   
necessarily incorporate a number of new technolo­  
gies and concepts, including non-kinetic cyber, infor­  
mation, electronic warfare, and DE activities. The   
demand for kinetic kills, however, will not dissipate   
anytime soon, and any prediction of its forthcoming   
demise will almost certainly be premature.   
Offensive and defensive fires will remain a cen­  
tral feature of the future battlefield. Operations in   
Ukraine, the Red Sea, and Israel have emphatically   
demonstrated their salience. Fires remain the king of   
battle, and long live the king.  
The authors thank the entire CSIS Missile Defense   
Project team, who contributed substantially to the   
research for this chapter—Grayson Phillips, Wes Rum­  
baugh, Masao Dahlgren, and Patrycja Bazylczyk.  
depleting limited stockpiles. China’s growing ballistic   
missile stockpile further exacerbates the deficit prob­  
lem. In the event of a conflict in the Indo-Pacific, the   
United States would likely run out of munitions in less   
than a week, including long-range precision-guided   
munitions that would be critical to military success in a   
Taiwan Strait conflict.38 The problem almost certainly   
necessitates a high-low mix of munitions, specifically   
a combination of commercial off-the-shelf technolo­  
gies and novel technologies designed specifically to   
counter emerging threats on the battlefield.   
Hunkering Down  
Active defense is necessary but insufficient. The entire   
joint force needs to “look up” and understand what   
it can and must do regarding the spectrum of air and   
missile threats. Nevertheless, the simple reality is that   
not all air and missile threats can or will be engaged,   
and damage limitation and consequence management   
must assume renewed importance. The shifting threat   
environment also requires military planners to develop   
capabilities for hunkering down, giving increased   
attention to passive defense (including mobility);   
counter–intelligence, surveillance, and reconnais­  
sance; hardening; and deception. For both offensive   
and defensive fires alike, there will be growing demand   
for mobile launchers that can better “shoot and scoot”   
to evade counterbattery fire and suppression. Passive   
defenses and the operational concepts to operate   
within an adversary’s weapon engagement zone rep­  
resent a necessary means to compensate for the simple   
reality of active AMD shortcomings.39   
Space Fires  
A final, emergent category of fires will soon appear in   
the newest warfighting domain: the heavens. Although   
tracking and interceptor capabilities will increase the   
resilience of forward-deployed assets, they will never   
be 100 percent effective. This implies a need for hard­  
ening and deception to minimize losses.40 As air and   
missile threats become more complex, it will be nec­  
essary to have military assets that can survive attacks   
that get through active defenses. Investing in harden­  
ing things like air bases, missile silos, and command   
centers is low-hanging fruit in AMD: The Department   
of Defense can increase the resilience of infrastruc­

**Page 66**

Emily Harding  
CHAPTER 07  
Intelligence in a   
Transparent World

**Page 67**

61  
Emily Harding  
”  
“  
“I think I may have found the people   
who tried to kill you.”  
–Bellingcat researcher Christo Grozev to Russian   
dissident Alexey Navalny, November 20201  
S  
hortly after the Russian Federal Security Ser­  
vice (FSB) attempted to poison Alexey Navalny   
in August 2020, Bellingcat researchers identi­  
fied not only the service responsible for the heinous   
attack, but the individuals.2 This intelligence feat was   
not the result of exquisite signals intelligence (SIGINT)   
or a highly placed human intelligence (HUMINT)   
source. It resulted from the in-depth sleuthing of   
an independent team of open-source intelligence   
(OSINT) experts. Bellingcat researcher Christo Grozev   
used leaked telephone metadata, flight records, and   
Navalny’s own recollections of his travel to cross-ref­  
erence which Russian agents appeared to be shad­  
owing Navalny’s movements. One unfortunate agent   
turned on his phone on the night of the poisoning,   
pinging off a cell tower just north of Navalny’s hotel.3   
This mystery’s resolution was but one of many   
Bellingcat exposures over the last decade. Their   
achievements, which include finding the agents who   
poisoned Sergei and Yulia Skripal, proof of Syrian   
chemical attacks, the Russian missile that downed   
MH-17, evidence of EU mistreatment of refugees, and   
the identities of several men who stormed the U.S.   
Capitol on January 6, have repeatedly proved the   
power of OSINT to uncover some of the same secrets   
as a multibillion-dollar intelligence enterprise.   
Along with the data capabilities required to carry   
out this kind of private intelligence, industry has   
delivered a slew of advancements that are reshaping   
other parts of the spy world. Quantum computing is   
already changing encryption standards, and ubiq­  
uitous technical surveillance is making traditional   
HUMINT tradecraft dangerously obsolete.   
These trend lines combine to form a clear hallway   
for the future of intelligence work—on one side is the   
stretching expanse of open-source data, which can   
provide insights or sow confusion, depending on how   
Hiding in the sea of data was once hard but   
doable, but the proliferation of AI processing   
tools and emerging quantum decryption   
capability mean that intelligence services   
will need to either create more extreme   
workarounds or accept the difficulty of   
hiding and learn to fight in the light.   
photo: digitalglobe/getty images

**Page 68**

62  
Intelligence in a Transparent World  
Modern Intelligence:   
Oceans of Accessible Data   
and Nowhere to Hide  
Intelligence is more than information; it is insight   
that helps policymakers avert strategic surprise.   
The vehicle for that advantage is largely irrelevant.   
Indeed, it has evolved over time in at least four pre­  
vious iterations, from when George Washington was   
the nation’s first spy master, reading other gentle­  
men’s mail; to an era of tactical warning and denial   
and deception operations in two world wars; to the   
covert action–heavy, spy-versus-spy world of the   
Cold War; to the age of counterterrorism, focused   
on identifying and unraveling low-tech but highly   
deadly networks.   
Today, computers and data define modern intelli­  
gence, thanks to the estimated more than 400 million   
terabytes of data the world produces every day.4 That   
sea of information makes open-source analysis easier   
and more impactful than ever before, but it has made   
traditional intelligence collection far more challeng­  
ing. Just as intelligence services can use this data to   
find secrets, rival services can use video data and a   
person’s “digital dust” to reveal the true identity of   
an officer operating under cover. Intelligence services   
should capitalize on the insights available from enor­  
states use it. On the other side, hemming in the capa­  
bilities of intelligence services worldwide, is the diffi­  
culty of operating in secret. Hiding in the sea of data   
was once hard but doable, but the proliferation of AI   
processing tools and emerging quantum decryption   
capability mean that intelligence services will need to   
either create more extreme workarounds or accept   
the difficulty of hiding and learn to fight in the light.   
In the immediate post–Cold War era, information   
was hard to obtain, particularly from behind the Iron   
Curtain. Access was rare and precious, and extraor­  
dinary measures were worthwhile to get information,   
including putting lives of assets and operators in grave   
danger. Today, the inverse is true. Information is   
cheap. Processing it is expensive, and sense-making   
is exquisite. True secrets still exist, but they are far   
rarer, and the cost-benefit calculation for obtaining   
them has shifted.   
This chapter explores these trend lines, particu­  
larly the challenges and opportunities of OSINT, and   
the efforts intelligence agencies will need to undertake   
to keep up with rapid developments in new dual-use   
technologies. It provides background on how intel­  
ligence is changing and then discusses how wars in   
Ukraine and the Middle East have brought these les­  
sons into acute relief. Finally, it lays out the implica­  
tions of these trend lines for national security leaders.   
Figure 7.1: Global Data Generated Annually  
Data Generated (zettabytes)  
2025  
2024  
2023  
2022  
2021  
2020  
2019  
2018  
2017  
2016  
2015  
2014  
2013  
2012  
2011  
2010  
0  
200  
100  
50  
150  
Source: Fabio Duarte, “Amount of Data Created Daily (2025),” Exploding Topics, last updated April 24, 2025, https://explodingtopics.  
com/blog/data-generated-per-day. Data from Petroc Taylor, “Volume of data/information created, captured, copied, and consumed   
worldwide from 2010 to 2023, with forecasts from 2024 to 2028,” Statista, June 30, 2025, https://www.statista.com/statistics/871513/  
worldwide-data-created/.

**Page 69**

63  
Emily Harding  
cause harm to an individual’s reputation, emotional   
well-being, or physical safety.”9 Beyond information   
on people, governments can obtain data on the health   
of shipyards based on soundscapes, the movements   
of submarines based on sonar designed to locate fish,   
or the location of tanks and troops based on commer­  
cial space assets.   
Critical to open-source work will be recognizing   
the potential pitfalls of this relatively new discipline.   
First, the ubiquity of data means it can be selected or   
manipulated to fit nearly any narrative. Second, in   
an era where data is power, democracies must walk   
a tight corridor between harvesting information and   
protecting the rights of citizens. Finally, for every   
Bellingcat exposure of nefarious action, there are   
likely a handful of crises averted because of exquisite,   
highly classified intelligence collection. OSINT should   
be additive to the intelligence picture, even serving   
as the intelligence of first resort, but it cannot fully   
replace clandestine collection.   
Lessons from Modern Wars  
Ukraine’s and Israel’s recent conflicts have much to   
teach about the power of intelligence and where the   
discipline is headed. The conflict in Ukraine has been   
revolutionary on two fronts: First, it has been a truly   
open-source war, with crowd-sourced intelligence   
work making both a tactical and a strategic difference.   
Publicly and commercially available data has been   
pivotal to widespread sharing at a high level among   
allies and on a tactical level between units in the field.   
Second, the Biden administration’s decision to declas­  
sify intelligence strongly indicating that Russia was   
about to invade teaches twin lessons—calling out Mos­  
cow’s plans did not deter Russia from invading, but it   
did help pre-bunk ridiculous narratives and galvanize   
allies to assist Kyiv in blunting the Russian offensive.   
Conversely, students of the practice of intelli­  
gence will study the tragedy of October 7, 2023, for   
decades. As a counterpoint, they will study Israel’s   
astonishing victory over Hezbollah in the ensuing   
year, in which Israel systematically dismantled the   
group’s fighting apparatus, for the opposite reason.   
Israel had all the information it needed to identify   
and preempt the Hamas attack, but cognitive bias   
mous amounts of publicly available data, but they   
also must find new ways to obtain the information   
that states try to keep secret.   
Human operations, once the bread and butter   
of spy work, changed dramatically in the last two   
decades, thanks to a proliferation of “smart city”   
technologies and biometric identity data.5 Back in   
2010, the Emirati intelligence services were able to   
quickly identify the members of a Mossad operation   
that assassinated a senior member of Hamas in Dubai.   
Using surveillance camera footage, travel records,   
and phone records, they identified the Mossad oper­  
atives responsible for the attack within a month.6   
Today, with AI-enabled facial recognition and Chi­  
nese companies selling security systems across the   
globe, it is too easy to connect dots and unravel an   
entire intelligence operation. Starting with an image   
of a suspected case officer meeting with an asset, an   
enterprising intelligence service can track that case   
officer’s movements across the world over the last 10   
years, using AI to identify everywhere they have been   
seen and whom they have been seen with. In 2018, a   
senior technology officer at the CIA said that in many   
places, “the level of surveillance was so mature that   
local security services no longer needed to follow the   
agency’s officers in order to know where they were.”7  
 Biometric passports make traveling under an assumed   
identity far more difficult, and false identities seem   
paper thin with no decades-long social media history   
to back them up. Plus, any border guard has the ability   
to fact-check backstories instantly. As The Economist   
points out: “A spy can be instantly quizzed on their   
assumed identity’s childhood route to school by an   
enterprising immigration officer using Google Maps.”8   
OSINT has the potential to fill at least some of the   
gaps left by more challenging HUMINT. A multitude   
of industries have decided that data is the new oil and   
are mining every available source to create massive,   
useful datasets. According to the Office of the Direc­  
tor of National Intelligence’s (ODNI) senior advisory   
group on commercially available information (CAI),   
“CAI includes information on nearly everyone that is   
of a type and level of sensitivity that historically could   
have been obtained, if at all, only through targeted   
(and predicated) collection, and that could be used to

**Page 70**

64  
Intelligence in a Transparent World  
Grandma Hanna’s house.” “What house does   
Grandma Hanna have?” “Well, everyone   
knows her!” “So you talk to people a little bit   
and realize where everything is,” Shevchuk   
added.16  
Classic honey traps have evolved for the online   
space. Defense Mirror reported that a Ukrainian   
woman used several Tinder profiles to collect infor­  
mation on more than 70 Russian soldiers, which she   
promptly passed to Ukrainian troops to help with   
strikes.17 Similarly, MI-6 reportedly used Grindr to   
find Russian troops.18  
Commercially available intelligence services have   
been a game changer in Ukraine. Kyiv has leaned into   
a relationship with space technology company Maxar,   
which provides fairly comprehensive satellite imag­  
ery on demand. The cyber war in Ukraine was also a   
proving ground for cyber defense firms. As a Micro­  
soft intelligence report said, “The first shots [in the   
Ukraine war] were in fact fired hours before, when   
the calendar still said February 23. They involved a   
cyberweapon called ‘Foxblade’ that was launched   
against computers in Ukraine. Reflecting the technol­  
ogy of our time, those among the first to observe the   
attack were half a world away, working in the United   
States in Redmond, Washington.”19   
The fact that commercial intelligence is available   
to everyone is an asset as well: Sharing across bor­  
ders is simpler if there is no declassification process,   
no calculation about revealing sources and methods.   
The United States does not need to protect Maxar’s   
secrets. The easy availability of unclassified evidence   
probably helped prompt the Biden administration to   
go public with additional intelligence that indicated   
Russia was planning an imminent full-scale invasion.   
That effort galvanized Europe to overcome its own   
cognitive bias—a false sense of hope that Russia would   
leave Ukraine alone.   
Israel: High-Tech Collection   
and Cognitive Bias  
In the run-up to October 7, Israel’s high-tech intelli­  
gence collection against Hamas worked; it was only the   
interpretation of that information that failed. At least   
prevented action. With Hezbollah, on the other   
hand, Israel took the threat from the group seriously   
and created in-depth, multiyear plans to strike, with   
devastating results when it eventually pulled the trig­  
ger.10 The failure-success juxtaposition of Gaza and   
Lebanon shows that a rigid mindset trumps even the   
most sophisticated intelligence, but the combination   
of detailed intelligence work and persistent attention   
to a threat can devastate even a talented adversary.   
Ukraine: The First   
Open-Source War   
Ukraine is the first truly open-source war. According   
to General Jim Hockenhull, commander of the United   
Kingdom’s strategic command, OSINT has been   
instrumental in providing Ukrainian commanders   
with anticipatory intelligence.11 Commercial satellite   
imagery, tech data, and social media helped expose   
Russian deployments well ahead of the February 2022   
invasion. A Russian submarine commander report­  
edly was killed after logging his daily run on the fit­  
ness tracking platform Strava.12   
Every citizen with a cellphone became a sensor,   
taking videos and photos of Russian troop move­  
ments. At first, they uploaded the geotagged images   
to social media. Then Kyiv adapted the Diaa app,   
originally designed to help Ukrainians access social   
services, to create the e-Enemy platform.13 By one   
estimate, 260,000 Ukrainians reported Russian loca­  
tions to the app in the first month of the invasion.14   
Ukraine’s Security Service also welcomes reports of   
sightings of “suspicious” activity via a Telegram chat   
function called @stop\_Russian\_War\_bot.15 Stories   
abound of Ukrainian commanders needing to know   
what was happening at a certain location, finding a   
business on Google Maps that was near that location,   
then calling to ask the proprietor to look outside and   
report what they saw:   
“We open a Google map, see a store, see its   
phone number, and dial it,” said Shevchuk,   
who described a typical conversation: “Good   
evening, we are from Ukraine! Do you have   
any Katsaps [Ukrainian slur for Russians]   
in the village?” “Yes.” “Where?” “Behind

**Page 71**

65  
Emily Harding  
importance of information warfare and how to capi­  
talize on, or undermine, an engaged population serv­  
ing as a network of sensors. On a larger scale, China   
in particular has perfected the art of staying below   
the threshold of antagonizing the United States while   
aggressively collecting its own intelligence. It also has   
fully committed to technological competition, push­  
ing ahead with the next generation of technologies   
that will provide an immense intelligence edge.   
Implications for the   
Future of Intelligence  
The wars in Ukraine and Israel and the accelerating   
competition between the United States and China   
underscore several implications for the future of intel­  
ligence work. Information is plentiful and can be used   
responsibly or selectively to serve a particular view­  
point. The wars of the future will be fought in condi­  
tions of near transparency, and intelligence collection   
efforts will be similarly exposed to scrutiny. But just   
because facts are available does not mean interpret­  
ing them will be straightforward. Intelligence profes­  
sionals will need to be humble about what they do   
not know, and they will need an extensive rolodex to   
find someone to help, and help quickly. The sections   
below explore these factors in more depth.   
Dueling Facts  
The oft-repeated quote “there are lies, damn lies,   
and statistics,” popularly attributed to Mark Twain or   
Benjamin Disraeli, will apply in force to the modern   
environment featuring oceans of data. With so much   
available information, a person can find data to sup­  
port any point of view. To use a popular example,   
data shows that shark attacks rise in lockstep with   
ice cream sales; bad data science could lead a person   
to assess that sharks prefer people who taste like ice   
cream. Intelligence assessments drawing on a seem­  
ingly endless sea of data must be rigorous in both   
logic and collection to avoid mistakes like mixing up   
correlation and causation (ice cream sales and shark   
attacks both go up when people spend time at the   
beach) or something far more serious, like decid­  
ing whether a pattern of data indicates a country is   
preparing for war. Decisionmakers must be discern­  
a year before the attack, Israeli intelligence collected   
a copy of Hamas’s attack plan, called “Jericho Wall.”   
The plan showed how Hamas planned to take apart   
automated security measures, including cameras and   
sensors built into perimeter fences.20 Months before   
the attack, a young female analyst wrote a report flag­  
ging that a Hamas day-long training exercise matched   
the stolen plan. Separately, Israel’s red team unit, look­  
ing at largely the same information, issued four warn­  
ings that Hamas was planning for a confrontation.21   
Around the same time, Egypt’s intelligence service   
told its Israeli counterpart that “something big” was in   
the works.22 And the night before the attack, security   
services saw dozens of Israeli SIM cards activated.23   
Despite all these signs, Hamas managed to send   
hundreds of fighters into Israel, causing at least   
1,200 casualties. The “why” of this failure will haunt   
Israel for decades, but early analysis boils down to a   
mental block, in the form of anchor bias and confir­  
mation bias.24 Humans tend to anchor their beliefs to   
certain information. They then use new information   
to confirm those perhaps erroneous beliefs. Unless   
officers work to identify and break these biases,   
disaster can strike even the most sophisticated intel­  
ligence service.   
Israel’s war on its northern border, however, was   
a highly effective—and lethal—combination of intel­  
ligence and warfighting. Israel pulled off a clever,   
tailored covert-action operation that caused more   
than 3,000 Hezbollah pagers to explode simultane­  
ously, disabling the bulk of Hezbollah’s fighting force   
and severing its communications network. Over the   
course of nearly 20 years, Israel had developed tar­  
geting packages against the totality of Hezbollah lead­  
ership and frontline positions. When the fight turned   
kinetic, the Israel Defense Forces destroyed more   
than 1,600 Hezbollah facilities and weapons sites.   
Those strikes killed four Hezbollah senior leaders,   
including Secretary General Hassan Nasrallah. In six   
weeks, Hezbollah went from the most capable terror­  
ist group in the world to a shell of its former strength,   
thanks to the strength of Israeli intelligence gathering.   
Both of these conflicts are instructive for an era   
of great power competition. China and Russia have   
learned lessons from the Ukraine war, including the

**Page 72**

66  
Intelligence in a Transparent World  
classified information in a high-side environment. An   
AI system that hallucinates preparations for a coup   
is exceedingly dangerous, but an AI system that can   
summarize 10 years of speeches in 10 minutes to   
analyze the decisionmaking style of a world leader is   
invaluable. As AI systems progress beyond data pro­  
cessing toward agentic decisionmaking, intelligence   
services will be able to send autonomous systems   
into hostile environments for long-dwell intelligence   
collection, with the system able to “decide” when it   
should emerge and report home.   
From Toiling in the Shadows   
to Fighting in the Light  
In the early days of the U.S. intelligence community,   
the National Security Agency (NSA) was referred to   
as “No Such Agency.” The National Reconnaissance   
Office did not exist. Today, CIA has an account on X,   
formerly known as Twitter; its famous first post was   
rather tongue-in-cheek.   
But far less humorous intelligence issues have   
spilled out into the public realm. A poorly informed   
debate about the intelligence community’s authorities   
under Section 702 of the Foreign Intelligence Surveil­  
lance Act took place surrounding the last two renewal   
battles, with privacy advocates making unfounded   
assertions about the intelligence community’s over­  
reaching collection and intelligence agencies largely   
unable to publicly explain why that information was   
incorrect out of an obligation to protect sources and   
ing, work with intelligence analysts to interrogate   
the data, ask for confidence levels, and investigate   
whether contradictory evidence exists to ensure   
strong outcomes. Patience will also be required—solid   
tradecraft takes time, and the first answers are almost   
never the right ones. An internet sleuth could be first   
to the scoop—and very wrong.   
AI-Enabled Insights  
AI and cloud computing are empowering those in   
and outside government to learn more, know more,   
and find more. If a curious individual can ask good   
questions, AI can find the data and sort the results   
as requested. Inside intelligence services, the good   
questions are the easy part. The hard part is ensur­  
ing the security of the AI systems and the integrity   
of its answers. The even harder part is the cultural   
change necessary to make best use of the revolution­  
ary technology. Fear of change is a serious friction   
point, and using AI as a copilot is a big change.25   
The U.S. intelligence community is already incorpo­  
rating AI and machine learning in processing huge   
amounts of video and imagery. MI-6 has reportedly   
used AI to summarize information and sift through   
the ever-growing sea of data, while China’s Ministry   
of State Security developed an AI system capable of   
tracking U.S. spies and other foreign agents.26 The   
next frontier will be using AI to process and summa­  
rize quantities of text in a dependable way, with a   
system capable of showing its sources and protecting   
CIA's first tweet.   
Source: CIA (@CIA), “We can neither confirm nor deny that this is our first tweet.,” Twitter post, June 6, 2014, 1:49 p.m., https://x.com/  
CIA/status/474971393852182528.

**Page 73**

67  
Emily Harding  
Boldly Going into New Intelligence Domains  
As technical and military advancements further   
intertwine, intelligence officers will hustle to keep   
up with both traditional topics and an increasing   
range of nontraditional topics. Operators will chase   
adversaries’ developments in bioengineering; quan­  
tum computing, sensing, and communications; AI;   
3D printing and additive manufacturing; autonomous   
systems; and critical minerals mining. Further, with   
global supply chains and intertwined economies,   
societal dynamics far abroad will have impacts on   
U.S. national interests. In a post-Covid-19 environ­  
ment, intelligence services will be asked to anticipate   
developments in public health, human migration,   
economic shocks, and other societal issues that are   
less secrets to steal than mysteries to unravel. Intel­  
ligence officers will need to think differently about   
collection and analysis, and they will especially need   
to reconceptualize expertise. Having deep experts on   
each of these topics as full-time employees will be a   
waste of time and resources; rather, the intelligence   
community will need to find people who can tempo­  
rarily consult on a niche topic, like what a particular   
subcomponent of a quantum system might do, or   
how economic shocks shape human migration. Intel­  
ligence has always been a team sport, but the team   
needs to become bigger, more fluid, and more agile.  
Conclusion   
At the intersection of intelligence work, massive   
data creation, and tech developments like AI and   
quantum computing, the world of spycraft changed.   
In some ways, the craft got easier, because data is   
easy to come by, but it also got harder because new   
information calls for new tradecraft. Further, tradi­  
tional intelligence collection became nearly impos­  
sible without extraordinary precautions. This new   
world is one in which intelligence services will need   
to “fight in the light.”   
AI will affect intelligence as much as it will war­  
fare. Within five years, agentic AI will be able to task   
collection systems, get an answer, analyze how the   
new information changes the operational picture,   
and send updated targeting information to a weapon   
methods. Similarly, in 2013, Edward Snowden stole   
an estimated 1 million pages of documents from NSA,   
which revealed some facts but also fed misconcep­  
tions about the checks on intelligence collection.   
Once again, the intelligence community was largely   
unable to defend itself.   
There is an inherent tension between democ­  
racy and intelligence work. Democracy is synony­  
mous with accountability, and direct accountability   
is impossible if most work is classified. The U.S. gov­  
ernment and other democracies have resolved this   
tension with indirect accountability: robust legal   
checks on the power of intelligence agencies and   
intensive oversight by specialized committees in Con­  
gress. The Church Committee created the intelligence   
committees in the House and Senate for exactly this   
purpose—even though every American citizen cannot   
inquire about the activities of their intelligence agen­  
cies, their elected representatives can conduct that   
oversight on their behalf.   
Still, the explosion of new technologies and the   
advent of robust open-source capabilities provide   
intelligence services more opportunities to step into   
the light. They can share more information than ever   
before with their own public and allied governments   
without fear of exposing hard-won secrets. Chances   
are good that the same information exists somewhere   
in the open-source realm, provided by a highly sen­  
sitive source or an exquisite satellite capability. Intel­  
ligence services should also do more to explain their   
processes to the American people, if not the outcomes   
of those processes. Leaders serious about preserving   
the power of intelligence services should work hard   
to explain the checks on that power.   
Intelligence has always been a team   
sport, but the team needs to become   
bigger, more fluid, and more agile.

**Page 74**

68  
Intelligence in a Transparent World  
bypassing the challenges of grappling with an ocean   
of data. But they do so at their peril. In a conflict, it   
is impossible to know which piece of information—  
which intelligence insight—will open an opportunity   
or provide crucial warning, and nations that are   
behind in OSINT risk willful blindness.   
Imagine that the investigation described at the   
beginning of the chapter is happening five years   
hence. The Bellingcat researcher has at their fingertips   
a powerful computer and an AI assistant. The assassin   
is far less able to hide his digital dust—his biometric   
passport pings off two airports, and a near-continu­  
ous train of security cameras in transit stations, on   
streets, in shops, and in taxis can easily piece together   
his movements. The would-be victim has a bioengi­  
neered compound in his pocket: a bio agent designed   
to change color when exposed to poison. As he drips   
his tea on the compound, it turned a shocking shade   
of blue. He takes a photo, posts it on social media,   
and calls on all the internet sleuths to “find the assas­  
sin—he must be nearby!” Our researcher would have   
reams of data to draw on, the computing power to   
sort through it, and the ability to call the local author­  
ities before the assassin could leave the city.   
Intelligence professionals should embrace the   
technology, the sleuths, and the speed. They should   
continue to lead the world in intelligence tradecraft,   
and a big part of that tradecraft training should be   
ethics, civics, and a mandate to lean into cooperation.   
system, all without a human in the loop. Bias and bad   
data in these systems can poison the entire kill chain,   
so defense of data will be critical, and efforts to throw   
off the enemy’s systems will become a priority. There   
is only so much classified data available for training,   
so manufactured data will fill the gap for many intel­  
ligence services. This is inherently dangerous—errors   
are magnified and natural variations in real life wash   
out of synthetic data. Manufactured data also provides   
opportunities for enterprising intelligence services to   
attempt to poison it. A supply chain attack on a large   
synthetic dataset could have widespread ramifications.   
As much as a sea of available data has made warf­  
ighting far more transparent than ever before, quan­  
tum decryption could remove the last veils of secrecy.   
It could decrypt communications and weapons telem­  
etry in real time, giving a technologically advanced   
state a critical edge in battlefield awareness.   
Lines between intelligence agencies, academia,   
and industry may become increasingly blurry.   
Because so many of these technological advance­  
ments are exquisite and outside the realm of the   
knowledge of a generalist, intelligence services will   
need to develop close ties to a range of experts in   
order to understand new developments—in particu­  
lar, to understand their significance. For authoritarian   
regimes, quick conscription and threats of retaliation   
for lack of cooperation come easy. Democracies, on   
the other hand, need to communicate the impor­  
tance of collaboration and recruit a team. Similarly,   
alliances will prove even more valuable. The chances   
of one intelligence service having the right expert on   
hand is smaller than the chance of, say, someone in   
the Five Eyes having a PhD in the right aspect of syn­  
thetic biology. This closer cooperation with allies,   
along with a proliferation of private sector “intelli­  
gence” organizations, could open the aperture of tar­  
gets in a conflict. Russia is already making extensive   
use of groups like Wagner for information gathering   
and operations. China views businesses as a useful   
extension of state power when asked to serve. Both   
are likely to view U.S. businesses as legitimate targets   
in a conflict, under certain circumstances.27  
Finally, OSINT is the genie that cannot go back in   
the bottle. Nations can effectively opt out of OSINT,

**Page 75**

Kari A. Bingen  
CHAPTER 08  
Extending the   
Battlespace to Space

**Page 76**

70  
Extending the Battlespace to Space  
”  
“  
The democratization of space technology   
has shifted traditional notions of who can   
wield space capabilities in war and created   
new motivations for warring sides to deny   
the advantages that satellites provide.  
orbit or critical infrastructure on Earth.   
Two days later, Ukraine’s Vice Prime Minister and   
Minister of Digital Transformation Mykhailo Fedorov   
took to Twitter pleading with Elon Musk to send Star­  
link satellite communications (SATCOM) terminals.3   
Over the next three years, Ukraine received over   
50,000 Starlink terminals to connect the battlefield   
and to “provide uninterrupted communication in the   
places where it is needed most—hospitals, schools,   
critical infrastructure facilities.”4 An unprecedented   
amount of satellite imagery flowed to Ukraine and into   
the public domain, documenting the movements of   
Russian forces.5 Even Russian troops sought the ben­  
efits of such satellite imagery and communications,   
including through the illicit acquisition of Starlink ter­  
minals, to improve their own battlefield coordination.6  
The war in Ukraine marked a turning point in the   
role of space in warfare. Once considered a remote   
and predominantly strategic domain, space is now   
central to the day-to-day conduct of armed conflict.   
While the United States has long relied on space sys­  
“@elonmusk, while you try to colonize Mars—  
Russia try to occupy Ukraine! . . . We ask you   
to provide Ukraine with Starlink stations   
and to address sane Russians to stand.”   
–Mykhailo Fedorov, Ukrainian Vice   
Prime Minister and Minister of Digital   
Transformation, February 26, 20221  
H  
ours before Russian tanks rolled across the   
Ukrainian border on February 24, 2022, the   
assault had already started. Soon after 0300   
UTC, tens of thousands of satellite modems across   
Ukraine and Central Europe were knocked offline.   
The first target in Russia’s invasion of Ukraine was a   
satellite system.2 The cyberattack, later attributed to   
Russian state-sponsored cyber actors, targeted a com­  
mercial satellite network to disable Ukrainian military   
communications, but it also led to widespread disrup­  
tion of internet services across Europe. In modern   
warfare, the first shot may not involve a rifle or a mis­  
sile, but a line of malicious code aimed at satellites in   
photo: planet observer/universal images group/getty images

**Page 77**

71  
Kari A. Bingen  
Space as a Battlefield Equalizer   
and Force Multiplier  
One of the most striking aspects of the war in Ukraine   
has been the extensive and effective use of space   
capabilities, especially from the commercial sector,   
to bolster a nation’s defenses and resilience under   
attack. This trend is likely to be more prevalent in   
future conflicts as space technologies increasingly   
proliferate and satellite data and services become   
more accessible.8 While Ukraine has minimal sover­  
eign space assets, it quickly mobilized support from   
foreign governments and international commercial   
providers to gain access to satellite imagery, commu­  
nications networks, and data analytics platforms.9 In   
many respects, space-based capabilities became a   
great equalizer and force multiplier, allowing Ukraine   
to punch above its weight on the battlefield.   
Leading up to and during the Russian invasion   
in February 2022, satellite imagery companies in   
the United States and Europe captured the buildup   
of Russian forces along the Ukrainian border and   
documented their movements into Ukrainian terri­  
tory.10 Satellite images published by the U.S. company   
Maxar showed a 40-mile convoy of Russian military   
vehicles en route to Kyiv.11 According to the Defense   
Intelligence Agency of the Ukrainian Ministry of   
Defense, Finnish company ICEYE, operating syn­  
thetic aperture radar (SAR) satellites that image the   
Earth at night and through clouds, collected data on   
the disposition of “enemy forces, its training grounds,   
military camps, mobilization deployment centers.”12   
Satellite imagery, paired with GPS-guided drones and   
other munitions, enabled Ukrainian forces to track   
Russian military movements, direct counterattacks   
(including deep within Russian territory), and plan   
defensive strategies with greater precision.   
On the battlefield, commercial satellites providing   
broadband internet services have also played a critical   
role. The widespread deployment of SpaceX’s Star­  
link terminals, prompted by the Twitter appeal from   
Fedorov, helped ensure Ukrainian forces maintained   
resilient communications despite Russian cyber and   
jamming disruptions. Called a “gamechanger” by one   
senior Ukrainian official, Starlink became a lifeline that   
tems to enable its military operations, dating back to   
Operation Desert Storm in 1991, Ukraine has demon­  
strated how even a militarily outmatched nation—with   
little indigenous space infrastructure—can leverage   
space capabilities to gain battlefield advantage. From   
the onset of the war, Ukraine has marshaled a range of   
space-based tools for communications, surveillance,   
targeting, and information sharing, many provided   
by commercial actors, leading some observers to call   
the Ukraine war the “first commercial space war” and   
space a “great equalizer.”7   
Simultaneously, as space systems continue to   
demonstrate their utility from peacetime to conflict,   
it is unsurprising that they are being targeted. The   
Ukraine conflict has revealed how adversaries can   
and will attempt to block access to space capabilities.   
In Ukraine, this has occurred largely through jam­  
ming and cyberattacks, but other conflicts could see   
more expansive use of both kinetic and non-kinetic   
means as adversaries seek to erode each other’s satel­  
lite systems. These actions underscore the increasing   
vulnerability of space assets, particularly those oper­  
ated by commercial entities that may not have been   
designed with wartime resilience in mind.  
The democratization of space technology has   
shifted traditional notions of who can wield space   
capabilities in war and created new motivations for   
warring sides to deny the advantages that satellites pro­  
vide. These modern conflicts are normalizing the idea   
that space—like land, sea, air, and cyber—is a domain   
to be exploited, attacked, and defended in wartime.   
This chapter explores four interlinked dimen­  
sions of space in modern warfare: (1) the equalizing   
effect of space capabilities in warfare, as seen on the   
Ukrainian battlefield, especially access to commercial   
satellites; (2) the imperative to deny the advantages   
that space capabilities provide to one’s opponent; (3)   
the broader implications of an increasingly transpar­  
ent battlefield where strategic surprise will be harder   
to achieve; and (4) the integration of counterspace   
weapons into battlefield operations. It concludes   
by examining the policy challenges posed by these   
trends and what they mean for the strategies and pol­  
icies of the United States and its allies and partners in   
the space domain.

**Page 78**

72  
Extending the Battlespace to Space  
damage to infrastructure, and document evidence of   
war crimes. In one stark example, a satellite captured   
the word дети (“children” in Russian) painted on the   
ground outside Mariupol’s theater prior to Russia   
bombing the location.15 These unclassified images have   
not only been useful for Ukrainian operational plan­  
ning but also as tools of public diplomacy, enabling the   
Ukrainian government and its allies to counter Russian   
disinformation and rally international support. As the   
Ukrainian ambassador to the United States noted in   
February 2024, while space capabilities are enabling   
military forces to communicate, they are also connect­  
ing hospitals and civil society and collecting evidence   
of war crimes to support judicial prosecutions.16  
It is not just the defender that seeks the ben­  
efits of space to provide military and information   
advantage, but the aggressor as well. While Russia   
remains a global space power, its space program has   
atrophied in recent years, suffering from sanctions,   
an aging population, and corruption.17 As a result,   
Moscow has resorted to using “others’ civil and com­  
mercial remote-sensing satellites to supplement” its   
allowed commanders to stay in contact with dispersed   
units, share intelligence, and conduct decentralized   
operations—a key advantage in resisting a more cen­  
tralized and conventionally superior adversary.13  
The Ukrainian battlefield has become a cruci­  
ble for experimentation, tactics development, and   
risk-taking, with private companies dropping into a   
war zone and the Ukrainian government embracing   
their technologies. Ukrainian and partner analysts   
have used satellite data—paired with drone data, sen­  
sitive intelligence collection, and other information   
sources—along with data fusion platforms, AI tools,   
and communications networks to rapidly identify   
targets and feed actionable information back to units   
on the ground.14 Space capabilities have played a   
crucial role in this convergence of technologies that   
has enabled a level of battlespace awareness and   
battlefield innovation unthinkable for a country like   
Ukraine just a few years ago.  
Space-based assets have also been employed for   
humanitarian and diplomatic purposes. Satellite imag­  
ery has been used to map evacuation routes, assess   
A convoy of hundreds of Russian military vehicles, as captured in high-resolution satellite imagery by U.S.   
company Maxar, seen roughly 40 miles northwest of Kyiv, Ukraine on February 27, 2022.   
Photo: Maxar/Getty Images

**Page 79**

73  
Kari A. Bingen  
come as no surprise that adversaries will seek to deny   
them. For both Russia and Ukraine, their means of   
denial and disruption have largely been through   
cyberattacks and electronic jamming systems, but   
other conflicts could see more expansive use of both   
kinetic and non-kinetic means as adversaries attempt   
to erode each other’s satellite systems. These coun­  
terspace weapons—employed by both attacker and   
defender and integrated into military units at the tac­  
tical and operational levels—aim to degrade the bat­  
tlefield effectiveness of space-enabled capabilities,   
including communications and precision weapons.  
Space Capabilities: An Early Target   
As noted at the beginning of this chapter, on Febru­  
ary 24, 2022, before artillery was fired or Russian   
tanks were driven into Ukraine, a cyberattack was   
launched against a commercial SATCOM provider,   
Viasat, aiming to disrupt Ukrainian government com­  
munications and military command and control. A   
targeted denial of service attack took tens of thou­  
own capabilities.18 For example, the Wagner Group   
acquired satellite imagery from Chinese companies   
such as Spacety and HEAD Aerospace, prompting the   
U.S. Treasury Department to issue sanctions against   
those providers in January 2023.19 Russian forces have   
reportedly also obtained Starlink terminals illicitly   
to improve their own connectivity and coordinate   
attacks on Ukrainian positions.20   
Today, any nation seeking military or information   
advantage, or any outgunned nation wanting to level   
the playing field, can take advantage of the high ground   
of space. Whether defender or aggressor, they will have   
an array of space-derived data and services available,   
and commercial companies willing to provide them.   
Denial and Disruption:   
The Battlefield Utility of   
Counterspace Weapons  
With space capabilities playing such a significant oper­  
ational and tactical role on the battlefield, it should   
Satellite imagery captured the before and after a Russian airstrike on the Mariupol Drama Theater (left   
image dated March 14, 2022, right image dated March 29, 2022). The word “children” written in Russian in   
white letters can be seen outside the theater in both images.   
Photo: Maxar/Getty Images

**Page 80**

74  
Extending the Battlespace to Space  
ations and other capabilities to degrade adversary   
C4ISR, weapon systems, and support nodes early in   
a conflict to seize information dominance.”25   
For the last three decades, the United States,   
in particular, has been able to project, stage, and   
maneuver forces with relative impunity, dominating   
all domains of warfare and conducting C2, sensem­  
aking, and target prosecution largely unimpeded.   
Yet trends in the global accessibility and acceleration   
of advanced technologies are creating challenges to   
that military dominance. Further, the People’s Liber­  
ation Army (PLA) intends to leverage its own C4ISRT   
networks to gain an edge.26 In modern warfare, par­  
ties now have to concern themselves with their own   
C4ISRT vulnerabilities, as well as contend with adver­  
saries utilizing advanced C4ISRT capabilities for their   
own operational and informational benefit.  
In future conflicts, the ability to disrupt or deny an   
adversary’s C4ISRT will be both a strategic objective   
and a vulnerability—placing a premium on one’s own   
resilient, adaptable C4ISRT architectures, capabilities,   
and processes in contested operating environments   
as well as investments in counter-C4ISRT capabilities.   
The Pervasiveness of Electronic Warfare  
One of the most dominant features of the modern   
battlefield has been the pervasiveness of electronic   
warfare (EW), especially for force protection. Aiming   
to erode the effectiveness of drones and other pre­  
cision munitions, EW systems provide a temporary   
and reversible way to target satellite navigation,   
communications signals, and intelligence, surveil­  
lance, and reconnaissance (ISR) collection. Beyond   
the Ukrainian battlefield, widespread electronic jam­  
ming and spoofing of GPS signals has been detected in   
Israel, along Russia’s western borders, and elsewhere   
around the globe.27   
EW systems have long been part of Russia’s   
military tool kit. Well before Russia’s full-scale inva­  
sion of Ukraine in 2022, Moscow demonstrated a   
capability and willingness to employ EW systems in   
regional conflicts. In 2018, the commander of U.S.   
Special Operations Command reflected that Syria had   
become “the most aggressive EW environment on the   
planet,” after reports surfaced that Russia had been   
sands of satellite modems offline across Central and   
Eastern Europe, not just affecting Ukrainian users but   
also knocking out wind turbines and internet access   
for civilians across Europe.21   
The attack, later attributed to Russian state-  
backed cyber operators, underscored a new reality   
of modern warfare: Space-based systems are prime   
targets in the opening salvos of an attack, especially   
those that provide command, control, communica­  
tions, computers, intelligence, surveillance, recon­  
naissance, and targeting (C4ISRT) capabilities.22   
Recent conflicts underscore this trend. On Octo­  
ber 7, 2023, Hamas attacked Israeli border surveil­  
lance cameras and communications towers to disable   
military communications and command and control   
(C2) and slow any responses.23 Likewise, during Oper­  
ation Rising Lion, on June 13, 2025, Israel conducted   
widespread strikes against Iranian military C2 nodes   
alongside attacks on nuclear sites and key personnel.   
While not targeting satellites (of which Iran has few), it   
was a bold act to degrade Iranian military command­  
ers’ situational awareness, operational coordination,   
and ability to respond to further strikes, including by   
the United States against Tehran’s nuclear infrastruc­  
ture.24 Though neither case involved direct attacks   
on satellites, both demonstrate how warring sides   
will target C4ISRT infrastructure and both challenge   
any assumptions that parties would not seek bold,   
extensive, and perhaps escalatory ways to cripple   
the other side’s C4ISRT systems—whether terrestrial   
or space-based—to degrade operational capacity and   
any information advantage.   
The U.S. military has long assessed that its C4ISRT   
systems—particularly those based in space—would be   
among the earliest targets in a conflict with China.   
In the Indo-Pacific, U.S. forces depend heavily on   
the “high ground” of space for deterrence, defense,   
and warfighting. Satellites are vital for providing   
indications and warning of Chinese military activity,   
connecting distributed forces across vast maritime   
distances, and enabling the employment of precision   
weapons. This assessment is reinforced in successive   
U.S. Department of Defense reports on China’s mili­  
tary and security developments, including one which   
noted that “PLA texts emphasize using cyber oper­

**Page 81**

75  
Kari A. Bingen  
capabilities and services—have become integrated   
with conventional ground forces and moved around   
the battlefield. Rather than holding these capabil­  
ities in strategic reserve, the Russian military has   
embedded EW systems within command and logis­  
tics units.36 This allows Russian forces to use them   
as force protection, shielding units from drones and   
smart weapons, while also disrupting Ukrainian tar­  
geting and coordination.37 These counterspace tools,   
once regarded as strategic instruments, have become   
part of the daily tool kit of ground forces at the tactical   
and operational levels of warfare.   
Israel also conducts widespread, persistent GPS   
jamming and spoofing, no doubt aiming to protect   
itself from missile and drone threats launched by Iran,   
Hamas, Hezbollah, and the Houthis.38 PLA military   
exercises “regularly incorporate jammers against   
space-based communications, radars, and navigation   
systems like GPS,” and the PLA “may be developing   
jammers to target SATCOM over a range of frequen­  
cies.”39 The United States has also begun to increase   
its inventories of EW systems fielded by the Army and   
Space Force to “disrupt their [adversaries’] comms   
and their kill chains and their targeting links.”40   
With electronic jamming and spoofing of   
space-derived services producing the desired military   
effect—eroding the ability of munitions and drones   
that rely on GPS to find their targets—this counter­  
space weapons trend is likely to continue. However,   
as the next section highlights, it is not a magic bullet   
for drone defense or protection against munitions   
strikes, as technologies and tactics continue to evolve   
to mitigate the effects of EW systems. Furthermore,   
those jammers—when on and radiating—can be   
detected, located, and struck if one’s targeting pro­  
cess can beat the time it takes to move the jammers.   
Not only will future battlefields see the ubiquity   
of EW, but regions outside of conflict zones will also   
experience greater electromagnetic interference,   
risking harm to civil and commercial transportation   
and public safety. As the CSIS Aerospace Security Pro­  
gram reported in the 2024 and 2025 editions of its   
Space Threat Assessment, in recent years, observers   
have tracked daily occurrences of GPS jamming and   
spoofing in regions like the Baltic Sea, Middle East,   
“disabling” U.S. AC-130 gunships and blocking small   
U.S. surveillance drones from receiving GPS satellite   
signals.28 That same year, the U.S. Army commander   
in Europe offered similar observations on Russia’s EW   
capabilities in Ukraine, noting that “you cannot speak   
on a radio or any device that’s not secure because it’s   
going to be jammed or intercepted or worse, it’s going   
to be found and then it’s going to be hit,” contrasting   
it to “something we never had to worry [about] in   
Afghanistan and Iraq.”29   
In the months prior to February 2022, an increase   
in GPS interference was detected along the Belar­  
us-Ukraine border and in the Donbas.30 This was   
preceded by reports in 2021 that unmanned aircraft   
systems (UASs) used by the Organization for Security   
and Co-operation in Europe (OSCE) for border mon­  
itoring continued to experience a high level of GPS   
signal jamming, affecting their ability to take off, land,   
and navigate.31   
As the war in Ukraine has progressed, both Rus­  
sian and Ukrainian forces have ramped up their use   
and production of EW systems that interfere with   
global navigation satellite system (GNSS) and SATCOM   
transmissions.32 Russian efforts have been aimed at   
undermining the performance of Western-supplied   
precision weapons, complicating the use of drones,   
and interfering with military C2 and communica­  
tions.33 For example, the High Mobility Artillery   
Rocket System (HIMARS), Excalibur 155 mm guided   
artillery shells, Ground-Launched Small Diameter   
Bomb (GLSDB), and Joint Direct Attack Munitions   
(JDAMs) have all reportedly experienced degraded   
accuracy due to intense GPS jamming, which causes   
the weapons to veer off course and miss their targets.34   
Ukraine has made its own progress in employ­  
ing electronic jammers and spoofers to erode Rus­  
sian drones and guided munitions reliant on satellite   
navigation signals. However, a former commander in   
chief of the Armed Forces of Ukraine wrote in 2023   
that Russia “continues to maintain a significant elec­  
tronic warfare superiority” with layered EW systems   
that “constantly change their location.”35   
These EW weapons—also considered counter­  
space weapons because their targets are space-based

**Page 82**

76  
Extending the Battlespace to Space  
ming systems and quickly suppress them.45 These EW   
systems have increasingly become high-value targets   
on the battlefield. The United States, for its part, is   
upgrading its GPS satellites with military transmission   
signals more resistant to jamming, investing in alter­  
natives to GPS, and developing more resilient and   
proliferated satellite communications architectures—  
like Starlink—to ensure operational continuity.46   
Going forward, EW will be the norm. Jamming   
and spoofing satellite navigation, communications,   
and ISR will be integral to maneuvering forces and   
protecting battlefield assets. Militaries will place a   
premium on operating effectively in degraded envi­  
ronments, geolocating and neutralizing electronic   
threats, and striking EW systems as part of opera­  
tional campaign plans.   
Battlefield Transparency   
The proliferation of space capabilities, including com­  
mercial space assets, has introduced a new level of   
transparency to modern warfare. From intelligence   
professionals and military forces to private open-  
source intelligence (OSINT) companies and amateur   
analysts, more groups will be able to assess military   
forces and posture and even counter disinformation   
thanks to access to commercial imagery and other   
publicly accessible data sources.   
This transparency has strategic implications. It   
enables rapid attribution of military activity, counters   
disinformation, and enhances situational awareness.   
During the early days of the Ukraine war, the availabil­  
ity of satellite imagery helped debunk Russian narra­  
tives and provided real-time evidence of atrocities and   
battlefield developments. Satellite imagery generated   
greater public awareness of Russia’s military aggres­  
sion and aided nations rallying to condemn Moscow’s   
actions in diplomatic forums, counter with security   
assistance to Ukraine, and assess damage to Ukraine’s   
infrastructure and places of cultural significance.   
Yet transparency is a double-edged sword.   
Adversaries also benefit from greater access to space   
capabilities and services. As noted earlier, Chinese   
companies have supplied satellite imagery to Rus­  
sian forces, and similar dynamics may emerge in   
and parts of South Asia.41 In 2023, the International   
Federation of Air Line Pilots’ Associations issued   
warnings to pilots about Chinese warships engaged   
in radio signal and GPS jamming over the South China   
Sea, Philippine Sea, eastern Indian Ocean, and north­  
west of Australia. Several UN agencies have empha­  
sized the harms of jamming and spoofing, noting   
that interference with satellite navigation signals is a   
threat to air and maritime safety and security.42  
Agility and Adaptability   
Russian counterspace weapons have also targeted sat­  
ellite communications in Ukraine, including through   
repeated attempts to jam Starlink terminals support­  
ing Ukrainian forces. However, SpaceX has demon­  
strated remarkable agility in countering this jamming,   
specifically by deploying rapid software updates. One   
U.S. defense official called Starlink’s updates “eye­  
watering,” contrasting them to the often-sluggish   
response cycles of traditional military systems.43 The   
episode underscored both the importance of commer­  
cial space assets in modern warfare and the battlefield   
agility and adaptability needed to counter EW threats.  
The Ukraine conflict has served as a proving   
ground for the agility and adaptability that will   
be needed in future conflicts, particularly as both   
sides contend with the disruptive effects of GPS and   
SATCOM jamming. Drone developers have played a   
central role in this adaptation, pushing innovation   
cycles to weeks rather than months or years. For   
example, in response to electronic interference,   
companies have fielded drones with electromagnetic   
interference detection kits, autonomous terminal   
guidance, and even fiber-optic tethers that eliminate   
reliance on wireless signals for communications and   
targeting altogether.44 These measures have allowed   
Ukrainian forces to maintain effectiveness despite   
widespread jamming while also providing valuable   
insights into how Western militaries might mitigate   
vulnerabilities in precision-guided weapons through   
a mix of technology and adaptive tactics.  
At a broader scale, both Ukraine and its part­  
ners have actively evolved their approaches to oper­  
ate through and counter EW. Ukrainian forces have   
expanded sensor networks to geolocate Russian jam­

**Page 83**

77  
Kari A. Bingen  
operations, Moscow proceeded with its invasion of   
Ukraine. Even Ukrainian President Volodymyr Zel­  
ensky expressed skepticism in the days leading up to   
the attack. Thus, while transparency can shape the   
information environment, it does not guarantee stra­  
tegic restraint.  
This transparency nevertheless made it harder for   
Moscow to deny its actions and for third-party coun­  
tries to ignore the facts. However, as technology con­  
tinues to advance in areas like adversarial AI, where   
new kinds of deception, obfuscation, and misinforma­  
tion can be generated at machine speeds, trust in such   
information will be tested in the years to come.  
Beyond the Tactical: The   
Expanding Counterspace Tool Kit  
While the conflict in Ukraine has illuminated the bat­  
tlefield utility of certain counterspace weapons, there   
is an array of counterspace capabilities being pursued   
by global actors to deny or disrupt the advantages   
that space assets provide in peacetime and conflict.49   
The war in Ukraine has provided an unprecedented   
look into how counterspace capabilities are actu­  
ally employed in conflict—not just in theory or doc­  
trine. While Russia has demonstrated a willingness   
to integrate EW weapons into conventional oper­  
ations for tactical and operational effect, it notably   
has refrained from using other elements of its coun­  
terspace arsenal. This selective employment raises   
important questions about doctrine, thresholds, and   
the evolving nature of escalation in the space domain.  
Russia has leaned heavily on reversible, non-ki­  
netic counterspace weapons—specifically EW systems   
that jam or spoof signals such as GPS and SATCOM.   
These tools have proved effective in degrading the   
performance of Ukrainian and Western-supplied   
precision munitions and drones. However, Russia   
has avoided more overt or escalatory counterspace   
actions, such as kinetic attacks or the use of laser   
weapons designed to blind or damage optical sensors   
in orbit.   
For instance, despite the heavy and transparent   
use of imagery satellites to track Russian forces, there   
is little publicly available evidence to suggest that   
other conflicts. By 2025, two Chinese entities had   
begun launching satellites for their Starlink-like, low   
Earth orbit broadband constellations, with other Chi­  
nese entities planning additional SATCOM constella­  
tions. The U.S. intelligence community assessed that   
“China has achieved global coverage in some of its   
intelligence, surveillance, and reconnaissance (ISR)   
constellations.”47 When global ISR coverage is paired   
with advanced processing, AI tools, and global distri­  
bution networks, China will possess real-time target   
detection and tracking across the planet, including   
of naval vessels, force movements, and aircraft. As   
one senior U.S. Space Force official noted, “the full   
deployment of a space-enabled targeting network   
means that China can hold U.S. and allied forces at   
risk with long-range precision weapons.”48   
U.S. and allied forces are not accustomed to oper­  
ating in an environment of persistent surveillance.   
The Cold War–era emphasis on denial and decep­  
tion waned after the 1990s. From 2001 onwards, two   
decades of counterterrorism operations in Iraq and   
Afghanistan were conducted with the United States   
and its allies and partners operating under the cover   
of dominant air, space, cyber, and electromagnetic   
spectrum capabilities. Now, with commercial and for­  
eign sensors proliferating, all militaries must adapt to   
a world where movements, emissions, and signatures   
are constantly monitored.  
This demands a fundamental shift in training,   
doctrine, operational planning, and posture. Military   
forces—especially those at fixed sites and massed in   
central locations—must assume that they will be seen   
and their movements and emissions detected. Oper­  
ating in this environment requires renewed emphasis   
on operational security, deception tactics, and elec­  
tromagnetic spectrum discipline. Exercises should   
simulate conditions where adversaries possess near-  
real-time ISR capabilities. The threat of persistent sur­  
veillance further reinforces the necessity of eroding   
an adversary’s ISR capabilities and the networks that   
enable them early in a conflict.  
It is also important to note that transparency does   
not always lead to deterrence. Despite overwhelm­  
ing satellite evidence and the disclosure of sensitive   
U.S. intelligence, including warnings about false flag

**Page 84**

78  
Extending the Battlespace to Space  
For the United States and its allies, this raises   
important questions. What thresholds are adversaries   
observing in space? What conditions on Earth precip­  
itate actions against space assets? And how should the   
United States and its allies respond to demonstrations   
that fall below traditional red lines but still aim to alter   
the strategic calculus? These are not theoretical con­  
cerns. Future conflicts are likely to be shaped by sim­  
ilar patterns of gray zone counterspace activity.  
Beijing, which possesses a full range of space capa­  
bilities that it is increasingly integrating into its own   
joint force, is undoubtedly watching these develop­  
ments closely. The U.S. intelligence community con­  
siders the People’s Republic of China (PRC) to be the   
most expansive space threat and a global space power,   
competing with the United States. In its 2025 annual   
threat assessment, the U.S. intelligence community   
assessed: “Counterspace operations will be integral to   
PLA [People’s Liberation Army] military campaigns,   
and China has counterspace-weapons capabilities   
intended to target U.S. and allied satellites.”52  
PRC doctrine has long emphasized the value of   
striking C4ISR capabilities early in a conflict to deny   
the U.S. military its operational edge. The lessons   
emerging from Ukraine—especially around EW, ISR   
denial, and the use of counterspace capabilities for   
both warfighting and signaling—are likely reinforcing   
China’s investments in a broad suite of space denial   
tools. Further, with the pursuit of large, prolifer­  
ated satellite constellations (involving hundreds or   
thousands of satellites) as an approach to enhance   
performance and resiliency in key capability areas—  
whether SpaceX’s Starlink for communications or the   
U.S. Department of Defense’s Proliferated Warfighter   
Space Architecture for tracking missiles—adversar­  
ies will inevitably look for ways to hold these sys­  
tems at risk.53 Such options are likely to shift toward   
methods that generate widespread effects, such as   
cyberattacks, debris-generating attacks to collapse   
an entire orbital plane, high-altitude nuclear detona­  
tions (HANDs), or attacks on physical infrastructure   
like ground stations. Indicators for such a shift could   
include research to understand the effects of HANDs   
on satellites, for example, as Chinese scientists are   
reportedly doing at a PLA research institute.54 Each   
Russia has used laser systems (such as the Peresvet   
and Sokol-Eshelon) or SAR jamming systems to blind   
ISR satellites.50 A European Space Agency SAR satel­  
lite did experience interference while imaging Sevas­  
topol in November 2023, echoing similar disruptions   
observed in 2021, but it was unclear whether this   
resulted from intentional satellite jamming or radar   
interference in the region.51   
At the same time, in the lead-up to its invasion,   
Russia engaged in a pattern of ambiguous demonstra­  
tions that could be interpreted as strategic signaling.   
In November 2021—just three months before its inva­  
sion—Russia conducted a direct-ascent anti-satellite   
(ASAT) missile test, generating significant debris in   
low Earth orbit. While the test was not directly tied   
to operations in Ukraine, its timing raised questions:   
Was this a message of intent, a readiness demonstra­  
tion, or a rehearsal for more aggressive action?  
Other activities further complicate the picture.   
The Russian “inspector” satellite Luch, believed to   
be for gathering signals intelligence, has maneu­  
vered and loitered in geostationary orbit throughout   
the Ukraine conflict near Western satellites provid­  
ing high-throughput communications over Europe.   
And perhaps most notably, in the same month that   
Russia invaded Ukraine, it launched an experimental   
satellite believed to be an ASAT weapon capable of   
carrying a nuclear device—though this development   
was not revealed publicly until February 2024. The   
timing and nature of these developments suggested   
a willingness to use space demonstrations as strate­  
gic signaling tools, possibly as a form of deterrence   
or coercive leverage, even if the weapons themselves   
were not directly employed in combat.  
These patterns—employing reversible, non-ki­  
netic means in a tactical fight and exercising restraint   
in some areas while signaling ambiguity in others—  
offer insights into how Russia may view the utility of   
counterspace weapons, the conditions under which   
certain weapons might be employed, and how it   
manages escalation risks. Moscow’s strategy blends   
tactical denial with strategic ambiguity—a doctrine   
that may favor deterrence through uncertainty rather   
than action.

**Page 85**

79  
Kari A. Bingen  
have traditionally relied on commercial capabilities   
as a supplement to national systems. Increasingly,   
these capabilities are at the core of operational plan­  
ning, with countries like Poland adopting commercial   
space solutions as the foundation for their sovereign   
satellite constellations.60  
This creates new challenges in acquisition, inte­  
gration, and protection.61 How can U.S. and allied   
forces rapidly incorporate commercial space services   
into joint and coalition operations? How can contracts   
and partnerships be structured to ensure responsive­  
ness and resilience in conflict? And what obligations   
does a government have to protect commercial assets   
that become military targets?  
One area of active debate is whether commercial   
satellites used for military purposes become legiti­  
mate targets under the laws of armed conflict. Rus­  
sian officials have made statements suggesting that   
they consider such systems valid military targets.62   
This raises concerns about the protection of dual-use   
infrastructure and the potential escalation of conflict   
into space.  
Another key issue is deterrence. How can the   
United States and its allies and partners deter attacks   
on their space assets, including those operated by com­  
mercial providers? What signaling, posture, and capa­  
bility mix is required to communicate resolve without   
provoking escalation? These questions are central to   
ongoing doctrinal development, especially within the   
U.S. Space Force, and the source of debate within the   
U.S., European, and Asian space policy communities.  
Classification is also a barrier. Much of the U.S.   
space architecture remains highly classified, as do cer­  
tain allied capabilities and cooperative space defense   
initiatives, complicating efforts to share information   
among allies and integrate commercial partners. As   
space becomes more contested and more crowded,   
information sharing and interoperability will be vital.  
Finally, space business leaders will increasingly   
find themselves in the middle of geopolitics and global   
security questions. Companies like SpaceX, Maxar,   
and others have found themselves making geopoliti­  
cal decisions—such as whether to provide services in   
contested regions, how to handle adversary access,   
of these variants of counterspace weapons has policy,   
operational, and technical trade-offs.55 Some would   
be highly escalatory and others, like HANDs, would   
be both escalatory and indiscriminate, presenting as   
much danger to the attacker’s own satellites as to its   
intended targets.  
Beyond Russia and China, the United States and its   
allies have become more explicit about their counter­  
space policies and investments to protect their assets   
and target adversary satellites.56 Although the United   
States has long held space control as a core mission,   
it has been reticent to publicly discuss its capabili­  
ties. But that stance is shifting. In April 2025, the U.S.   
Space Force released a space warfighting framework   
emphasizing both “offensive and defensive actions”   
to achieve space superiority.57 France has been par­  
ticularly outspoken among Western nations, outlin­  
ing plans to develop and field orbital counterspace   
capabilities and bodyguard satellites, potentially with   
shoot-back or jamming systems on board.58 Even com­  
mercial companies, like U.S.-based True Anomaly, are   
developing new “spacecraft purpose-built for space   
superiority.”59 This raises the specter that in the future   
satellite operators could contract with private firms   
to protect their assets.  
As space systems prove critical from peacetime to   
conflict, they are increasingly vulnerable to a grow­  
ing array of counterspace weapons as adversaries   
seek to erode each other’s space-based advantages.   
In Ukraine, Russia has employed reversible, non-ki­  
netic tools for tactical denial of space services while   
exercising restraint and signaling ambiguity with   
others—revealing a nuanced approach in the employ­  
ment of counterspace weapons and highlighting the   
complexity of deterrence and escalation involving   
counterspace weapons in modern warfare.  
Policy Challenges   
and the Road Ahead  
The use of space in the Ukraine conflict raises pro­  
found policy questions for the future of warfare.   
First, the centrality of commercial space capabilities   
to military operations demands a rethinking of pub­  
lic-private relationships. U.S. and allied governments

**Page 86**

80  
Extending the Battlespace to Space  
   
and how to balance global business interests with   
national security.63  
There are also emerging signs of adversarial coop­  
eration in space. Russia and China have expressed   
interest in greater space collaboration, and Chinese   
support for Russian military efforts in Ukraine sug­  
gests a growing willingness to share capabilities. U.S.   
and allied strategies must account for the potential of   
a “coalition of convenience” in space.  
Conclusion  
The evolving role of the space dimension in modern   
warfare is reshaping how conflicts are fought and who   
can influence them. The greater accessibility of satel­  
lite data and services can both level the playing field   
for underdogs and serve as a force multiplier for those   
best able to exploit them and mitigate attacks against   
them. The persistent coverage of terrestrial activities   
by space assets is making the battlefield more trans­  
parent, diminishing strategic surprise, and inviting   
the public to peer into the fight in unprecedented   
ways. Business leaders, too, increasingly find them­  
selves in the middle of geopolitics, crises, and war.   
The war in Ukraine has crystallized these trends,   
demonstrating the power of commercial systems, the   
impact of persistent surveillance on force posture and   
movements, and the growing risks of counterspace   
threats. These lessons are urgent and enduring. The   
space domain will be central to future conflicts—not   
just as a support function, but as a contested arena   
of operations. Policymakers must act decisively to   
update doctrine, enhance resilience, deepen pub­  
lic-private integration, and prepare forces for a world   
in which space systems are not only accessible to all,   
but visible to all.  
The evolving role of the space   
dimension in modern warfare is   
reshaping how conflicts are fought   
and who can influence them.

**Page 87**

Aosheng Pusztaszeri and Emily Harding  
CHAPTER 09  
Technological Evolution   
on the Battlefield

**Page 88**

82  
Technological Evolution on the Battlefield  
”  
“  
Ultimately, the next generation of warfare will   
not be defined solely by who possesses the   
most advanced technology, but by who can   
integrate, adapt, and counter it the fastest.   
“Soldiers hike for miles, ducking into cover, through   
drone-infested territory too dangerous for jeeps,   
armored personnel carriers or tanks. Soldiers say it   
has become strangely personal, as buzzing robots   
hunt specific cars or even individual soldiers. It is,   
they say, a feeling of a thousand snipers in the sky.”  
–Marc Santora, “Rise of the Dragons: Fire-Breathing   
Drones Duel in Ukraine,” New York Times1  
I  
n war, soldiers get creative. They find new ways   
to use old equipment and ask for new technolo­  
gies to solve problems as they emerge. In turn,   
those new technologies drive tactics and operations   
for warfighting in unprecedented and sometimes un­  
predictable ways. The party that innovates, procures,   
and adapts first secures an often insurmountable   
edge. For instance, during World War I, the British   
developed the first rudimentary tank to break the   
stalemate of trench warfare, spawning successive   
models that ultimately helped turn the tide on the   
Western Front.2   
The recent conflicts in Ukraine and the Middle   
East have represented a leap forward in the employ­  
ment of technology on the battlefield by sophisticated   
actors. Ukraine and Russia have each evolved to shape   
a battlefield defined by drone warfare and drawn to a   
stalemate, and Israel has used its technological edge,   
including AI-generated target recommendations, to   
devastate Hamas.   
However, overdependence on technology courts   
dangerous consequences. For example, Israel’s   
tech-intensive Gaza border defenses clearly failed on   
October 7, 2023, and the Israeli government has also   
been heavily criticized for its use of AI systems for   
targeting and identifying alleged members of Hamas   
in large crowds. Further, in the race to out-innovate   
the adversary, there is a real risk of overlooking eth­  
ical considerations and the need for rigorous testing   
in favor of speed and lethality.  
This chapter examines how emerging technolo­  
gies are reshaping modern warfare by considering the   
ongoing conflicts in Ukraine and around Israel. In this   
photo: pavlo bahmut/ukrinform/future publishing/getty images

**Page 89**

83  
Aosheng Pusztaszeri and Emily Harding  
enemy trenches, burning away the vegetation they   
use for concealment.7 Because drones cause fear, they   
can also drive adversary behavior; for example, Rus­  
sian forces have used drones to funnel columns of   
Ukrainian troops into minefields.8   
Further, tanks and armored personnel carriers   
are easy targets, so troops on both sides have adapted   
to operate in smaller units, which advance more   
cautiously and often on foot.9 The drone war has   
extended to sea, too, with Ukraine using uncrewed   
surface vessels (USVs), such as the Magura-V5, to   
decimate Russia’s Black Sea Fleet.10 Small enough   
to avoid radar detection, these USVs can carry 500   
to 700 pounds of explosives and infiltrate harbors   
to damage or sink Russian ships.11 In May 2025,   
Ukrainian Magura-7 drone boats armed with infra­  
red-guided air-to-air missiles successfully downed   
two Russian Sukhoi Su-30 fighter jets over Novoros­  
siysk and Crimea—marking the world’s first recorded   
shootdown of fighter aircraft by a sea drone.12   
On land, both Ukraine and Russia have expanded   
their use of unmanned ground vehicles (UGVs). In   
northeastern Kharkiv, for instance, Ukrainian forces   
used UGVs to clear mines and conduct reconnaissance   
missions. This operation was supported by unmanned   
mine-laying vehicles and aerial drones, marking the   
“first documented machine-only ground assault” of   
the war, according to Ukraine’s Khartiia Brigade.13  
Aerial drone units are also becoming central to   
battlefield strategy, prompting both sides to intensify   
recruitment and training programs for new UAS units,   
which require a vastly different skill set than traditional   
infantry.14 Ukrainian UAS operators must master avia­  
tion meteorology, learn to operate collision avoidance   
systems, and perform takeoffs and landings in a wide   
range of conditions.15 Ukraine created the world’s first   
drone-focused branch of the military in 2024, calling   
it the Unmanned Systems Forces.16   
Innovation  
The war in Ukraine has established a blistering cycle   
of measures and countermeasures, with both sides   
rapidly innovating to stay ahead of enemy advance­  
ments. According to Nick Reynolds of the Royal   
United Services Institute, current technology has a   
future landscape, conflicts will increasingly resemble   
Ukraine’s high-tech cat-and-mouse game rather than   
the Battle of Medina Ridge and Desert Storm.3 It will   
be less of a grind, making the best use of the forces   
as they exist, and more of a game of leapfrog, where   
parties try to leap ahead of each other for a techno­  
logical edge.   
Lessons from Ukraine   
Emerging technologies have reshaped battlefield   
tactics and weaponry in Ukraine. The most marked   
change is cheap, flexible, and highly maneuverable   
intelligence, surveillance, and reconnaissance (ISR)   
drones.4 Cover and concealment are of the utmost   
importance, and large combined arms maneuvers   
involving columns of highly visible tanks and per­  
sonnel carriers are more vulnerable to drone strikes   
and less capable of achieving the same rapid break­  
throughs seen in previous conflicts.5 This has led   
to a highly iterative game of cat and mouse, with   
advancements in electronic warfare meeting drone   
advancements step for step. Beyond drones, the   
war has changed in other ways, including aggressive   
information warfare, cycles of cyber war, and initial   
uses of true autonomy with the advent of AI. The last   
three years of warfare have dramatically accelerated   
technology innovation, and the years ahead point to a   
growing global acceptance of drone-based and auton­  
omous warfare.   
Unmanned Vehicles  
As reflected by the quotation at the beginning of the   
chapter, drone warfare has defined the battlefield in   
Ukraine. For reconnaissance, Russia and Ukraine have   
incorporated first-person view (FPV) drones into their   
military tactics, which locate enemy tanks and infan­  
try vehicles, then signal their positions to artillery and   
attack drones to conduct precise strikes. Drones of all   
sizes serve as highly flexible kinetic-strike vehicles,   
whether by dropping “dumb” bombs or themselves   
serving as the delivery vehicle in a one-way strike mis­  
sion. Ukrainian unmanned aircraft system (UAS) units   
use advanced quadrotor drones to drop grenades   
into Russian tank hatches with pinpoint accuracy.6   
So-called dragon drones spew burning thermite into

**Page 90**

84  
Technological Evolution on the Battlefield  
nodes and smaller radios to reduce the detectability   
of its signals and make it harder for Russian forces to   
track and jam their communications.21   
Innovation does not necessarily mean high-tech   
solutions. As AI-enabled drones have gotten good at   
locating tanks and armored vehicles, the Russian mil­  
itary has switched to donkeys and horses for moving   
troops and delivering supplies. “It’s better if a donkey   
gets killed than two men in a car carrying the things   
necessary for battle and sustenance,” said Russian   
Lieutenant General Viktor Sobolev.22 Meanwhile, the   
Ukrainian military has employed hand carts for the   
same purpose.23   
Information Warfare  
Information warfare has leapt ahead in the Ukraine   
conflict, with Moscow focusing on spreading mis- and   
disinformation at home and abroad and Kyiv using   
facial recognition to identify Russian soldiers and   
lost children. Both sides have capitalized on AI. In   
March 2022, for example, Russia released a deepfake   
video of Ukrainian President Volodymyr Zelensky sur­  
rendering.24 AI has also played a crucial role in doc­  
umenting and verifying facts on an unprecedented   
scale. Ukraine has used AI-powered facial recognition   
software to identify over a quarter of a million Russian   
soldiers in the country.25 The software was also instru­  
mental in locating 198 missing Ukrainian children   
who were kidnapped and taken to Russia early in the   
war and in enabling Ukraine’s Prosecutor’s Office to   
identify the people in Russia who “adopted” them.26   
AI has further been used to counter Russian propa­  
ganda: While Moscow often downplays or conceals   
its battlefield losses, Ukrainian authorities have used   
the same AI to create an online database of identi­  
fied Russian soldiers killed on the battlefield to notify   
their families in Russia.27 Additionally, AI software has   
been used to collect evidence of war crimes, clear   
land mines, assist in refugee resettlement, and even   
combat corruption.28  
Cyber War  
Both Russia and Ukraine have used cyberattacks as   
additive to their war efforts. Even before the full-scale   
invasion, Russian-affiliated cyber actors targeted   
“six week learning cycle on the battlefield.”17 This   
dynamic is most acute in electronic warfare. As each   
side has found new ways to jam drone signals, the   
other side has found ways to get around that jam­  
ming. Ukraine has significantly improved its radio   
jamming capabilities and can now disrupt the com­  
munications link between Russia’s satellite-guided   
KAB and UMPK glide bombs and its GLONASS sat­  
ellite constellation (Russia’s equivalent of GPS),   
causing Russian glide bombs to veer off course by   
up to a kilometer and detonate harmlessly in open   
fields.18 Further, Ukraine has developed AI-enabled   
drones that can lock onto pre-identified targets in   
the final phase of flight—an innovation designed to   
counter Russian jamming.19 Both sides have reverted   
to operating drones using fiber-optic cables, which   
keep drones tethered but can reach up to a 10 km   
range and are impervious to jamming. Additionally,   
Russia has made advancements in directed energy   
weapons, providing Moscow with a more cost-effec­  
tive way to counter Kyiv’s inexpensive FPV drones.20   
Ukraine has also adopted a more decentralized com­  
munications model, using multiple dispersed radio   
The logo of Ukraine’s new Unmanned Systems Forces is   
an AI-generated image of a robotic swallow. The swallow   
is a Ukrainian symbol of victory.   
Source: Olivia Savage, “Ukraine conflict: Ukraine establishes   
world’s first unmanned force,” Janes, June 14, 2024, https://  
www.janes.com/osint-insights/defence-news/air/ukraine-  
conflict-ukraine-establishes-worlds-first-unmanned-force.

**Page 91**

85  
Aosheng Pusztaszeri and Emily Harding  
technology and cost advantages.34 Ukraine has also   
streamlined its procurement processes by offering   
economic incentives to private companies and eased   
its restrictions on AI defense development. Kyiv has   
also significantly reduced administrative barriers   
for acquiring unmanned systems (cutting procure­  
ment timelines from months or years to just weeks)   
and increased the adoption of off-the-shelf commer­  
cial technology, allowing military units to bypass   
long wait times for custom-developed systems and   
quickly acquire new technology.35  
Lessons from Israel   
As in Ukraine, emerging technologies have played a   
critical role on the battlefield in Gaza and are reshap­  
ing the conduct of the war. However, the Gaza war   
has yielded fewer insights on the impact of emerging   
technologies, as Israel was already a global leader in   
incorporating technological solutions. Further, the   
conflict was less evenly matched—Israel’s quick bursts   
of activity and Hamas’s lack of technological prowess   
have not resulted in the leapfrogging technological   
achievements that have featured in Ukraine.   
Among the technologies that have been publicly   
acknowledged, the most notable is the AI-enabled   
decision-support systems (AI-DSS) that the Israel   
Defense Force (IDF) uses for targeting, which has dra­  
matically accelerated the processing and analysis of   
battlefield information. AI tools have also supported   
Israeli forces in tracking the movements of suspected   
Hamas operatives at checkpoints across Gaza and the   
West Bank. To support these systems, Israel has sig­  
nificantly increased its demand for data storage and   
cloud computing, drawing heavily on commercial   
providers as well as its startup ecosystem to rapidly   
field new technology for the battlefield.   
High-Speed Information Processing  
The ongoing conflict in Gaza is rapidly transforming   
how information is processed and used in warfare.   
For instance, Israel has increasingly relied on AI-DSS   
such as Gospel for its targeting.36 Gospel is a decision   
support tool used by the IDF that aggregates vast   
amounts of intelligence data, including “cell phone   
messages, satellite imagery, drone footage and . . .   
Ukrainian oil and gas companies, Ukraine’s largest   
commercial bank, and the Ministry of Defence’s web­  
sites.29 These attacks were likely aimed at undermining   
the Ukrainian public’s trust in the military, disrupting   
their access to money and fuel needed for evacuation,   
and trapping them in the line of fire, further damp­  
ening hope. As the conflict escalated into open war,   
Russia shifted its cyber focus to government institu­  
tions, communication networks, power grids, and   
media.30 As of April 2024, technology companies on   
the ground in Ukraine reported an ongoing onslaught   
of Russian attacks, in particular directed at the power   
grid and banks. Ukraine, too, has expanded its own   
cyber operations, primarily through its “IT Army”—a   
volunteer force of thousands of hackers conducting   
offensive cyber campaigns against Russian financial   
systems, state services, and media (to counter Russian   
disinformation and propaganda campaigns and con­  
duct propaganda campaigns of their own).31 Ukraine in   
particular has proven highly resilient to these attacks—  
the result of more than a decade of preparation and   
enduring Russian cyber operations.   
AI-Enabled Information Processing  
The speed of information processing and decision­  
making is also rapidly changing, with both sides   
using ISR drones to collect vast amounts of data and   
AI to exploit the data for usable insight. AI plays an   
increasing role in Ukraine’s targeting operations.   
Ukrainian UAS units now use AI to automate drone   
takeoffs and landings and assist in target identifi­  
cation (albeit with human oversight), sometimes   
reducing the time from detection to destruction   
to just over 30 seconds.32 The Ukrainian Ministry   
of Defence is using AI software to “analyze satel­  
lite imagery, open-source data, drone footage, and   
reports from the ground” and provide Ukrainian   
commanders with lists of potential military targets.33  
Incorporating Commercial Tech  
Recognizing the advantages of commercial technol­  
ogy, Ukraine has begun restructuring its military   
acquisition system away from traditional state-  
owned research and development (R&D) models   
in favor of the commercial sector, a shift driven   
in part by the battlefield successes of commercial

**Page 92**

86  
Technological Evolution on the Battlefield  
have provided approximately 50 percent of the anti-  
drone systems deployed by the IDF during the conflict   
so far.45  
Ravenous Need for Data Storage  
The ongoing war in Gaza has highlighted the growing   
wartime demand for large-capacity data storage and   
cloud computing—capabilities now largely provided   
by commercial vendors. As the IDF’s use of AI has   
expanded during the conflict, so too did its need for   
supporting cloud infrastructure.46 However, by the   
early months of the war, Israel’s domestic server capac­  
ity had come under strain, possibly due to the large   
mobilization of reservists from the technology sector   
and preexisting declines in foreign direct investment.   
In response, the IDF significantly increased its reliance   
on overseas cloud providers.47 According to the Asso­  
ciated Press, the amount of IDF data stored on Micro­  
soft servers more than doubled between March and   
July 2024, surpassing 13.6 petabytes—the equivalent of   
roughly 14 billion printed books.48 Beyond direct mili­  
tary applications, Israel has also relied on foreign cloud   
providers to support systems such as Rolling Stone—a   
tool developed by Israeli security forces to manage cer­  
tain population registries in the West Bank and Gaza.49   
(It remains unclear whether this is part of the same   
system used at border checkpoints mentioned earlier.)   
As the war continues, the demand for cloud computing   
and expansive data storage is only expected to grow.  
Danger of Overreliance on Technology  
The ongoing war in Gaza has revealed the ethical   
and practical risks of overreliance on technology.   
The pace of Israel’s offensive against Gaza led the   
IDF to lean into AI to ease the burden on operators.   
According to The Guardian, the IDF’s policy of target­  
ing all individuals with ties to Hamas, including those   
of junior rank, significantly expanded the scope and   
volume of potential targets and quickly overwhelmed   
human operators.50 Some analysts admitted there   
was insufficient time to carefully “incriminate every   
target” while another admitted to spending just 20   
seconds per target, processing dozens each day, and   
contributing “zero added-value as a human, apart   
from being a stamp of approval.”51 Further, during   
the early months of the Gaza conflict, IDF command­  
seismic sensors” to identify potential Hamas com­  
pounds, bases, and homes for targeting.37 Gospel is   
capable of generating significantly more targets than   
traditional intelligence teams. Previously, IDF officers   
could manually identify 50 targets per year; Gospel   
can generate more than 100 per day.38 These AI-gener­  
ated recommendations are then reviewed by human   
analysts, who relay approved targets to the Israeli Air   
force, Navy, and Ground Forces through an app called   
Pillar of Fire.39  
Israel has also increasingly relied on AI-driven   
facial recognition at security checkpoints. The IDF   
uses these systems to scan the faces of passing indi­  
viduals and to detain those flagged as having ties to   
Hamas.40 While facial recognition technology has   
been used in the region for over a decade, Israel has   
significantly expanded its use during the current war,   
using tools developed by Corsight, a private Israeli   
company, to scan and cross-reference the faces of   
Palestinian residents against a “wanted persons”   
database. If the algorithm identifies a match, they are   
detained for questioning.41  
Commercial Technology  
As in Ukraine, the conflict in Gaza has witnessed a   
sharp rise in the use of commercial technology on   
the battlefield. Like the Ukrainian Armed Forces, the   
IDF is capitalizing on the strengths of smaller, more   
agile companies capable of rapidly fielding new and   
innovative designs. For example, as of late 2024, the   
Israeli Defense Ministry enacted a “green path” pro­  
gram for certain startups to fast-track their licensing   
processes.42 Between October 2023 and December   
2024, the ministry also awarded 101 contracts collec­  
tively worth ILS 782 million ($219 million) to startups   
and small firms, many of which sprang up out of skills   
gained in service with the IDF.43 According to military   
expert Isaac Ben-Israel, startups in particular excel in   
this environment, as they are often “a group of few   
people that can do something in weeks” rather than   
months or years.44 This shift has been particularly   
evident in the development of anti-drone technolo­  
gy—a critical need as the IDF faces a constant barrage   
of varied drones and hardware launched from Gaza,   
Lebanon, Iran, and Yemen. In response, startups

**Page 93**

87  
Aosheng Pusztaszeri and Emily Harding  
When both sides have AI-enabled   
targeting and processing, the   
incentive will lean heavily toward   
deferring as much as possible to   
the AI’s capability. For now, that   
surely will lead to mistakes.  
With that ease comes the peril of using AI as a   
crutch: When both sides have AI-enabled targeting   
and processing, the incentive will lean heavily toward   
deferring as much as possible to the AI’s capability.   
For now, that surely will lead to mistakes. AI is not   
trained or tested enough to take on such life-and-  
death responsibility. Finally, this entire ecosystem   
of rapid innovation and speedy decisionmaking will   
require the heavy involvement of industry, not only   
back at factories and in labs, but at or near the front   
lines, to receive rapid feedback and anticipate the   
next adaptation.   
Ready to Fight in Full View  
UAS units will prove a quick, lethal tool in future   
conflict. Drone teams will be able to detect enemy   
armaments and movement on supply lines within   
minutes and take rapid action to destroy targets.   
Units must prepare to fight in full view of the enemy,   
rendering large-scale combined arms maneuvers less   
common. Troop transport will be dangerous, neces­  
sitating movement in small numbers and likely under   
cover of some other purpose. Meanwhile, valuable   
military targets will need to be outfitted with increas­  
ingly advanced electronic warfare systems and con­  
stantly patrolled by interceptor drones to counter   
enemy UASs and glide bombs. The air domain will be   
increasingly contested, with UASs engaging in aerial   
combat for temporary control of the skies. The sea   
domain will also change dramatically: If a $500 drone   
can destroy a multimillion-dollar tank, so, too, can a   
USV swarm destroy a fleet of ships. Counter-drone   
solutions will be decisive on the future battlefield.  
ers pushed their analysts to “bring [them] more tar­  
gets,” which caused human analysts to increasingly   
defer to and trust AI’s recommendations.52 Border   
guards fear making errors and tend to assume that   
the AI is more accurate than they could be, leading   
to false positives.53 While the Israeli firm behind the   
facial recognition system claims its technology can   
accurately recognize a face even if 50 percent is   
obscured, anonymous IDF officers told the New York   
Times that the software still struggles with partially   
covered faces and grainy drone footage and noted   
that the system occasionally misidentifies individu­  
als as being connected to Hamas.54 Israel also leaned   
heavily on technology to secure the border between   
Gaza and Israel before October 7, with disastrous   
effects. Hamas knew how to dismantle static, auto­  
mated systems, rendering defenses largely useless.   
(For more on this dynamic, see Chapter 7: Intelli­  
gence in a Transparent World.)  
Implications for the   
Future of Warfare  
The last three years of warfare have prompted a   
leap forward in technology on the battlefield, and   
the near future points to several continuing trend   
lines. First, the stealthy maneuver of large land and   
sea forces will become increasingly rare, thanks to   
small aerial drones using flexible, cheap commercial   
overhead imagery, crowd-sourced intelligence, and   
camera-guided one-way USVs at sea. Logistics chains   
will be in constant peril for many of the same reasons   
and will increasingly depend on disposable UGVs to   
perform tasks too dangerous for humans.   
Defenders who can dig in with effective count­  
er-drone measures will have a significant advantage,   
and those who must cross open land will be at a sig­  
nificant disadvantage. Future commanders will have   
access to a massive amount of information from a   
multitude of sources, demanding that they operate   
on a rapid-spin OODA (observe, orient, decide, act)   
loop. There is great promise for AI to make this pro­  
cess easier. It has already appeared on the battlefield   
in limited ways, but it is poised to rapidly expand as   
warriors get comfortable with the technology and   
iterate on its use.

**Page 94**

88  
Technological Evolution on the Battlefield  
semi-autonomous support robots. These systems will   
require two enablers: (1) dependable communications   
to network the effort and (2) fuel to keep it running.   
First, secure, redundant communication systems are   
essential to making this highly networked form of war   
possible. Units will need resilient mesh networks to   
ensure continuous communication even if multiple   
nodes go dark.59 Second, highly mobile units will need   
mobile fuel. Ideally, they will not struggle under the   
weight of heavy rucksacks loaded with old, bulky bat­  
teries and instead can use compact, efficient, newer   
forms, alongside readily dependable alternative fuel,   
like high-efficiency solar and biofuels.   
Rapid Adaptability Cycles  
Future wars will likely feature extremely fast cycles   
of innovation and adaptation, as seen in Ukraine.   
With a more widespread battlefield, the front lines   
may evolve at different paces or in divergent ways,   
necessitating central nodes to facilitate sharing les­  
sons learned. To keep up with the pace of innovation,   
militaries must adopt a more streamlined procure­  
ment process, allowing commercial vendors to rap­  
idly iterate. Additionally, the speed of adaptation   
means creating bespoke equipment will likely be too   
slow; units must make do with off-the-shelf commer­  
cial technologies. Central commands can help push   
these commercial products in the right direction by   
telegraphing anticipated needs, giving industry a   
strong demand signal and a head start on the next   
iteration. This approach bypasses the time-intensive   
process of developing custom technologies and could   
reduce procurement timelines from years to weeks.  
No Front Lines  
The future of warfare will further blur the line   
between combatants and noncombatants. As the   
commercial sector takes on a greater role in military   
operations, civilian service providers—such as those   
supplying power, cloud storage, and internet connec­  
tivity to warring nations—could increasingly be seen   
as legitimate military targets.60 Future militaries will   
need to develop clear policies about defense of pri­  
vate sector assets. For instance, companies deploy­  
ing personnel and equipment to the front lines may   
warrant greater military protection than those pro­  
Highly Empowered Individual Units  
The future of warfare is shifting toward smaller, highly   
mobile, adaptable units, where field commanders are   
empowered to make decisions about cover, conceal­  
ment, and tactics while minimizing their communi­  
cations signature. These units will rely on technology   
designed for hit-and-run attacks and ambushes, such   
as quiet ISR drones followed by autonomous swarm   
attacks, which might provide a distraction from a pre­  
cise sabotage operation that must be conducted by a   
human. Rather than large-scale mechanized maneu­  
ver—such as the tank battles of Desert Storm—guerril­  
la-style tactics, hit-and-run operations, and sabotage   
will define the front lines of battle.55   
Troubled Logistics Tails  
Supplying the front lines will be more challenging—  
and likely deadlier—than ever. Modern armies need   
to anticipate that only a fraction of supplies will get   
through, given adversaries’ ability to identify and   
eliminate targets quickly. As a result, armies will seek   
to minimize deliveries to the front lines. Where pos­  
sible, drone deliveries of goods will be preferable to   
protect the lives of pilots, sailors, and cargo drivers.   
Additionally, militaries will increasingly turn to inex­  
pensive, expendable UGVs for mine clearing, mine   
laying, and frontline reconnaissance.  
In response, militaries will adopt technologies   
that increase self-sufficiency. For instance, advance­  
ments in 3D printing could enable the on-site pro­  
duction of specialized replacement parts, reducing   
the need to use long and vulnerable supply routes.56   
Similarly, bacteria-based biofuels could allow units to   
generate their own energy, increasing mobility and   
reducing reliance on traditional fuel supply lines.57   
Autonomous fuel-delivery vehicles are also expected   
to play a greater role in resupplying frontline units,   
minimizing the need for manned convoys that remain   
vulnerable to enemy drone attacks.58   
Highly Networked Forces  
Future militaries will be equipped with cutting-edge,   
integrated technologies that form highly advanced   
battle networks. These include quantum positioning   
systems, autonomous drones, and autonomous or

**Page 95**

89  
Aosheng Pusztaszeri and Emily Harding  
an unparalleled advantage. A combination of AI and   
powerful computing power, quantum or traditional,   
will allow for leaps ahead in bioengineering, includ­  
ing new chemical combinations and edited viruses for   
biowarfare; alternatively, these advancements could   
create biofuels or medicine tailored to a soldier’s spe­  
cific needs. Each of these adaptations could change   
the way of warfare all over again.   
Conclusion   
The conflicts in Ukraine and the Middle East have   
shown how emerging technologies—particularly   
unmanned vehicles, AI, and information warfare—  
are reshaping combat, forcing militaries to adapt or   
risk obsolescence. Modern conflicts are increasingly   
defined by speed, adaptability, and innovation. Ulti­  
mately, the next generation of warfare will not be   
defined solely by who possesses the most advanced   
technology, but by who can integrate, adapt, and   
counter it the fastest.   
This trend line will challenge most political sys­  
tems based on capitalism and democracy. The market   
will take time to catch up to need and respond to   
demand, whereas a centrally planned system will   
shortcut those steps. The United States in particular,   
despite excelling at invention and problem solving,   
is tragically slow at purchasing and integrating that   
new technology. To compete in this iterative form   
of warfighting, Washington needs to shift away from   
the fear of corruption and the reams of regulations   
designed to squash it. Policymakers must recognize   
a more pressing fear: that the United States is forced   
into a hot war with last-generation technology while   
its adversaries sprint ahead—a position it has not   
experienced since World War I.   
Still, future militaries will need to incorporate   
technology without depending on it. A force mul­  
tiplier is a high-priority target for an opponent,   
and militaries must be ready to lose those tools and   
keep fighting. Using technology as a crutch happens   
today—overdependence on signals intelligence at the   
expense of human intelligence contributed to a criti­  
cal intelligence failure before the attacks on October   
7.62 Against a highly capable adversary, however, the   
extent of the failure could be far worse. For example,   
viding services from thousands of miles away. As mil­  
itaries become increasingly reliant on commercial   
technology, they will have to navigate the influence   
of corporate leadership, many of whom have their   
own (sometimes conflicting) sets of priorities—such   
as revenue growth, shareholder interests, or com­  
pany reputational risk. This misalignment is likely to   
become a recurring challenge in military operations.  
Humans and AI  
Future militaries will likely depend heavily on AI   
for targeting, with AI systems able to autonomously   
identify and eliminate targets with minimal or no   
human intervention, making combat faster.61 Militar­  
ies already have autonomous systems for defense, in   
particular missile defense; a shift to offense is likely   
to take place first as matched targeting—for example,   
AI drone swarms attacking AI drone swarms. Later   
usages will include autonomous “find, fix, finish” of   
clear military targets, like ships and tanks. The last   
frontier will be strikes on particular human targets.   
However, increasing reliance on AI in life-and-death   
decisions raises serious ethical concerns. Human   
error in war is already too common today, but if a   
human operator allows an AI system to mistakenly   
target a school bus instead of an enemy tank, who   
bears responsibility? What are the accountability   
mechanisms? If an AI system is the cause of a friend­  
ly-fire incident, who is to blame?   
The Next Decade of Warfare  
The future holds other uncertainties for warfare in   
the next 10 years. Adversaries are already employing   
AI for deepfakes designed to sow doubt and confu­  
sion. The next iteration could entail deepfake mili­  
tary orders or highly realistic denial and deception   
operations designed to sow tactical chaos. In the   
next few years, sophisticated adversaries will prob­  
ably find ways to combine AI and cyberattacks, with   
offense likely outstripping defense at first. AI agents   
will be able to find vulnerabilities and exploit them,   
perhaps in series, without phoning home and raising   
alarms, which will allow for persistence on networks   
in a way never seen before. A quantum computer   
able to defeat military-grade encryption is likely 5   
to 10 years out, and the first state to use it will hold

**Page 96**

90  
Technological Evolution on the Battlefield  
militaries depending entirely on GPS for precision   
navigation and timing of weapons systems could find   
themselves toothless, should the GPS satellite cluster   
go dark. Quantum sensing might be a future alterna­  
tive; in the meantime, the U.S. Naval Academy is teach­  
ing coping mechanisms like navigating by the stars.63   
A drone swarm accompanying a mobile attack squad   
can be a force multiplier, but if that swarm is taken   
down by an electromagnetic pulse or another form of   
electronic warfare, the squad must be able to fight on.   
If undersea cables are cut and war in space imperils   
satellite communications, militaries need a backup   
plan to continue to coordinate multidomain warfare.   
While technology offers significant advantages,   
it also introduces new vulnerabilities, as adversaries   
are continuously innovating and developing counter­  
measures. The rise of AI-enabled decisionmaking,   
for instance, raises ethical concerns about the trend   
of human deference to AI recommendations. More­  
over, the increasing role of the commercial sector   
in warfare is blurring the lines between combatants   
and noncombatants. Militaries must strike a delicate   
balance: using technology without becoming overly   
reliant on it and maintaining ethical safeguards and   
rigorous testing to keep technology safe. The side that   
strikes this balance will be best positioned to harness   
the full potential of technology in the ever-changing   
landscape of warfare.

**Page 97**

Clayton Swope  
CHAPTER 10  
The Evolution of Airpower

**Page 98**

92  
The Evolution of Airpower  
”  
“  
“Victory smiles upon those who anticipate the   
change in the character of war, not upon those who   
wait to adapt themselves after the changes occur.”  
– Giulio Douhet, Command of the Air, 1921  
G  
iulio Douhet, an Italian general who direct­  
ed the first wartime use of airplanes in 1911,   
called the airplane the “offensive weapon par   
excellence,” alone capable of deciding the outcome of   
wars.1 The core military functions of airpower today—  
long-range bombardment, support to military surface   
forces, surveillance and reconnaissance, and trans­  
portation, as well as counterair operations—would   
look remarkably familiar to Douhet.   
However, the tools and tactics used to perform   
these functions are constantly changing, having expe­  
rienced a particularly rapid evolution on the battle­  
field in Ukraine. Air operations there and in the Middle   
East have been shaped by the mass production and   
deployment of both armed and unarmed uncrewed   
systems at scale, operational challenges arising from   
the lack of air superiority, and the effectiveness of   
electronic warfare and signal jamming. The conver­  
gence of these developments has produced new ways   
to carry out long-range bombardment and support to   
military surface forces, as well as tested and honed   
counterair operations using modern, layered inte­  
grated air defenses.  
The future of military airpower will undoubtedly   
reflect warfighting experiences from Ukraine and the   
Middle East. But trends observed from recent con­  
flicts should only serve as jumping off points for the   
future, rather than the playbook for air operations in   
the next war. As Douhet observed, wars are won by   
those who can anticipate changes in warfighting and   
not through merely adapting to the last war.   
Anticipating the future, it is quite likely that   
thinking machines will play a major role in air and   
counterair operations. AI-enabled lethal autonomous   
weapons, which to date have barely been deployed,   
will play a prominent role, which in turn presages a   
diminishing role for human-piloted aircraft. Air oper­  
Trends observed from recent conflicts   
should only serve as jumping off points   
for the future, rather than the playbook   
for air operations in the next war.  
photo: george bekris/getty images

**Page 99**

93  
Clayton Swope  
the establishment and maintenance of air superior­  
ity, the increased use of uncrewed airborne systems,   
and the widespread disruptions to the use of radio   
frequency spectrum caused by effective electronic   
warfare measures. Though undoubtedly airpower   
will continue to evolve—during both peacetime and   
subsequent conflicts—these developments provide   
insights into how military airpower will be used in   
future wars.  
Challenges to Achieving Air Superiority  
Typically, air superiority, also sometimes called   
command of the air, has been viewed as a spectrum   
of balance between two opposing air forces. The   
U.S. Department of Defense (DOD) defines it as the   
“degree of dominance in the air battle by one force   
that permits the conduct of its operations at a given   
time and place without prohibitive interference from   
air and missile threats.”5 There is a range of relative   
airpower in any given conflict or arena. On one end is   
air denial—being denied the ability to operate in the   
air domain by an opposing force. Air parity is a situ­  
ation in which neither side has control of the air and   
is “typified by fleeting, intensely contested battles at   
critical points,” as defined by U.S. Air Force doctrine.6   
Next is air superiority, an advantage in the air domain   
that may still be contested by an opponent. Finally, air   
supremacy is the ultimate level of superiority, when   
one side is not capable of any resistance or interfer­  
ence to the opposing side’s air operations.  
Throughout the war in Ukraine, neither Ukrainian   
nor Russian forces have been able to establish a recog­  
nizable level of air superiority, though—as detailed   
more thoroughly in the following section—each side   
has been able to interfere with each other’s air oper­  
ations.7 Neither side has demonstrated the means to   
disable or destroy the opposing side’s integrated air   
defenses, resulting in a prolonged state of air parity.   
According to analysis by the CSIS Futures Lab, Russia   
launched over 11,000 missiles, one-way suicide   
drones, and other munitionized airborne systems   
into Ukraine from September 2022 to October 2024.8   
Though Ukrainian counterair operations have proven   
mostly effective, they have not been able to deny Rus­  
sian forces the ability to launch air attacks.9 Similarly,   
ations in the future will also be challenged by the pro­  
liferation of increasingly sophisticated and diverse   
sensors, which will make it harder to maintain air   
superiority over any given area.  
The Character and Functions of   
Military Airpower  
The basic functions of military airpower have been   
apparent since at least the end of World War I and are   
likely to remain fairly unchanged, though the weap­  
ons and how those weapons are used will evolve.2 Air­  
craft, missiles, one-way drones, and other airborne   
projectiles are used for long-range bombardment,   
attacking an enemy’s ability to make war by striking   
targets located well behind the front lines, such as   
economic and national infrastructure. Airpower is   
also used to attack elements of an enemy’s armed   
forces engaged in warfighting and to support joint   
operations across all domains. Additionally, airpower   
can provide surveillance and reconnaissance (e.g.,   
scouting, one of the earliest proposed military uses   
for the airplane) and transportation capabilities.3  
To provide for the command of the air—allowing   
one’s own forces to use airpower for the aforemen­  
tioned aims and preventing an adversary from doing   
so—the final basic function of military airpower is   
counterair operations.4 All sides of the conflicts in   
Ukraine and the Middle East have used air power for   
long-range bombardment, support to military sur­  
face forces, surveillance and reconnaissance, and   
transportation, and have all engaged in counterair   
operations. Of these functions, airpower used for   
transportation has played only a minor role in both   
conflicts due to the compact geography of their zones   
of operation.  
Adapting to Change: Lessons   
from Ukraine and the Middle East  
The conflicts in Ukraine and the Middle East provide   
a window into the evolution of military airpower   
and presage the rough outlines of the challenges and   
opportunities that will confront military planners in   
future air operations. Key observations relate to the   
role of modern counterair measures in obstructing

**Page 100**

94  
The Evolution of Airpower  
of operations over Iran, spycraft and the element of   
surprise.17  
Future conflicts may very well look like the one   
that has played out in the Middle East since late 2023.   
In that notional case, a technologically advanced,   
well-resourced, and well-trained force operating a   
layered air defense system would have a leg up on   
the opposing force. But pitting two peers who are   
roughly equivalent in terms of technology, resources,   
and training against each other might easily result in a   
conflict that looks more like the persistent state of air   
parity over Ukraine’s skies. To gain superiority, each   
side in a future conflict will aim to disable or destroy   
its opponent’s air defenses on both a sector-by-sec­  
tor and a layer-by-layer basis, possibly through sheer   
numbers and mass—an approach Russia has tried   
in Ukraine without using enough mass to actually   
gain air superiority—or through attacks coming from   
unexpected directions that rely extensively on the   
element of surprise, as was the case in Operation Spi­  
der’s Web. The effectiveness of attacks from unex­  
pected directions was also demonstrated in Israel, for   
instance, when a lone Houthi drone came in from an   
unusual trajectory and was able to penetrate Israel’s   
air defenses.18 This also foreshadows the importance   
of keeping counterair defenses in the dark as long   
as possible, blinding kill chains to allow temporary   
access, and using decoys and deception—another   
lesson from Israel’s operations in Iran and Ukraine’s   
Operation Spider’s Web, during which drones were   
transported undetected closer to their targets.  
Proliferation of Uncrewed Systems  
Unmanned aircraft systems (UASs) can be grouped   
into two main categories: systems intended for one-  
way, single-use munitionized applications (e.g., mis­  
Russian air defenses have been able to down and dis­  
able many, but not all, Ukrainian drones aiming at   
targets inside Russia.10 Ukraine’s Operation Spider’s   
Web, a radical departure from conventional thinking,   
however, introduced low-altitude munitionized air­  
borne systems into an environment in which Russia   
had not deployed countermeasures and, in so doing,   
managed to circumvent Russian air defenses.11  
In stark contrast to the situation in Ukraine,   
Israel has managed to establish an effective degree of   
air superiority throughout the surrounding region,   
defending the skies over Israel and showing that it   
can strike targets in Iran, Lebanon, and Syria with­  
out interference.12 In October 2023, Hamas fired   
thousands of rockets and missiles at Israel—but   
nearly 90 percent of them were intercepted by Isra­  
el’s air defenses.13 In October 2024, Iran launched 170   
drones, 30 cruise missiles, and 120 ballistic missiles   
at Israel. Of the entire barrage, all but a handful of   
the ballistic missiles were shot down.14 But the overall   
intercept rate may obscure important nuances. Sub­  
sonic cruise missiles and one-way drones are almost   
all getting shot down, while supersonic cruise and   
ballistic missiles are much harder to intercept, even   
if they are still getting shot down in large numbers.15   
In addition to maintaining air superiority over Israel,   
Israeli forces have achieved that same feat over Iran;   
Israel arguably achieved total air supremacy over   
Iran by mid-June 2025. Israel used its command of   
the air to carry out sustained air attacks on Iranian   
military targets and laid the foundation for the U.S.-  
led Operation Midnight Hammer, which targeted Ira­  
nian nuclear facilities.16 For both homeland defense   
and the projection of airpower, Israel achieved its air   
superiority by maximining the use of cutting-edge   
technologies, training, and tactics and, in the case   
Figure 10.1: Spectrum of Air Power  
Air Denial  
Air Parity  
Air Superiority  
Air Supremacy  
Note: The color shift from green to red reflects increasing control of the air domain.  
Source: CSIS Defense and Security Department.

**Page 101**

95  
Clayton Swope  
nated area over a period of time, waiting for direction   
from a human operator or sensor-triggered action to   
strike its target.26 Israel’s Harpy drone is a loitering   
munition designed to detect and destroy air defense   
radars by homing in on radar signals. Iran’s Shahed   
drone is another example of a loitering munition.27   
During the conflict in the Middle East, UASs have also   
been used for surveillance, not only by Israel and Iran   
but also by nonstate actors like Hezbollah.28  
Based on their use and evolution in Ukraine   
and the Middle East, there can be little doubt that   
UASs will play significant roles in future conflicts.   
Drones will be manufactured and deployed on mas­  
sive scales—Ukraine alone claims it can manufacture   
2.5 million drones per year.29 Whereas operations   
in Ukraine or the Middle East may have involved   
dozens or hundreds of UASs, future operations may   
include thousands of drones operating according to   
pre-programed instructions or under the control of   
a human operator or AI-enabled algorithm. Drones   
will be used for long-range bombardment, support   
to military surface forces, surveillance and recon­  
naissance, and transportation. Due to their cost-ef­  
fectiveness, drones will also be used for counterair   
operations, with Ukrainian forces having already   
demonstrated the use of one-way drones for inter­  
cepting and destroying their hostile Russian counter­  
parts.30 Additionally, reusable loitering drones are   
likely to become more important, possibly as carri­  
ers for one-way attack drones or missiles.31 Finally,   
as both Israel’s operations in Iran and Operation Spi­  
der’s Web demonstrate, the impact of munitionized   
drones increases when they can be conveyed—for   
example, by suitcase or truck—without detection into   
areas without specialized counter-drone defenses.32  
Effectiveness of Electronic Warfare  
The effectiveness of pervasive signal jamming in   
Ukraine as a tool of counterair operations has under­  
lined that battlefield communications are fragile and   
easily disrupted. This has the potential of interfer­  
ing with the ability of human operators to control   
uncrewed systems, including those operating in the   
air domain. Russian signal jamming in Ukraine has   
also impacted the reception of position, navigation,   
siles, rockets, guided bombs, loitering munitions, and   
kamikaze or suicide drones) and systems designed   
for return and reuse. Either type of system can be   
used for attack, surveillance, or transportation. Both   
types can be operated under the direct control of   
a human operator or use various degrees of auton­  
omy to perform their operations. UASs designed for   
return and reuse can serve as carriers for one-way,   
single-use systems, such as one-way drones, missiles,   
or mines.19 The conflicts in Ukraine and the Middle   
East have seen widespread use of both single-use sys­  
tems and systems designed for return and reuse, as   
well as extensive use of counterair operations using   
integrated air defense systems. In these conflicts,   
one-way systems have primarily been used to deliver   
munitions, while reusable systems have been primar­  
ily used for intelligence and surveillance purposes.   
Both Ukraine and Russia have relied heavily on   
the use of one-way systems during the conflict in   
Ukraine.20 Since February 2022, Ukraine has been   
subjected to almost daily attacks by Russian airpower,   
primarily by one-way UASs.21 These one-way weapons   
have conducted long-range bombardment of national   
infrastructure—including infrastructure that was pri­  
marily civilian in nature, such as power and energy   
facilities.22 Small one-way drones have also been used   
to great effect against surface forces, like tanks and   
individual soldiers.23 Many of the one-way drones   
used by both sides are based on mass-produced,   
inexpensive, commercially available models that   
have been retrofitted to carry a small munition. This   
approach has allowed the economical deployment   
of one-way munitionized drones on a vast scale and   
facilitated a trial-and-error approach to developing   
new drone systems and tactics.  
Meanwhile, one-way drones—particularly drones   
manufactured by Iran—have been used extensively by   
Iran and the Houthis in the Middle East.24 Hamas used   
a variety of one-way and reusable drones during its   
October 7, 2023, terrorist attacks on Israel, especially   
for targeting monitoring and communications sys­  
tems and dropping munitions on tanks, soldiers, and   
emergency responders.25 Israel has deployed a spe­  
cific variant of one-way attack drone, usually called a   
loitering munition, which is designed to circle a desig­

**Page 102**

96  
The Evolution of Airpower  
AI-Enabled Autonomy  
Automated decisionmaking for weapons that oper­  
ate in the air and other domains is not a new con­  
cept. Heat-seeking missiles, mines, and torpedoes,   
as well as systems like the Phalanx radar-guided   
gun and Israel’s Harpy drone, make lethal decisions   
autonomously, albeit following a very tight script   
that probably falls short of being considered artificial   
intelligence.35 Though a magnetic underwater mine   
detonating is an automatic reaction to it coming near   
a metallic warship hull, the action—the “decision”   
made—looks more like the instincts of a closing Venus   
flytrap than human decisionmaking. AI-enabled solu­  
tions using machine learning, trained to make deci­  
sions like people, are the evolution of these “Venus   
flytrap” platforms.  
The designers of these legacy weapons turned to   
autonomy for one of two reasons: a requirement to   
make sense of a situation and act faster than would be   
possible with a human in the loop, or a need to make   
a decision in the absence of human input. Looking to   
the future, airpower will rely on autonomous deci­  
sionmaking for these same two reasons—but unlike   
today, decisions with lethal consequences will be   
made by AI-enabled algorithms trained using machine   
learning. One new driver for this shift is the increas­  
ing effectiveness and impact of electronic warfare   
and its ability to sever the links between uncrewed   
machines and human operators. Another evolving   
driver is the availability and need to quickly make   
and timing (PNT) signals received from GPS satel­  
lites, eroding the accuracy and effectiveness of mis­  
siles and drones that rely on GPS to find their targets.   
The architecture of proliferated satellite constella­  
tions has offered some protection against jamming,   
but Russia is increasingly successful at degrading   
Starlink service and has consistently been able to   
disrupt many other signals—like GPS and drone com­  
mand and control links.33  
Experts have been trying to enhance the jam   
resistance of weapons systems as part of the cat-and-  
mouse game between the jammers and the jammed,   
with each side racing to develop technologies that   
defeat the other’s latest and greatest capabilities.34 As   
a result, the ability to remotely command and control   
uncrewed systems and communicate with crewed   
ones can never be assured from mission to mission. It   
also means that it may not be possible to rely entirely   
on GPS or any signal-based PNT technology. In support   
of counterair operations, based on its effectiveness in   
Ukraine, electronic warfare—and electronic counter­  
measures—will feature prominently in future conflicts.   
The threats to signal-based positioning, navigation,   
and links used for timing and command and control   
communications emphasize the need for incorporat­  
ing greater autonomous decisionmaking into UASs.  
Anticipating the Future: Looking   
Over the Horizon  
Though there are lessons for the future of airpower   
that can be directly gleaned from Ukraine and the   
Middle East, there are also trends that can be seen   
through a glass, darkly, with only the rough contours   
visible on the horizon. In the future, AI-enabled lethal   
autonomous weapons, which to date have not been   
extensively—if at all—used in combat, will play a main   
role. Such a development will lead over time—it is too   
early to say whether that time is measured in years   
or decades—to a decreasing need for human-piloted   
aircraft. The proliferation of sensors, and AI-enabled   
solutions making sense of that data at machine speeds,   
will make it more difficult for airborne systems to   
evade detection, leaving air platforms exposed to kill   
chains enabled by these technologies and making it   
harder to maintain air superiority.  
The proliferation of sensors, and   
AI-enabled solutions making sense of   
that data at machine speeds, will make   
it more difficult for airborne systems to   
evade detection, leaving air platforms   
exposed to kill chains enabled by   
these technologies and making it   
harder to maintain air superiority.

**Page 103**

97  
Clayton Swope  
on radar.41 In some applications, infrared seekers are   
used as guidance systems for missiles, which hone   
in on the heat or thermal signatures of their targets   
rather than their radar signatures. In addition to radar   
and infrared, other types of sensors play increasingly   
prominent detection and tracking roles, including   
acoustic, visual, and LiDAR-based sensor networks.42   
To date, these non-radar sensors have been primarily   
used in counterair point defense systems intended   
for defeating airborne threats in close proximity to   
their targets.   
Due to the reliance on radar for all but close-prox­  
imity point defense systems, stealth technology has   
enabled strikes against a wide range of important and   
presumably well-defended military targets by Israel   
in Iran and Syria, such as during Operation Midnight   
Hammer. While terrestrial radar will likely continue   
playing a central role to enable kill chains for airborne   
targets, space-based systems, including electro-op­  
tical sensors, will begin to serve similar purposes.   
Future space-based sensor webs will be able to detect,   
identify, and track objects in real-time using a combi­  
nation of phenomenologies beyond just radar.43 This   
will pose a challenge to stealth aircraft trying to avoid   
detection by an adversary’s air defenses: Though   
designed to avoid detection by radar, stealth aircraft   
can certainly be seen by the naked eye and, thus, are   
susceptible to optical space-based sensors.   
It is not difficult to imagine a time in the near   
future when every point on the globe is observable   
by a space-based sensor at all times, with no break   
in coverage. This can be achieved by a constella­  
tion of satellites in lower Earth orbits or by a series   
of high-resolution satellites in geostationary orbits.   
Notably, China has already deployed a number of   
electro-optical satellites in geostationary orbit.44 The   
United States is investigating the use of satellites for   
tracking targets in the air.45 Pairing data from space-  
based sensors with AI-enabled processing will pro­  
duce systems capable of identifying and tracking   
aircraft, including those using stealth technologies.   
Challenging the efficacy of traditional stealth will   
challenge the ability of air forces that rely on it to   
secure and maintain air superiority. However, new   
uses of electro-optical space-based sensors in kill   
sense of the deluge of data collected from a myriad   
of sensors monitoring the battlespace. The amount   
of data is already so enormous that it cannot be com­  
pletely assessed at operationally relevant timescales   
using human input.36  
There are interim solutions on the horizon that   
attempt to keep the human in the loop for UASs in   
highly jammed signal environments. In Ukraine, some   
operators have resorted to fiber-optic lines to main­  
tain the ability to communicate with their drones.37   
This solution is unwieldy and will not scale to a   
future battlefield environment in which thousands   
if not millions of drones are operating together. The   
long-term response will involve implementing more   
AI-enabled autonomous decisionmaking in uncrewed   
aircraft, including decisionmaking that involves the   
use of deadly force. Defenses operating at machine   
speeds can deploy countermeasures much faster   
against hypersonic weapons and drone swarms than   
a system relying on human reaction times. The United   
States is already buying an AI-enabled counter-drone   
system—the Bullfrog robotic gun system—capable of   
fully autonomous operations.38  
Though researchers have observed that AI-en­  
abled decisionmaking cannot today replicate human   
judgment, AI-enabled problem solving will probably   
improve over time.39 But exactly when that could   
happen is hard to predict. Until that point—when   
machines make as good as or better warfighting deci­  
sions than people—AI-enabled airborne systems will   
have to operate side-by-side with human pilots and   
crews. This creates challenges for both the human   
and machine, as each will struggle to operate most   
efficiently and effectively unless both sides learn how   
to predict and understand how the other side reacts   
in situations encountered on the battlefield.  
Next-Generation Camouflage   
and the Element of Surprise  
The conflicts in Ukraine and the Middle East have   
demonstrated the importance of early-warning and   
fire-control radars for detecting, tracking, and defeat­  
ing airborne threats.40 Today, air threat detection   
and tracking systems supporting long-, medium-,   
and short-range integrated air defense systems rely

**Page 104**

98  
The Evolution of Airpower  
ably be a balancing act, perhaps a temporary one, on   
the edge of a razor—air superiority may be ephem­  
eral or something that is never fully achievable. Ulti­  
mately, there is probably a lot that cannot be foreseen   
about the future of military airpower based on lessons   
from today. It is worth keeping in mind the advice of   
the father of the U.S. Air Force, Billy Mitchell, who   
opined: “in the development of airpower one has to   
look ahead and not backward and figure out what is   
going to happen, not too much what has happened.”47  
chains do not foreshadow the obsolescence of stealth   
technology. Because radar can see through weather   
phenomena (such as clouds) that render electro-op­  
tical sensors less effective, radar will likely retain its   
critical place in integrated air defense detection and   
tracking architectures. But stealth platforms will have   
to operate in environments in which optical sensors   
play a greater role in kill chains. This development   
will require improved tactics—perhaps flying most   
sorties when there is cloud cover or inventing new   
types of high-tech camouflage that can hide aircraft   
from space-based optical sensors.46   
Future conflicts may see greater use of the under­  
sea domain to deploy airpower, as undersea systems   
offer unique opportunities for stealth and surprise.   
Because submarines can be designed to minimize   
their detectability, crewed and uncrewed submarines   
may see greater use as platforms from which drones   
are deployed, aiming to reduce the time air defense   
systems have to identify, acquire, track, and neutral­  
ize hostile airborne targets. Just like suitcases and   
trucks were used by Israel and Ukraine in June 2025   
to smuggle drones closer to their intended targets,   
undersea systems may be used for a similar effect in   
future wars.  
Conclusion  
The contribution of airpower to future wars will be   
shaped by the evolution and use of technologies and   
tactics that have appeared on the battlefield in Ukraine   
and the Middle East. That future will see greater use   
of uncrewed systems, AI-enabled lethal autonomous   
weapon systems, and improved camouflage tech­  
nologies masking radar, thermal, sound, and—pos­  
sibly—visual signatures. These technologies and the   
evolving tactics for deploying them, such as AI-en­  
abled systems working side-by-side with humans, will   
be required to operate under the shadow of ever more   
sophisticated counterair capabilities.  
The goal will be to provide sufficient command of   
the air to execute core military airpower functions.   
This is unlikely to mean total air supremacy—but   
Israel has shown that it is still possible to obtain and   
maintain near-total control of the skies in certain cir­  
cumstances. However, command of the air will prob­

**Page 105**

Mark F. Cancian  
CHAPTER 11  
The Future of Seapower

**Page 106**

100  
The Future of Seapower  
”  
“  
Having a variety of naval capabilities   
available facilitates a response even if   
the tools are not initially available in the   
desired quantity. Expanding an existing   
capability is much easier than developing   
a new one in the crucible of conflict.  
2.   
Do aircraft carriers still have a role?   
3.   
What is the future role of uncrewed naval   
systems?   
4.   
Why have Russia’s Black Sea submarines not   
had more impact?   
5.   
Can inventories of naval munitions ever be   
adequate?  
The discussion of each question contains a sum­  
mary of wartime experience and ends with insights   
into how navies can adapt to the new maritime envi­  
ronment. Because current data is imperfect and not   
necessarily indicative of a war between great powers,   
each discussion also includes indicators that can show   
where naval combat may be headed.  
The Viability of Surface Ships   
in High-Intensity Conflict  
Ukraine has achieved extraordinary naval success in its   
war with Russia.1 Without the conventional attributes   
of a navy—ships and land-based aircraft—it has sunk or   
destroyed eight major Russian surface ships and one   
T  
he conflicts in Ukraine and the Middle East   
present the best opportunity to assess war­  
time naval operations since the 1982 Falk­  
lands War. Nothing is simulated, operations include   
all of the messiness of the real world, and difficulties   
cannot be assumed away as they can in peacetime   
exercises. Although maritime operations in these   
conflicts have had secondary—or even tertiary—im­  
portance after the ground and air campaigns, the ex­  
perience they provide merits close analysis, as it can   
offer valuable insights about the future of seapower.  
In parallel with these conflicts, analysis of a hypo­  
thetical U.S.-China conflict over Taiwan has suggested   
how a modern air and naval campaign might unfold   
(discussed further below). While these assessments   
lack the authority of actual operations, they comple­  
ment insights derived from the current wars.  
This chapter discusses five questions that arise   
from these conflicts and analyses:   
1.   
Are surface ships viable in high-intensity con­  
flict?   
photo: pavlo bahmut/ukrinform/future publishing/getty images

**Page 107**

101  
Mark F. Cancian  
inventories are depleted. Perhaps naval warfare has   
reached the state envisioned by Admiral Karl Dönitz,   
the head of Nazi Germany’s fleet during World War   
II. Dönitz had a painting in his office entitled “The   
Fleet in 1955” (see below). It showed an empty ocean,   
reflecting his belief that submarines would become so   
dominant that surface ships would be rendered obso­  
lete. That did not happen in 1955, but has it happened   
in 2025 because of antiship missiles?4  
While Russian naval losses might suggest that for   
high-end conflicts, U.S. LSCs have nonetheless been   
valuable in the Red Sea and Gaza operations. Posi­  
tioned in the Red Sea and Eastern Mediterranean,   
these ships have had 400 engagements with Houthi   
missiles. No missiles hit the warships, few hit Israel,   
and maritime traffic continued through the Red Sea,   
though at a reduced level. The ships’ missile defenses   
were highly effective against the small missile volleys   
that the Houthis could launch. While this success is   
encouraging, it is not determinative; the ships remain   
untested against the volume of fire that a great power   
such as China could employ.  
submarine, pushed Russian naval forces out of Russia’s   
forward naval base at Sevastopol, and contested the   
entire Black Sea. This success particularly raises the   
question of the future viability of surface ships.   
Wartime Experience   
Ukraine’s sinking of the Russian battlecruiser Moskva   
by long-range antiship missiles launched from the   
shore shocked Russia and the world. Nor was this   
an isolated event: Other Russian surface ships have   
fallen victim to one-way (“suicide”) drones (two ships   
destroyed) and long-range surface-to-surface missiles   
(six ships destroyed).2  
Wargames by CSIS, the Center for Strategic and   
Budgetary Assessments, the Hudson Institute, and   
the International Institute for Strategic Studies have   
questioned the survivability of surface ships in a great   
power conflict against China, especially large surface   
combatants (LSCs), the multibillion-dollar destroyers   
and cruisers that have been the backbone of fleets   
since World War II.3 Volleys of Chinese missiles can   
overwhelm ship defenses and push surface ships back   
hundreds of miles to seek safety until Chinese missile   
Admiral Karl Dönitz shown with the painting “The Fleet in 1955” in his home in December 1974.   
Photo: Werner Baum/picture alliance/Getty Images

**Page 108**

102  
The Future of Seapower  
be even more threatened. This is a perennial debate,   
having gone on for 50 years. It affects the U.S. Navy   
the most, as it operates 11 aircraft carriers, but eight   
other countries have invested in carriers: China (3),   
the United Kingdom (2), India (2), Italy (2), Japan (2),   
France (1), Spain (1), and Turkey (1).  
Wartime Experience   
Unfortunately, current events provide little insight   
into the role of aircraft carriers in combat between   
highly capable opponents. Russia’s sole carrier has   
not participated in the Ukraine war. The sinking of the   
Moskva, an old battlecruiser without escorts, does not   
provide a sufficient example of what might happen to   
a modern aircraft carrier with its air wing and escorts.   
Events in the Eastern Mediterranean reinforce histor­  
ical experience. U.S. carriers have conducted many   
missions to intercept Iranian and Houthi missiles.   
Missile threats did not force them to retreat. However,   
the carriers did not face the massive missile salvos   
that Russia or China could launch.  
The debate on aircraft carriers might fade into the   
background, except that recent wargaming has also   
raised questions about aircraft carrier survivability.   
China’s massive missile inventories could overwhelm   
carrier air defenses, and its fleet of 65 submarines might   
penetrate a carrier’s defensive screen. Wargames alone   
are unlikely to change naval attitudes toward carriers,   
but they have kept the question on the table. And the   
matter of carrier cost is always present.14 Nuclear carri­  
ers cost about $13 billion each, plus $8 billion for the air   
wing and another $8 billion for escorts. Helicopter and   
short-takeoff carriers cost about half that.  
On the other hand, carriers show their usefulness   
every day for crisis response, regional conflicts, and   
deterrence. (For a more detailed description of this   
debate, see the carrier discussion in the 2022 CSIS   
report on military forces.15) U.S. carriers have been in   
constant demand and routinely conduct real-world   
missions. The same is true for other countries. Since   
2014, UK and French aircraft carriers have launched   
airstrikes against ISIS targets in Iraq and Syria as part   
of an international coalition.16 Carriers also played a   
key role in enforcing the NATO no-fly zone during the   
Libyan Civil War.17  
Adapting to the New Environment   
Given this uncertainty, the U.S. Navy appears to be hedg­  
ing its bets. The current fleet has 85 LSCs in a total fleet   
of 293.5 This is far below the 104 LSC goal in the 355-  
ship Navy called for by the first Trump administration.6   
However, it roughly equals the 87 LSC goal in the Navy’s   
2023 381-ship fleet plan. Thus, between 2016 and 2023,   
the overall fleet plan increased by 7 percent, but the goal   
for LSCs decreased by 8 percent, reflecting this concern   
about LSC survivability. The U.S. Navy’s alternative   
shipbuilding plan for FY 2025 further sacrificed surface   
fleet numbers to reduce shipbuilding costs, projecting a   
gradual decline in LSCs to 70 total.7 Extrapolating these   
long-term plans produces an even lower projection for   
LSCs: The plan envisions a 1-2-1-2-1 building profile (i.e.,   
three ships every two years) for the late 2030s.8 With an   
expected LSC service life of 35 years, that equates to a   
long-term inventory of 53 vessels.9  
The recent reconciliation bill (“One Big Beautiful   
Bill”) developed by Congress and signed by the presi­  
dent added two destroyers, indicating some support   
for LSCs if funding were available.10  
China’s Navy—the People’s Liberation Army Navy   
(PLAN)—has taken the opposite approach, building a   
large fleet of LSCs now numbering more than 100.11   
Where the United States builds two to three LSCs per   
year, China builds five.12 Although China has made   
advances in uncrewed systems, the PLAN has priori­  
tized building LSCs for its near-seas defense.13  
Looking Ahead  
An event showing high surface ship vulnerability,   
which is already widely discussed, would push many   
navies to reconsider their LSC programs. Alterna­  
tively, a revival could occur, driven by uncrewed   
surface vessels (USVs) equipped with sensors. These   
USVs would act as scouts, thereby reducing the vul­  
nerability of surface ships. Regardless, ships need a   
lot of sea room to survive. The days of fleets standing   
close off a hostile shore are gone.  
The Future Role   
of Aircraft Carriers  
If LSCs struggle to survive in modern naval combat,   
aircraft carriers—the apex surface combatants—would

**Page 109**

103  
Mark F. Cancian  
marines. Interestingly, the reconciliation bill does not   
provide any money for aircraft carriers despite having   
$29 billion for shipbuilding overall.  
All countries face an additional influence in   
designing naval forces: the need to maintain a viable   
shipbuilding industrial base. For the U.S. Navy, that   
requirement has sometimes driven it to consider   
unwise policies, such as building more nuclear air­  
craft carriers, to satisfy the shipbuilding industry,   
but retiring older carriers early to satisfy critics. This   
increases the amortized cost of an aircraft carrier   
from $220 million per year to $370 million.19 Other   
navies with carriers face similar pressures, as carriers   
represent the largest naval ship they build. All coun­  
tries should remember that shipbuilding industrial   
bases exist to put strategically useful ships to sea, not   
to maintain themselves.  
Looking Ahead  
Eventually, the debate will be resolved; a high-intensity   
conflict will occur, and carriers will either show their   
survivability and value or be so severely damaged that   
their limited utility becomes evident. Resolution could   
happen tomorrow, or it might not happen for decades.   
Until then, expect continuing debate.  
Eventually, the debate will be   
resolved; a high-intensity conflict   
will occur, and carriers will either   
show their survivability and value   
or be so severely damaged that their   
limited utility becomes evident.  
The Future Role of   
Uncrewed Naval Systems  
The rise of uncrewed systems in the Ukraine war is   
a major change from earlier wars and a recurring   
theme throughout this volume. The experience at sea   
has been particularly dramatic.  
As a result, the number of nations operating air­  
craft carriers has not changed. There are nine today,   
and there were nine 50 years ago in 1975 (Argentina,   
Australia, Brazil, France, India, Spain, the United   
Kingdom, the United States, and the Soviet Union).   
What has changed is that some medium powers have   
dropped out (Argentina, Australia, and Brazil), while   
some rising powers have joined the group (China and   
Turkey), as has Italy, a reviving naval power.18  
Table 11.1: Navies with Aircraft Carriers,   
1975 and 2025  
1975  
2025  
Argentina  
China  
Australia  
Italy  
Brazil  
Turkey  
France  
France  
India  
India  
Spain  
Spain  
United Kingdom  
United Kingdom  
United States  
United States  
Soviet Union  
Russia  
Source: John Moore, Jane’s Fighting Ships 1975-76 (New York:   
Jane’s Publishing, 1975); and Janes, Janes Fighting Ships   
2025-2026 (New York: Jane’s Publishing, 1975), https://shop.  
janes.com/fighting-ships-25-26-yearbook-6541-3000250021.  
Adapting to the New Environment  
Aircraft carrier usefulness for regional conflicts and   
crisis response, coupled with the maritime prestige   
they bring, will keep them in the world’s navies going   
forward. For most countries, cost and naval budgets will   
drive carrier construction decisions more than theory.   
The U.S. Navy is doing what it did before World   
War II: pursuing all options until an answer is clear.   
In the 1930s, that meant maintaining both battleships   
and aircraft carriers. Today, it means sustaining air­  
craft carriers as well as potential replacements such as   
ground-based missiles, long-range aircraft equipped   
with antiship missiles, uncrewed systems, and sub­

**Page 110**

104  
The Future of Seapower  
North Korean bases. Japan’s Kure naval base is about   
650 miles from the Chinese naval base at Shanghai.   
All could conduct USV attacks on their adversaries   
or similar attacks with uncrewed underwater vessels   
(UUVs).   
A U.S. naval drone strike against Chinese ships   
would be more difficult because of the much longer   
distances. Guam, the closest base to China in U.S. ter­  
ritory, is 2,000 miles away. The United States would   
need to arrange close-in basing with an ally or partner.  
However, one-way naval drones are an entirely   
different approach to uncrewed vessels than most   
countries have taken. The U.S. Navy has no programs   
for one-way naval drones, at least in the unclassified   
space. USVs in development have focused on long-  
range shooting and sensing, not one-way attacks. The   
primary U.S. Navy program for UUVs with strike capa­  
bility is the Orca, designed for reconnaissance and   
mine-laying operations. The U.S. Navy has ordered   
six vessels (one test article and five prototypes), but   
only one prototype is in testing, delayed by years of   
technical difficulties.21 At $110 million each, they are   
too expensive for a one-way mission.22 U.S. Navy ship­  
building plans envision hundreds of USVs and UUVs   
in the fleet, but budgets do not yet reflect that. No   
USV or UUV is a program of record (a formal acquisi­  
tion program with funds allocated and building plans   
specified in future budgets).23  
The reconciliation bill makes a big bet on   
uncrewed and autonomous systems, adding $16.6   
billion overall (11 percent of the defense increases).   
Of this amount, about one third ($5.3 billion) goes to   
Navy programs. This represents a substantial invest­  
ment and a strong congressional statement about   
where increased efforts are needed.  
Other navies are taking similar initiatives, though   
with access to fewer resources. The UK and French   
navies both have UUV programs underway that focus   
on minesweeping and intelligence, surveillance, and   
reconnaissance. The Royal Navy will begin trials for   
a crewless submarine in June 2025 as part of Project   
Cetus.24 In 2024, France announced a program to   
develop the first UUV specifically designated for combat   
operations.25 All are moving more slowly than Ukraine.  
Wartime Experience   
The use of small USVs has been a tremendous and   
unexpected Ukrainian success in operations against   
Russian forces. As noted earlier, Ukrainian USVs sank   
two major warships and half a dozen small vessels,   
while damaging several others. Controlled remotely   
and laden with explosives, Ukrainian USVs traveled   
far offshore (200–400 miles) to detonate against Rus­  
sian targets. These attacks helped drive the Russian   
fleet from Sevastopol to the Russian naval base at Nov­  
orossiysk, 300 miles east.   
These successes occurred in favorable circum­  
stances. Ukraine had excellent intelligence on Rus­  
sian dispositions; the Russian ships must spend most   
of their time at anchor in known ports because of   
the Black Sea’s confines, and the distances are rela­  
tively short. Further, despite excitement about how   
USVs have revolutionized naval warfare, most Rus­  
sian naval losses have been to long-range precision   
missiles against stationary ships in port, not surface   
drones. USV use in warfare is just beginning.  
Adapting to the New Environment  
Many navies face the problem of operating inside   
an adversary’s defensive zone. Surface ships have   
difficulty doing that, but uncrewed systems—which   
are smaller, cheaper, and more expendable—could.   
The favorable circumstances that Ukraine enjoys   
for employing USVs describe the environment that   
most navies face. NATO navies, for example, are only   
a short distance from Russian ports, enjoy excellent   
reconnaissance, and have lots of time to prepare. This   
presents NATO navies with an opportunity.   
One could imagine countries adapting existing   
systems, as Ukraine has done, to strike their adver­  
sary’s vessels in port. As an illustration, a CSIS report,   
Inflicting Surprise: Gaining Competitive Advantage in   
Great Power Conflicts, imagined a surprise strike by   
U.S. autonomous underwater vessels against Russian   
ships of the Northern Fleet.20   
The circumstances also apply to navies in the   
Pacific, with the important exception of the United   
States. The Philippines is next to the South China Sea,   
a region of great tension and possible future conflict.   
South Korean naval bases are only 100 miles from

**Page 111**

105  
Mark F. Cancian  
of the Cold War, Russia has prioritized its submarine   
fleet at the expense of other naval capabilities like sur­  
face ships. Submarines have had a major impact on   
U.S. Pacific wargames, prompting the United States   
to invest billions of dollars in shipyards to accelerate   
production. Before the Moskva, the last major surface   
combatant sunk in conflict was the Argentine cruiser   
Belgrano, torpedoed by the UK submarine Conqueror   
during the 1982 Falklands War.   
Wartime Experience  
At the beginning of the war, the six relatively modern   
Kilo-class submarines in Russia’s Black Sea fleet were   
expected to have a major impact. Yet, these subma­  
rines have been largely invisible, and not simply   
because they were submerged. There are no refer­  
ences to any operations they have conducted. Indeed,   
the most prominent mention of Russian submarines   
has been the loss of one, which was struck in dry dock   
by long-range Ukrainian missiles.   
The answer may simply be a lack of targets.   
Ukraine has no major naval vessels, and Russia has   
been unwilling to use submarines to attack grain-  
laden cargo ships. Perhaps their mission was to keep   
NATO forces out of the Black Sea, and in that, they   
succeeded. Still, the lack of activity is curious.  
Adapting to the New Environment   
This lack of submarine impact will not alter anything   
in the U.S. shipbuilding plan for submarines, which is   
currently driven by expectations about a U.S.-China   
conflict in the Western Pacific. Submarines’ stealth   
enables them to penetrate China’s defensive bubble,   
where surface ships and even aircraft cannot go.   
NATO navies are also unlikely to change their   
plans for submarines because they are largely   
driven by the Russian submarine fleet. That fleet has   
become more active in the last decade, having recov­  
ered from its post–Cold War doldrums. The current   
wars have not shed any light on submarine-ver­  
sus-submarine conflict.  
Other maritime powers and many minor powers   
will maintain their submarine fleets because it is the   
only way they can enter the major leagues of naval   
power. Submarines allow even a minor power to   
Navies also face the prospect of being attacked by   
such systems, which are available to weak states and   
nonstate actors as well as major powers. As Russia has   
discovered, a navy’s greatest vulnerability is in port   
when ships are stationary for an extended period and   
an adversary can execute a strike that requires time   
to plan and execute. The U.S. Navy experienced this   
with the terrorist attack on the USS Cole in 2000; that   
short-range attack by suicide bombers badly damaged   
the ship and killed 17 sailors.26 The proximity of NATO   
and Pacific navies to their adversaries, therefore, cre­  
ates vulnerability as well as opportunity.  
Naval anchorages have not faced long-range naval   
threats since World War II. Then, Japanese mini-sub­  
marines attacked anchorages at Pearl Harbor, Sydney,   
Australia, and Ulithi Atoll, the last two attacks being   
successful in sinking a ship.27 Italian mini-submarines   
attacked the British anchorage at Alexandria, Egypt,   
sinking two battleships. The German U-47, under its   
celebrated captain, Gunther Prien, snuck into the   
Royal Navy’s anchorage at Scapa Flow and sank a   
battleship. Navies face a “back to the future” moment.   
Thus, navies will need to defend against USV and   
UUV attacks by hardening anchorages, a precaution   
that has been unnecessary since World War II. After   
both the Cole and 9/11 attacks, the U.S. Navy imple­  
mented new force protection procedures. These will   
need some expansion to deal with this new kind of   
threat—and better to do the next round of enhance­  
ments before an incident occurs. However, counter­  
measures cannot be too expensive, given all the other   
demands on naval budgets, or too intrusive, given the   
need for continuous naval operations.  
Looking Ahead  
Watch for future attacks against ships at anchor. The­  
oretical threats may drive some action, but a success­  
ful attack outside the Black Sea would galvanize the   
target navy and provide another alert to global navies.   
The Small Impact of Russia’s   
Black Sea Submarines  
This is the dog that did not bark.28 Submarines are   
regarded as the ultimate weapon in naval combat   
because of their stealth and lethality. Since the end

**Page 112**

106  
The Future of Seapower  
Looking further back in history, the Royal Navy   
expended over 200 antisubmarine weapons to   
counter the single Argentine submarine at sea during   
the 1982 Falklands War. Despite this immense expen­  
diture, the submarine was not damaged.34 Whether   
the Royal Navy was trigger-happy, unlucky, or saddled   
with ineffective munitions, the high rate of expendi­  
ture was—and still is—worrisome.  
The need for larger inventories of naval and other   
munitions is, therefore, old news. The U.S. Depart­  
ment of Defense got the message and has increased its   
production of nearly every type of missile. For exam­  
ple, production of SM-6s will increase from 125 to 300   
per year by 2027, while production of LRASMs will   
increase from about 100 to 230 per year in 2027 (total   
Navy and Air Force procurement).35 NATO navies are   
also expanding their inventories of naval munitions.36   
That is an important step forward and will   
strengthen the joint force’s capabilities to fight in   
high-intensity conflicts. However, U.S. forces in the   
CSIS wargame fired about 100 LRASMs per day, so the   
expanded inventories would last longer in a conflict   
but not beyond several weeks. It is difficult to build   
large inventories of expensive weapons ($4.4 million   
for an SM-6, $3.5 million for a LRASM) with limited   
shelf lives (about 20 years).37 Ultimately, this is an   
unsolved problem.  
Adapting to the New Environment  
It is reasonable for all navies to build larger munitions   
inventories despite the high cost. Nearly all wars last   
longer than planners expect. Nevertheless, militaries   
must find affordable solutions to the missile inventory   
challenge because they cannot build inventories large   
enough for a protracted conflict. Solutions might   
include less expensive missiles or different technol­  
ogies, such as directed energy.  
Looking Ahead  
Watch munition procurement levels when the war in   
Ukraine ends. Although the war in Ukraine does not   
drive U.S. or NATO demands for naval missiles, the   
end of that war may undermine the urgency of build­  
ing stockpiles in general. This has been an industry   
concern, partly offset by multiyear contracts, which   
lock in future production.   
threaten an adversary's largest warships and mer­  
chant fleet. This is unlikely to change.  
Looking Ahead   
Watch for the composition of Russia’s postwar Black   
Sea fleet. If Russia withdraws its submarines from the   
Black Sea, that represents its assessment that the sub­  
marines’ contribution was insufficient and that this   
asset would be better used in one of the other fleets—  
Northern, Baltic, or Pacific. If the submarines remain,   
the assessment is that submarines were Russia’s ace   
in the hole. In either case, Russia’s assessment will   
help the West better understand wartime submarine   
operations in the twenty-first century.  
The Adequacy of   
Naval Munitions Inventories  
Ships fire a lot of munitions in combat. Although this   
indicates a requirement for large inventories, the high   
cost of munitions prevents navies from stockpiling   
everything they might need in a protracted conflict.  
Wartime experience.   
U.S. operations in the Red Sea against Houthi missiles   
expended 200 missiles over 15 months, in addition to   
cannon rounds.29 This has dented U.S. inventories and   
raised concerns about their adequacy for a major con­  
flict. For example, 180 of these missiles were SM-2s or   
their replacement, SM-6s. In past years, the U.S. Navy   
has procured 125 missiles per year.30 That means that   
one limited series of engagements expended a year   
and a half of missile production.  
Ukraine’s air war has shown the same dynamic.   
Attacks by cruise missiles and one-way drones have   
required large numbers of air defense missiles in   
response, overwhelming the limited inventories of   
the United States and NATO.  
A series of CSIS wargames found that in a conflict   
with China, the United States ran out of Long-Range   
Anti-Ship Missiles (LRASMs) within the first week—  
often within the first several days.31 A later CSIS analysis,   
Empty Bins in a Wartime Environment, described muni­  
tions shortfalls in many areas.32 Indeed, many analyses   
have identified inadequate munitions inventories as a   
major weakness.33

**Page 113**

107  
Mark F. Cancian  
The fundamental problem is that munitions   
struggle to compete in peacetime budget debates.   
Although vital in protracted conflict, they are a “ster­  
ile” investment: Investments in ships, aircraft, and   
combat vehicles are visible over the decades of their   
operational lives. Munitions go into secure bunkers,   
never to be seen again until they are expended or   
demilitarized.   
Conclusion  
Naval analysts should not extrapolate too much from   
recent events in the wars in Ukraine and the Middle   
East, since naval activity was limited and ancillary to   
the primary campaign on land. Nevertheless, some   
insights are clear enough to implement now: expand­  
ing munitions inventories, accelerating the devel­  
opment and production of uncrewed systems, and   
hedging on major surface combatants.  
There are also many things to watch for as indica­  
tors for additional action. These recognize the uncer­  
tainty of projecting limited current experiences into   
the future, but acknowledging possible futures is the   
first step in adapting to them. Having thought through   
a problem ahead of time facilitates a response. Thus, it   
is worthwhile to spend time thinking about responses   
to different futures.  
Finally, having a variety of naval capabilities avail­  
able facilitates a response even if the tools are not ini­  
tially available in the desired quantity. Expanding an   
existing capability is much easier than developing a   
new one in the crucible of conflict. Because expan­  
sion is easier than introduction, having a variety of   
capabilities already at hand provides a better hedge   
against an uncertain future.

**Page 114**

Daniel Byman, Seth G. Jones, and Sofia Triana  
CHAPTER 12  
The Evolution of   
Irregular Warfare

**Page 115**

109  
Daniel Byman, Seth G. Jones, and Sofia Triana  
”  
“  
U.S. and allied planning, posture, and   
doctrine must prepare for irregular   
warfare, incorporating the impact   
of civilians and recognizing the vital   
roles of special operations forces and   
intelligence services in conflict.  
can inflict many casualties, undermine resil­  
ience, and raise the price of occupation.   
2.   
Civilians are often at the heart of irregular   
warfare—as shields, as victims, and as targets   
of coercion—and governments must consider   
this when confronting opponents who use   
irregular warfare and in their own irregular   
warfare operations.   
3.   
Intelligence is critical to counter irregular   
warfare, as Israel’s successes show, and in   
general an effective response can limit the   
coercive power of irregular warfare.  
U.S. and allied planning, posture, and doctrine   
must prepare for irregular warfare, incorporating   
the impact of civilians and recognizing the vital roles   
of special operations forces (SOF) and intelligence   
services in conflict. This, in turn, will require adap­  
tation, including recognizing differences between   
irregular warfare involving great powers (as com­  
pared with past U.S. efforts against weaker insurgen­  
cies and terrorist groups) and ensuring that private   
T  
he wars in Ukraine and the Middle East of­  
fer many lessons for better understanding,   
conducting, and countering irregular war­  
fare.1 On October 7, 2023, the Hamas attack on Israel   
combined attacks on Israeli military bases near Gaza,   
border security infrastructure, and military commu­  
nications equipment with atrocities against Israeli ci­  
vilians and the taking of civilian hostages. Russia, for   
its part, accompanied its February 2022 invasion of   
Ukraine with cyberattacks, attempts to kill President   
Volodymyr Zelensky, and a deepfake in March 2022   
to try to encourage Ukraine’s surrender. Ukraine has   
used guerrilla attacks, sabotage, and leadership as­  
sassinations to fight Moscow. Some combination of   
these and other forms of irregular warfare is likely in   
future conflicts.  
Drawing on the lessons from the Ukraine and   
Middle East wars, this chapter makes the following   
arguments about irregular warfare:  
1.   
Irregular warfare often occurs as a prelude   
to, or side-by-side with, regular warfare and   
photo: mohammed huwais/afp/getty images

**Page 116**

110  
The Evolution of Irregular Warfare  
Nations reports over 12,000 civilians have died so far,   
including many in territory occupied by Russia.4   
Ukraine has also targeted Russian warships in the   
Baltic Sea as well as railway networks, blowing up the   
Sveromuysky tunnel in eastern Russia and damaging   
a critical railway bridge near the city of Kinel. In the   
case of the Sveromuysky tunnel attack, Ukraine’s   
Security Service reportedly sabotaged a train’s fuel   
tank, causing it to catch fire as it moved through the   
tunnel. Other trains scheduled to go through the   
tunnel were then rerouted to a bridge where they   
were damaged as explosive devices planted along the   
alternate route promptly detonated.5   
In the Middle East, some groups, like the   
Lebanese Hezbollah, have integrated irregular   
approaches to warfare into their order of battle and   
military doctrine. Hezbollah has long fought Israel   
with rocket and missile strikes, guerrilla warfare,   
and terrorist attacks, and it has also trained groups—  
like Hamas—that have a similar set of capabilities,   
if less powerful. Israel, which has mostly fought a   
conventional war against its opponents, nonethe­  
less has mixed a conventional invasion of Gaza with   
leadership strikes on Hamas throughout the Middle   
East and Hezbollah in Lebanon.  
The High Cost of Irregular Warfare   
Irregular warfare is often considered a weapon of the   
weak, yet it can still inflict considerable costs on a   
strong opponent. Hamas was undeterred by Israel’s   
military superiority and killed around 1,200 Israelis—  
mostly civilians—on October 7, inflicting an extremely   
high number of casualties on a small and casualty-sen­  
sitive country. Over 400 more Israeli soldiers have   
died in subsequent combat in Gaza, where Hamas   
has used hit-and-run attacks, improvised explosive   
devices (IEDs), and other indirect means to inflict   
casualties while avoiding a direct confrontation with   
the better-armed and better-trained Israel Defense   
Forces (IDF).6 The ensuing conflagration has similarly   
led to the deaths of some 60,000 Palestinians, fur­  
ther illustrating the high costs of irregular warfare. In   
addition to the death toll in the Gaza war, the Hamas   
attacks pushed Israel into war not only in Gaza but   
also in Lebanon and Yemen.   
sector technology and expertise are incorporated   
into U.S. efforts.  
This chapter has three sections. The first section   
notes several lessons from the Ukraine and Middle   
East wars; the second examines Israeli and Ukrainian   
successes regarding irregular warfare; and the third   
discusses the implications of these lessons for the   
future of warfare.  
Lessons from Ukraine   
and the Middle East  
The experiences of Ukraine and the Middle East offer   
many lessons on how to think about irregular war­  
fare now and in the future. First, irregular warfare   
often occurs side by side with conventional warfare,   
and it is necessary to prepare for the two happening   
simultaneously as well as in isolation. Second, the   
death toll and other costs of irregular warfare can be   
high, especially for enduring conflicts. Third, hostage   
taking, terrorism, assassination, and other means of   
conducting and fighting irregular warfare are often   
part of broader efforts to coerce and deter opponents.  
Irregular and Conventional Warfare   
in Tandem   
In both the Ukraine and Middle East wars, irregu­  
lar warfare has occurred simultaneously with regu­  
lar warfare. In parts of Ukraine occupied by Russia,   
Ukrainian partisans, directed by Ukrainian special   
operations forces, used guerrilla attacks to kill Rus­  
sian forces, disrupt lines of supply and communica­  
tion, and sabotage Russian weapons systems. These   
efforts disrupted the flow of military supplies and   
forced the Kremlin to divert resources from the front   
lines to the repair and defense of its rail infrastructure   
instead, placing additional strain on an already strug­  
gling railroad network. Ukrainians have also used   
nonviolent resistance, such as wearing yellow ribbons   
in solidarity and distributing information to counter   
Russian propaganda.2 Overall, Ukraine’s efforts have   
hindered the movement of Russian troops and cre­  
ated supply bottlenecks.3 More importantly, they   
have also prevented Russia from successfully incor­  
porating captured Ukrainian territory into Russia.   
The cost for Ukrainian civilians is high: The United

**Page 117**

111  
Daniel Byman, Seth G. Jones, and Sofia Triana  
Russian families and refusing to return them to their   
Ukrainian relatives.11   
In part because irregular forces hide among   
civilians, countering irregular warfare can involve   
considerable death and suffering in the civilian pop­  
ulation. Hamas fighters have blended in with Gazan   
civilians and hidden arms and fighters in civilian   
infrastructure, such as hospitals and schools. Isra­  
el’s response has been devastating for ordinary   
Gazans, with over 60,000 Gazans killed in total as   
of August 2025, most of them civilians, as well as   
most of Gaza’s infrastructure destroyed. Operations   
that involve numerous civilian casualties place an   
additional burden on democracies, which are more   
likely to receive criticism when their military opera­  
tions involve civilian deaths.   
Israel has devastated Hamas and Hezbollah   
through assassinations, and both Russia and Ukraine   
have used assassinations as well. Although Ukrainian   
authorities rarely claim responsibility for their covert   
actions, they have carried out high-profile assassi­  
nations in occupied Ukrainian territories as well as   
on Russian soil. Among the individuals successfully   
targeted by Kyiv are Vladlen Tatarsky, a Russian mili­  
tary blogger; Igor Kirillov, the chief of Russia’s radio­  
active, chemical, and biological defense forces; and   
Illya Kyva, a pro-Russia former Ukrainian member of   
parliament who fled to Russia during the war. Ukraine   
has also targeted leaders in occupied Ukraine who   
collaborated with Russia.12 Moscow, for its part, has   
also undertaken a broad campaign of targeted assas­  
sinations in Ukraine and across Europe, poisoning the   
wife of Ukraine’s military intelligence chief, killing   
a senior Ukrainian covert action leader, plotting to   
assassinate the chief executive of German arms maker   
Rheinmetall, and gunning down a Russian military   
defector in Spain.13   
Countering Irregular Warfare  
Although irregular warfare is difficult to combat, both   
Israel and Ukraine have scored many victories. The   
Lebanese Hezbollah, one of the world’s premier guer­  
rilla organizations and one that fought Israel to a stand­  
still in their last all-out clash in 2006, largely failed in   
its use of irregular warfare against Israel and ended up   
Such irregular warfare measures have raised the   
price of occupation. Fighting insurgents, especially in   
densely populated areas like Gaza, requires a grind­  
ing counterinsurgency with high force levels. For the   
Gaza war and other Middle East conflicts, Israel mobi­  
lized some 360,000 reservists.7 As of August 2025,   
Israel has conducted a 22-month war to suppress   
Hamas, yet the group remains the strongest organi­  
zation in Gaza. Similarly, Russia has not fully pacified   
the territory it occupies.8   
Irregular Warfare as a Tool of Coercion   
and Deterrence  
The threat of irregular warfare can also be used in   
attempts to coerce and deter. Iran, for example,   
relies heavily on Hezbollah and other proxy groups to   
impose costs on Israel, the United States, and its Arab   
enemies. The threat of Hezbollah rocket and terrorist   
attacks was in part meant to deter Israeli operations   
against Iran itself. In addition, Iran-backed groups like   
the Houthis attacked Red Sea shipping to coerce Israel   
into ending its war in Gaza. Russia has also engaged   
in a comprehensive campaign of sabotage in Europe   
to punish countries that supported Ukraine and limit   
future support. Moscow’s increasingly brazen attacks   
have included jamming GPS systems to disrupt civil   
aviation, causing deliberate damage to undersea gas   
pipelines and telecommunications cables, sabotaging   
water utilities in Poland and France, and conducting   
arson attacks in the United Kingdom, Czech Repub­  
lic, Germany, Lithuania, and Latvia.9 Russia has also   
targeted facilities with more direct links to the war in   
Ukraine, including a BAE Systems munitions factory   
in Wales and a U.S. military base in Bavaria.10  
Hostage taking has proved an important part of   
both the Gaza and Ukraine wars. In Gaza, Hamas and   
other Palestinian groups initially took 251 hostages—  
including children, the elderly, and other noncomba­  
tants as well as many non-Israelis—and, as of August   
2025, around 50 are still in captivity, although more   
than half of these are presumed dead. The presence of   
hostages has complicated Israeli targeting and offered   
a form of protection for Hamas leaders. In occupied   
Ukraine, Russia has engaged in forced deportations of   
almost 20,000 children to Russia, placing them with

**Page 118**

112  
The Evolution of Irregular Warfare  
highly public way. In part due to threats from Israel   
and the United States, Iran also hesitated to escalate   
further and counseled some of its proxies, such as   
those in Iraq, to limit attacks on U.S. bases.16 When   
Iran and Israel (joined by the United States) entered   
into the larger conflict in June 2025, Israel was quick   
to gain air supremacy and, in a short but effective air   
campaign, set back Iran’s nuclear program and killed   
many Iranian leaders, with only a small number of   
casualties on the Israeli side.  
Implications for the Future   
of Irregular Warfare  
During the Cold War, the most frequent type of com­  
petition between the Soviet Union and the United   
States was irregular warfare, as the two sides fought   
proxy wars in Africa, Asia, Europe, and Latin Amer­  
ica. The same may be true in the coming years as   
China expands its global presence. Although a Chi­  
nese invasion of Taiwan is possible, more likely are   
cyberattacks, disinformation, sabotage, and military   
threats to coerce Taipei and undermine morale.   
In addition, the staggering cost of the Ukraine war   
in both money and lives suggests that an exhausted   
but predatory Russia may in the future prefer to use   
irregular war instead of conventional attacks to expand   
its influence. Russia’s Main Directorate (GRU), Foreign   
Intelligence Service, semiprivate military compa­  
nies, and other state and nonstate organizations are   
likely to continue assassinations, sabotage operations,   
offensive cyber campaigns, disinformation operations,   
intelligence collection, and other clandestine activities.   
The GRU’s Service for Special Activities is likely to be   
particularly active, including Unit 29155 (also known   
as the 161 Center or, more formally, the 161 Intelligence   
Specialists Training Center), Unit 54654, and the GRU’s   
headquarters and planning department.17 Russia will   
also likely continue to wage a disinformation campaign   
against the United States, conduct offensive cyber cam­  
paigns against U.S. and Western government agencies   
and companies, and engage in a range of other activi­  
ties such as assassinations and sabotage.  
Iran, for its part, emphasizes irregular warfare   
given the weakness of its conventional forces. It will   
taking tremendous losses. Israeli intelligence deeply   
penetrated Hezbollah, sabotaging its pagers and   
walkie-talkies and gaining precise information on the   
locations of Hezbollah leaders. With this intelligence,   
Israel was able to decimate Hezbollah’s senior leader­  
ship, including killing the group’s longtime secretary   
general, Hassan Nasrallah, and inflicting significant   
losses on its rank and file. Israel also successfully tar­  
geted much of the group’s rocket and missile arsenal.   
This stockpile, estimated to contain between 120,000   
and 200,000 projectiles, was reduced by half due to   
Israeli airstrikes.14 Hezbollah was forced to sue for   
peace, ending its attacks on Israel and agreeing to   
withdraw its forces from the Lebanon-Israel border,   
with Israel making few concessions.  
Iran’s ties to Hezbollah, militant groups in Iraq,   
and the Houthis did not deter the United States or   
Israel from acting against it militarily. Israel in par­  
ticular targeted Iranian military leaders in Syria and   
Lebanon and the leader of Hamas when he was in Iran.   
Tehran did try to restore its credibility with drone and   
missile attacks on Israel, but this too was a failure, with   
Israel—helped by the United States, Jordan, and other   
countries—tracking and downing most of the attacking   
force. When Israel and Iran fought a bigger battle in   
June 2025, Hezbollah avoided joining the fray.  
Hamas’s seizure of Israeli hostages has likewise   
not proven an effective deterrent. Despite the pres­  
ence of over 200 hostages, Israel launched an all-out   
assault on Gaza, and in its operations has conducted   
highly destructive attacks that have threatened the   
hostages as well as their Hamas kidnappers. Israeli   
ground forces have also accidentally killed hostages.15   
Finally, Israel and the United States have pre­  
vented Iran from escalating irregular warfare into   
conventional success; indeed, Tehran’s efforts to do   
so have led to embarrassing failures. After the killing   
of Iranian, Hezbollah, and Hamas leaders, Iran twice   
launched large salvos of rocket, missile, and drone   
attacks on Israel, and Israel responded with limited   
but precise attacks—the first time Iran and Israel have   
directly attacked each other’s territory. Effective intel­  
ligence and air defense, however, prevented Iran’s   
salvos from causing significant casualties in Israel, dis­  
playing Tehran’s conventional military weakness in a

**Page 119**

113  
Daniel Byman, Seth G. Jones, and Sofia Triana  
mation about their operations, specifically regarding   
their harmful impact on civilians.  
Assassination and sabotage are likely to remain   
part of irregular warfare, both on offense and   
defense. If the Russia-Ukraine conflict is a guide, some   
of these assassinations are likely to occur far from the   
front lines, requiring new security protocols in more   
remote bases and even in faraway homelands. Sabo­  
tage of U.S. bases and supply lines, as well as those of   
allies, is also highly likely.  
SOF will play a particularly critical role in com­  
batting irregular warfare in the future. SOF need   
to adapt given the many differences between fight­  
ing against forces of or supported by a great power   
versus fighting terrorists. Russian forces, for exam­  
ple, have persistent surveillance and airpower that   
will make clandestine operations against them far   
harder for U.S. forces compared with U.S. efforts   
fighting terrorist groups. It will also be important   
to develop programs to raise forces to gather intelli­  
gence and fight behind enemy lines. Hostage rescue   
may also be required, even as military operations   
occur in close proximity.  
Success in irregular warfare requires superb intel­  
ligence. Targeting adversary leadership (and protect­  
ing one’s own) necessitates detailed information on   
leadership movements and communications. Striking   
irregular forces while limiting harm to civilians also   
requires excellent knowledge about the locations of   
fighters and the presence of nearby civilians. Sabo­  
tage, such as what Russia is currently conducting in   
Europe, needs to be disrupted, attributed, and called   
out to rally unified allied support. In addition, some   
intelligence may need to be released to counter claims   
that, for instance, the United States has targeted civil­  
ian infrastructure without military purpose.  
Authoritarian states are also vulnerable to irregu­  
lar warfare, of course, including information warfare.   
By leveraging commercial technologies, the United   
States and its partners should target the domestic   
populations of China, Russia, Iran, and other countries   
through covert, clandestine, and overt means, where   
appropriate. The commercial sector can be helpful in   
developing and utilizing AI, large language models,   
continue to pose an irregular warfare threat to the   
United States and its allies and partners across the   
Middle East using a range of partner forces such as   
the Houthis in Yemen, Hezbollah in Lebanon, Hamas   
and other groups in the Palestinian territories, and   
the Popular Mobilization Forces in Iraq. In addition,   
Iranian government entities such as the Islamic Rev­  
olutionary Guard Corps, as well as their nonstate   
partners, will likely improve their offensive cyber   
capabilities and their ability to conduct attacks   
against the United States and its allies and partners at   
home and abroad. Although Iran and its proxies’ set­  
backs in 2024 and 2025 will make Iran more hesitant   
to take on Israel, Tehran has little choice but to fall   
back on irregular warfare, as its conventional forces   
are poorly armed.  
In addition to excelling at high-end conflict, the   
United States and its allies must be prepared for irreg­  
ular operations with attacks on civilians and the use   
of civilians as shields, ensure there are civil affairs   
officers who can repair civilian infrastructure, create   
partnerships with private sector companies with   
cyber and other expertise, and develop other capa­  
bilities to better counter irregular warfare.  
Even as the United States emphasizes great   
power competition, it must not lose the knowledge   
gained after its interventions in Afghanistan, Iraq,   
and other parts of the world in the post-9/11 era—as   
happened when the U.S. military deliberately tried   
to put the Vietnam War behind it and, at high cost,   
had to relearn how to fight insurgencies. In addition,   
unlike in the Vietnam era, insurgents and other irreg­  
ular forces may have great power support, including   
better weapons, funding, and intelligence. There is   
also a risk of escalation that must be managed when   
irregular forces have a great power sponsor.  
Fighting irregular opponents often risks large   
numbers of civilian deaths. In some theaters there   
will be media and international scrutiny of the   
impact of military operations on the civilian pop­  
ulation. Countries fighting in these regions will   
require a media and public relations strategy to go   
along with their operations, all while targeting pro­  
cedures that seek to minimize harm to civilians. In   
addition, countries must be prepared for disinfor­

**Page 120**

114  
The Evolution of Irregular Warfare  
Finally, an important goal is to limit the escala­  
tion of irregular warfare into conventional conflict.   
This can occur when major powers feel the need to   
respond to attacks on their proxies or when proxy   
attacks compel their targets to respond against the   
ultimate source. Israel and the United States achieved   
this with Iran in 2024, where Tehran’s fear of U.S. and   
Israeli escalation led Iran to try to calibrate its initial   
attacks to avoid escalation and to avoid additional   
attacks after its failed drone and missile salvos.19  
Conclusion  
The wars in Ukraine and the Middle East demonstrate   
that irregular warfare is not a relic of the past, but a   
defining feature of contemporary conflict—one that   
democratic states must be institutionally and opera­  
tionally prepared to confront. Civilians are often the   
primary victims, caught between actors that deliber­  
ately use population centers for tactical advantage   
and militaries that must operate under intense legal   
and normative scrutiny. Indeed, in dense urban envi­  
ronments like Gaza City, civilians are often used as   
shields, and in Ukraine, noncombatants are the princi­  
pal victims of coercive tactics intended to undermine   
resilience and morale. The persistent threat of assassi­  
nation, sabotage, and hostage taking—often executed   
through or with support from intelligence and SOF—  
will remain a central feature of irregular campaigns.   
As adversaries grow more adept in their use of irregu­  
lar means, democracies must invest not only in better   
intelligence, cyber defense, and targeting capabilities,   
but also in public communication strategies to counter   
disinformation and preserve legitimacy.  
Still, the wars in Ukraine and the Middle East have   
also demonstrated that well-coordinated efforts can   
reduce the impact of irregular warfare. Ukraine has   
disrupted numerous plots to assassinate President   
Volodymyr Zelensky. For Israel, timely and effective   
intelligence allowed it to decimate Hezbollah’s ranks   
and quickly neutralize massive Iranian drone and   
rocket attacks.  
Strategic adaptation is essential. The United States   
and its allies must preserve hard-won knowledge from   
post-9/11 counterinsurgency operations while rec­  
ognizing that great power–backed irregular warfare   
and software that directs information to specific audi­  
ences that Beijing, Moscow, Tehran, and other regimes   
are attempting to control. Offensive information opera­  
tions could focus on a range of issues, including domes­  
tic grievances and societal divisions, human rights   
abuses, economic problems, and corruption.  
Military operations and intelligence units will   
likely need to develop greater capabilities to compete   
in the information space, including for such activi­  
ties as covert influence and counter-value operations   
(targeting an adversary’s civilian population). In   
cooperation with the commercial sector, AI and large   
language models have significant potential for irregu­  
lar warfare applications. AI translation and message   
crafting can provide government officials with the   
ability to rapidly communicate in any language with   
anyone in the world. Advances in natural language   
processing will accelerate intelligence work, helping   
analysts sort through reams of text and drawing con­  
nections a human brain might not.  
The military and intelligence communities need   
to fundamentally change the way they work with   
the commercial sector to compete more effectively   
in irregular warfare—both on offense and defense.   
Commercial innovation and commercial production   
capacity provide a major advantage for the United   
States and its allies and partners in irregular war­  
fare, including for intelligence and military-related   
activities. But the United States has not adequately   
leveraged this advantage because of risk aversion,   
slow and burdensome contracting and acquisitions   
regulations, and a failure to adequately understand   
viable options in the commercial sector. There is a sig­  
nificant need to rethink the framework of government   
collaboration with this sector and to treat commercial   
entities as partners serving a common goal.  
There is also a growing need to improve next-gen­  
eration intelligence platforms, systems, and software   
that can quickly collect and analyze vast amounts   
of information on adversary activities for irregular   
warfare. Adversaries will likely attempt to hide their   
actions in a variety of terrains, including jungles,   
mountains, dense forests, subsurface locations, and   
tightly packed megacities. They will also attempt to   
use denial and deception tactics and techniques.18

**Page 121**

115  
Daniel Byman, Seth G. Jones, and Sofia Triana  
poses far more sophisticated challenges than ever   
before. This includes preparing SOF for operations   
against technologically capable adversaries, building   
rapid and resilient intelligence-sharing platforms, and   
rethinking how the government works with commer­  
cial innovators to harness advances in AI and data ana­  
lytics for irregular conflict. Future military operations   
will require increased readiness for irregular methods   
such as assassinations and sabotage, excellent intelli­  
gence, better cooperation with the private sector, and   
preparation for irregular warfare in an environment   
of great power competition. Future success will also   
depend on mitigating escalation risks—particularly   
when attacks by proxies or in the gray zone threaten to   
pull major powers into direct confrontation. The les­  
sons from Ukraine and Israel point to a critical imper­  
ative: Irregular warfare is not only a tactical reality   
but a strategic domain in its own right, and ignoring it   
would be a grave miscalculation in an era of persistent   
geopolitical competition.  
The wars in Ukraine and the Middle   
East demonstrate that irregular   
warfare is not a relic of the past, but   
a defining feature of contemporary   
conflict—one that democratic   
states must be institutionally and   
operationally prepared to confront.

**Page 122**

PART III  
Implications for Defense   
Planning and Industry

**Page 123**

Seamus P. Daniels  
CHAPTER 13  
Defense Budgets in   
an Uncertain Security   
Environment

**Page 124**

118  
Defense Budgets in an Uncertain Security Environment  
”  
“  
G  
lobal defense spending has increased dra­  
matically since the outbreak of the war in   
Ukraine in February 2022. As Russia has   
poured resources into funding its invasion and on­  
going operations, NATO allies have sought to boost   
their own defense capabilities in light of the threat   
on their borders. Meanwhile, China has continued to   
report sustained annual growth in its defense budget   
as it modernizes and grows its military in pursuit of   
its strategic objectives. And in the summer of 2025,   
Congress provided an additional $156 billion for de­  
fense as a one-time supplemental fund to enhance the   
United States’ military capabilities.1  
Uncertainty in the current global security envi­  
ronment and heightened threats have prompted   
much of this growth in defense spending as states per­  
ceive themselves and their interests to be at greater   
risk. However, despite these increases, and an agree­  
ment among NATO allies for further growth, deci­  
sions on defense spending levels remain as much a   
product of political and economic realities as they are   
Decisions on defense spending levels remain   
as much a product of political and economic   
realities as they are a response to strategic   
demands and the security environment.   
a response to strategic demands and the security envi­  
ronment. States will ultimately balance the urgency   
of their security concerns against fiscal concerns and   
other spending priorities.   
This chapter explores trends in global defense   
spending, particularly since Russia’s 2022 invasion   
of Ukraine. It first tracks changes in spending levels   
from NATO allies and the United States in the context   
of the alliance’s defense budget commitments and the   
ongoing conflict. It then assesses trends in defense   
spending by Russia and China. The chapter concludes   
with a discussion of considerations that may impact   
defense spending levels in the future.  
NATO’s Budgetary Response   
to the Ukraine War  
European governments responded to Russia’s 2022   
invasion of Ukraine by increasing their defense bud­  
gets, a clear indication that their perception of the   
threat environment has grown starker since Russia’s   
initial aggression in 2014. While the United States has   
photo: beata zawrzel/nurphoto/getty images

**Page 125**

119  
Seamus P. Daniels  
appropriated additional resources to backfill equip­  
ment stocks sent as assistance to Ukraine, it has also   
imposed budgetary limits on its own defense funds,   
highlighting the impact of fiscal and political consid­  
erations on defense spending.  
In response to Russia’s 2014 annexation of   
Crimea, NATO allies at the Wales Summit later that   
year agreed to a benchmark to increase their defense   
spending and military capabilities to counter the Rus­  
sian threat. NATO allies agreed to aim to spend the   
equivalent of 2 percent of each state’s GDP on defense   
and 20 percent of defense budgets on equipment.2  
However, total defense spending by the alliance   
increased only incrementally following the decla­  
ration of that agreement. Between 2014 and 2022,   
NATO’s total defense spending, as reported by the   
alliance, increased 12 percent in real terms at a com­  
pound annual growth rate of 1.3 percent.3 Notably,   
as Figure 13.1 shows, spending by European allies   
and Canada (excluding the United States) grew by 34   
percent, adjusted for inflation, over that nine-year   
period, a 3.3 percent growth rate each year. The   
number of allies meeting the 2 percent of GDP bench­  
mark rose from 3 out of 27 NATO members in 2014 to   
7 out of 29 in 2022 (members meeting the threshold   
peaked at 9 in 2020, but this was a product of declin­  
ing GDP from the Covid-19 crisis).4  
Russia’s official invasion of Ukraine in 2022   
prompted a more immediate reaction from NATO   
members in terms of spending, as governments per­  
ceived a more tangible threat to their borders. Total   
defense spending is estimated to increase 22 percent   
in real terms between 2022 and 2025. That includes   
an estimated 50 percent increase in spending by   
European members and Canada.   
In the wake of Russia’s invasion, several allies   
announced notable shifts in their defense policy   
or spending plans. Just days after the war began,   
then-Chancellor Olaf Scholz announced a Zeiten­  
wende, or “historical turning point,” in German   
foreign and defense policy to rethink relations with   
Russia and called for a €100 billion fund to invest in   
the military.5 While implementation of the policy has   
been described as “lackluster” and others have ques­  
tioned whether the fund was sufficient to transform   
the military, the focus on bolstering national secu­  
Figure 13.1: NATO Reported Defense Spending  
United States  
NATO Europe & Canada  
Total  
Defense Spending per NATO Deﬁnition (in 2021 U.S. dollars)  
$0B  
$200B  
$400B  
$600B  
$800B  
$1,000B  
$1,200B  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
$1,400B  
Note: 2024 and 2025 based on estimated data.  
Source: “Defence Expenditure of NATO Countries (2014-2025),” NATO, August 28, 2025, https://www.nato.int/cps/en/natohq/  
news\_237171.htm.

**Page 126**

120  
Defense Budgets in an Uncertain Security Environment  
both increased their defense spending by over $18 bil­  
lion, followed by Spain with a boost of nearly $16 bil­  
lion. The Netherlands and Italy both increased their   
spending by over $12 billion each.  
The boost in NATO defense spending following   
Russia’s 2022 invasion also led to a significant increase   
in the number of member states meeting the 2 per­  
cent of GDP benchmark, as shown in Figure 13.3. In   
2023, 10 members met the threshold—up from 7 in   
2022—while notably all 31 NATO allies are expected to   
reach the benchmark in 2025. According to the 2025   
estimates, Poland is estimated to have spent the great­  
est percentage of its GDP on defense of all member   
states, at 4.5 percent, followed by Lithuania (4.0 per­  
cent), Latvia (3.7 percent), and Estonia (3.4 percent).   
Luxembourg, Spain, North Macedonia, and Czechia   
are estimated to spend the smallest percentage of   
their GDP on defense.  
Despite these increases, the United States under   
the second Trump administration has pushed for   
greater burden sharing among NATO allies and an   
increased spending threshold. President Trump first   
called for a 5 percent of GDP benchmark prior to   
taking office and has continued to make that demand   
in office.14 NATO Secretary General Mark Rutte pro­  
posed a plan for allies to eventually match that target,   
calling for an increase to 3.5 percent of GDP spend­  
ing on classic defense activities with an additional   
1.5 percent of spending on other security-related   
investments.15 NATO heads of state agreed to the new   
threshold at the Hague Summit in June 2025, with   
the goal of meeting the 5 percent level by 2035 and   
a requirement to submit annual plans of how each   
state would reach it (differentiating it from the Wales   
Summit’s 2 percent plan).16   
While topline defense spending measured as a   
percentage of GDP represents one metric for assess­  
ing burden sharing in the alliance, the second bench­  
mark agreed to at the Wales Summit—percentage of   
defense expenditure allocated toward equipment—  
provides a measure of the capabilities in which states   
are investing. The Wales Summit agreement called on   
NATO members to allocate 20 percent of their defense   
budgets toward procuring major equipment, as well   
as conducting research and development.17 The NATO   
rity has continued in Germany.6 In March 2025, the   
Bundestag voted to exempt defense spending from   
its strict constitutional debt limit, and in May that   
year, then-Chancellor-elect Friedrich Merz promised   
to transform the German military into the “strongest   
conventional army in Europe.”7  
Poland dramatically boosted its spending as it   
undertook a military modernization initiative to   
upgrade its capabilities.8 The increase was funded by   
growth within the budget as well as an extra-budget­  
ary mechanism known as the Armed Forces Support   
Fund, established in 2022, with the main funding   
derived from issuing bonds.9 Prime Minister Keir   
Starmer also announced in February 2025 that the   
United Kingdom would spend 2.5 percent of GDP on   
defense by April 2027 in what he touted as the “big­  
gest sustained increase in defence spending since the   
end of the Cold War.”10  
The European Commission has additionally taken   
measures that will allow EU members to increase   
defense spending during what Commission Presi­  
dent Ursula von der Leyen described as the “most   
momentous and dangerous of times.”11 Under the   
ReArm Europe Plan/Readiness 2030 announced in   
March 2025, EU member states have greater flexibility   
to increase their defense spending against the Euro­  
pean Union’s strict debt limitations in light of Rus­  
sia’s invasion of Ukraine. The European Commission   
also established a new financial mechanism called   
the Security Action for Europe (SAFE), which allows   
member states to access loans for defense spending   
from a €150 billion fund.12 Finally, the plan seeks to   
increase investments from the European Investment   
Bank for defense projects and mobilize private capi­  
tal.13 Taken together, these different measures could   
provide up to an additional €800 billion in defense   
funding, according to the European Commission.  
Figure 13.2 shows the estimated change in   
defense spending by European NATO members and   
Canada from 2022 to 2025 in constant 2021 dollars.   
NATO allies, with the exception of Greece, increased   
spending over that period. While the NATO data did   
not provide a 2025 estimate for German spending,   
Germany’s defense spending increased by over $23   
billion between 2022 and 2024. Canada and Poland

**Page 127**

121  
Seamus P. Daniels  
cent in 2014, rising to 27 percent in 2023, and an esti­  
mated 33 percent in 2025.   
While Russia’s invasion of Ukraine and the height­  
ened threat environment have directly contributed   
to European NATO members increased defense   
budgets, trends in U.S. defense spending have also   
been shaped significantly by broader political and   
economic developments. Figure 13.5 shows U.S.   
national defense spending from FY 2014 through FY   
2025. While funding did peak in FY 2024 based on   
data tracks spending in three additional categories,   
including personnel expenses, infrastructure, and   
other. However, spending on equipment provides   
added capabilities and warfighting potential for the   
alliance collectively as opposed to spending on the   
military personnel of individual states.  
As Figure 13.4 shows, the average percentage of   
defense spending NATO members allocate to equip­  
ment has risen steadily since 2014 relative to other   
investment areas. States allocated on average 13 per­  
Figure 13.2: Real Change in Defense Spending, 2022–2025  
(in 2021 U.S. dollars)  
$-5B  
$0B  
$5B  
$10B  
$15B  
$20B  
$25B  
Greece  
Montenegro  
North Macedonia  
Albania  
Croatia  
Estonia  
Slovak Republic  
Hungary  
Slovenia  
Bulgaria  
Latvia  
Luxembourg  
Lithuania  
Romania  
Portugal  
Czechia  
Finland  
Belgium  
United Kingdom  
Sweden  
France  
Denmark  
Norway  
Türkiye  
Italy  
Netherlands  
Spain  
Poland  
Canada  
Germany\*  
\*Germany data shows 2022-2024 real change as no 2025 data reported.   
Source: “Defence Expenditure of NATO Countries (2014-2025),” NATO, August 28, 2025, https://www.nato.int/cps/en/natohq/  
news\_237171.htm.

**Page 128**

122  
Defense Budgets in an Uncertain Security Environment  
of 2011 to limit federal deficits and the national debt.   
However, a series of budget deals passed over that   
time increased funding levels above the original man­  
dated caps.18 Congress similarly imposed the Fiscal   
Responsibility Act of 2023 to cap spending levels in   
FY 2024 and FY 2025.19 Yet military aid to Ukraine   
the provision of military aid to Ukraine and the subse­  
quent replacement of U.S. stocks, yearly fluctuations   
in spending levels are consistently shaped by fiscal   
limitations imposed by Congress. From FY 2012 to   
FY 2021, the Department of Defense (DOD) operated   
under budget caps imposed by the Budget Control Act   
Figure 13.3: NATO Members' Percentage of GDP Spent on Defense  
2014  
2022  
2024\*  
2025\*  
0%  
0.5%  
1%  
1.5%  
2%  
2.5%  
3%  
3.5%  
4%  
4.5%  
5%  
Luxembourg  
Spain  
North Macedonia  
Czechia  
Belgium  
Portugal  
Italy  
Canada  
Albania  
Slovenia  
Montenegro  
Croatia  
Slovak Republic  
France  
Hungary  
Bulgaria  
Romania  
Türkiye  
United Kingdom  
Netherlands  
Germany\*  
Sweden  
Finland  
Greece  
Denmark  
United States  
Norway  
Estonia  
Latvia  
Lithuania  
Poland  
\*No 2025 data reported for Germany.   
Note: 2024 and 2025 based on estimated data.  
Source: “Defence Expenditure of NATO Countries (2014-2025),” NATO, August 28, 2025, https://www.nato.int/cps/en/natohq/  
news\_237171.htm.

**Page 129**

123  
Seamus P. Daniels  
spending, to the dismay of congressional defense   
hawks who criticized the White House and DOD for   
its budget request and apparent misuse of the rec­  
onciliation funds.21 Moreover, cuts and rescissions   
to non-defense funding pursued by the White House   
and congressional Republicans could make Dem­  
ocrats reluctant to grow defense spending without   
guarantees over non-defense priorities.  
Growth in Russian and   
Chinese Defense Spending  
Russian and Chinese defense spending has also   
increased since the outbreak of the 2022 war. Russia’s   
spending, unsurprisingly, has been driven by the cost   
of conducting operations in Ukraine and reconstitut­  
ing its military capabilities. China’s defense budget   
marks a continuation of its strategic priority to mod­  
ernize its military forces.  
Analysis of Russia’s and China’s defense spend­  
ing, the United States’ principal competitors, is con­  
strained by a lack of both available data and limited   
transparency in the data that is released by each   
government. Both states’ official defense budgets   
do not appear to be inclusive of all military-related   
funding. However, the limited data available clearly   
and other supplemental funds did not apply to the   
spending under the cap level.   
Fiscal concerns, however, may be overcome   
by political prerogatives. In July 2025, congressio­  
nal Republicans passed reconciliation legislation to   
extend and expand tax cuts, increase defense and   
border security funding, slash non-defense spend­  
ing priorities, and raise the debt ceiling. These mea­  
sures, enacted reluctantly by budget hawks within the   
Republican party, is estimated to increase the federal   
deficit by $4.1 trillion between 2025 and 2034.20 The   
legislation included $156 billion to provide a one-time   
supplemental boost in funding intended by Congress   
to enhance U.S. military capabilities between FY 2025   
and FY 2029.  
Yet fiscal concerns persist which, coupled with   
political divisions, may limit further growth in U.S.   
defense spending. In its FY 2026 defense budget   
request, the Trump administration touted the first-  
ever trillion-dollar defense budget. However, the   
administration only requested $892.6 billion in dis­  
cretionary funding from Congress, proposing to use   
$119 billion from the reconciliation funding in FY   
2026. This could signal that the administration does   
not intend to pursue further increases in defense   
Figure 13.4: Average Percentage of NATO Members' Defense Spending by Category  
0%  
20%  
40%  
60%  
80%  
100%  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024\*  
2025\*  
Equipment  
Personnel  
Infrastructure  
Other  
Note: 2024 and 2025 based on estimated data.  
Source: Defence Expenditure of NATO Countries (2014-2025),” NATO, August 28, 2025, https://www.nato.int/cps/en/natohq/  
news\_237171.htm.

**Page 130**

124  
Defense Budgets in an Uncertain Security Environment  
fell significantly—by almost 19 percent in real terms—  
from 2016 to 2017 and largely stayed flat for the next   
several years. However, the war in Ukraine led Russia   
to increase its defense expenditures dramatically above   
inflation. Spending is estimated to have increased by   
69 percent in real terms between 2021 and 2024, with   
annual increases of approximately 29 percent (2021–  
2022), 23 percent (2022–2023), and 38 percent (2023–  
2024). One alternative estimate of Russia’s defense   
spending calculated a 53 percent increase in total mili­  
indicates that Russian and Chinese defense spending   
is increasing in parallel with NATO budgets: Russia   
as a direct result of its invasion and continued war in   
Ukraine, and China through its consistent and sus­  
tained approach to modernizing its military.  
Russian defense spending has unsurprisingly   
increased dramatically year-on-year from its invasion   
of Ukraine. Figure 13.6 shows Russian spending from   
2014 to 2024 as estimated by the Stockholm Interna­  
tional Peace Research Institute (SIPRI).22 Defense funds   
Figure 13.5: U.S. Defense Spending, FY 2014–FY 2025  
U.S. National Defense Budget Authority in FY 2025 Dollars (includes discretionary and supplemental)  
$750B  
$800B  
$850B  
$900B  
$950B  
$1,000B  
FY 2014  
FY 2016  
FY 2018  
FY 2020  
FY 2022  
FY 2024  
Source: Author’s analysis of “Fiscal Year 2025 Public Budget Database,” Office of Management and Budget, March 11, 2024, https://  
www.govinfo.gov/app/collection/budget/2025/BUDGET-2025-DB.  
Figure 13.6: Russian Defense Spending, 2014–2024  
$60B  
$80B  
$100B  
$120B  
$140B  
$160B  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
In Constant 2023 U.S. Dollars  
Source: “SIPRI Military Expenditure Database, 1949-2024,” Stockholm International Peace Research Institute, https://www.sipri.org/  
databases/milex.

**Page 131**

125  
Seamus P. Daniels  
ing the makeup of spending, as official estimates are   
understood to routinely report lower levels of funding.   
Consequently, estimates of China’s topline spending   
vary considerably, ranging from the government-re­  
ported $245 billion level announced in March 2025 to   
an estimated $700 billion from some analysts.28 Figure   
13.7 shows China’s reported defense budget in current   
RMB and the announced annual growth rate. While   
the announced growth rate fell dramatically from a   
2014 peak to 2017, it has remained steadily consistent   
over the last several years, despite the Chinese econ­  
omy facing significant fiscal headwinds.29  
Estimates of actual Chinese defense spending also   
demonstrate sustained growth over time. Data from   
SIPRI, shown in Figure 13.8, depicts steady growth in   
military expenditures adjusted for inflation. Accord­  
ing to SIPRI, Chinese defense spending grew over 70   
percent in real terms between 2014 and 2024, or at   
a compound annual growth rate of 5 percent. That   
tary-related expenditures from 2023 to 2024, adjusting   
for inflation.23 The Russian defense budget is expected   
to grow again in 2025, although at a more meager 3.4   
percent, according to the latter estimate.24   
Analyzing Russia’s defense spending is further   
challenged by the declining levels of transparency   
since its 2022 invasion of Ukraine, with 30 percent of   
the 2024 budget designated as classified in 2024 and   
budget changes that made it difficult to estimate actual   
spending over the year.25 Nevertheless, Russia spent a   
significant amount of its 2024 funding on procuring   
new weapons systems for the war in Ukraine, support­  
ing its defense industry, and covering military person­  
nel costs, according to the Stockholm International   
Peace Research.26 Another source notes that Russia   
has doubled its armored vehicle output and dramat­  
ically increased munitions production since 2022.27  
Analyses of China’s defense budget suffer from an   
even larger dearth of reliable source material regard­  
Figure 13.7: China's Reported Defense Budget and Announced Growth Rate  
2025  
2024  
2023  
2022  
2021  
2020  
2019  
2018  
2017  
2016  
2015  
2014  
2013  
0  
1000  
800  
600  
400  
200  
1800  
1600  
1400  
1200  
Billions of RMB  
0%  
10%  
8%  
6%  
4%  
2%  
14%  
12%  
Growth Rate (%)  
Announced budget  
Announced growth rate  
Note: Take from: https://chinapower.csis.org/military-spending/.  
Source: “What Does China Really Spend on its Military?,” CSIS, ChinaPower, updated March 5, 2025, https://chinapower.csis.org/  
military-spending/.

**Page 132**

126  
Defense Budgets in an Uncertain Security Environment  
that the threat on their borders has significantly less­  
ened, which seems unlikely should Russia continue   
to reconstitute and rebuild its military after the war.  
Yet, questions remain as to whether Russia can   
sustain its current defense spending levels. The lower   
growth rate in its 2025 budget and potential decreases   
in real terms for 2026 and 2027 suggest a decline   
could be on the horizon.30 At an economic forum in   
June 2025, the Russian economy minister suggested   
that the country was headed toward a recession, with   
some commentators suggesting defense cuts could   
be on the line.31 However, other analysts suggest that   
Putin’s will to modernize and empower the country’s   
military will take priority over preventing an eco­  
nomic downturn.32  
While a change in the threat landscape could shift   
European defense spending trends, economic trends   
could have an impact as well. European states also   
face fiscal challenges which could hinder their ability   
to meet the new NATO spending threshold and their   
willingness to allocate more resources to defense at   
the expense of other priorities.33 An economic down­  
turn could force states to limit defense spending   
growth and allocate a greater percentage of funding   
toward non-defense priorities.  
Barring a major change in the security environ­  
ment that directly affects the United States or its allies   
or partners, political and fiscal realities will continue   
growth has funded an impressive military moderniza­  
tion campaign to produce advanced capabilities and   
platforms across a range of domains as well as various   
reform initiatives.  
Conclusion: Prospects for   
Continued Defense Spending   
Growth  
The deteriorating global security environment and   
ongoing war in Ukraine have contributed to significant   
increases in defense spending across the world. The   
growth in NATO members’ budgets demonstrates the   
clear impact of the threat landscape on defense spend­  
ing decisions. The dramatic growth in Russian military   
expenditures shows the costs required to maintain   
complex military operations at scale. However, as   
the case of the United States demonstrates, fiscal and   
political factors also determine defense funding.  
Changes in the threat environment will shape   
global defense spending levels in the near future   
as states weigh how to allocate resources between   
defense and other spending and political priorities.   
While a resolution to the war in Ukraine has the   
potential to slow spending growth from European   
states and Russia, the cessation of combat operations   
alone will not guarantee a moderation of defense   
spending levels. European states, particularly those   
in the Baltics and Eastern Europe, must also perceive   
Figure 13.8: Chinese Defense Spending, 2014–2024  
$150B  
$200B  
$250B  
$300B  
$350B  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
In Contstant 2023 U.S. Dollars  
Source: “SIPRI Military Expenditure Database, 1949-2024,” Stockholm International Peace Research Institute, https://www.sipri.org/  
databases/milex.

**Page 133**

127  
Seamus P. Daniels  
additional growth, further escalation of conflicts   
globally could nevertheless lead to even greater   
spending levels.  
to have a major impact on U.S. defense spending   
levels in the near future. Historically, the federal defi­  
cit has been a driver in the most recent downturns   
in U.S. defense spending in the late 1980s and early   
2010s.34 Moreover, slim Republican majorities in   
both chambers of Congress necessitate Democratic   
support for passing additional increases in regular   
defense appropriations, which may be unlikely given   
the current partisan divide on spending. However, as   
the United States’ reaction to Russia’s 2022 invasion   
demonstrated—in which it rapidly distributed aid to   
Ukraine, increased its military posture in Europe, and   
passed supplemental funding to backfill equipment   
stocks—a sudden threat to the homeland, U.S. allies   
and partners, or U.S. interests could push the govern­  
ment to take immediate action.  
Fiscal headwinds are less likely to slow Chi­  
na’s consistent and sustained spending growth as   
it continues its ambitious military modernization   
program. However, as the PLA develops, procures,   
and fields more exquisite and advanced weapons   
systems in its force structure, it will be forced to   
spend additional funds to operate and sustain those   
platforms. Absent continued increases in defense   
spending over time, operation and sustainment as   
well as personnel costs may consume a larger por­  
tion of China’s defense budget.  
International defense spending levels have   
grown dramatically in light of increasing conflicts   
and the deteriorating global security environment.   
While economic and fiscal realities may challenge   
Barring a major change in the   
security environment that directly   
affects the United States or its   
allies or partners, political and   
fiscal realities will continue to have   
a major impact on U.S. defense   
spending levels in the near future.

**Page 134**

Cynthia R. Cook  
CHAPTER 14  
Industrial Roadblocks  
Producing at Scale and   
Adopting New Technologies

**Page 135**

129  
Cynthia R. Cook  
”  
“  
R  
ussia’s full-scale invasion of Ukraine in   
February 2022 was the starting point for a   
long-overdue refocus on defense industrial   
base issues. The United States led the allied effort   
to supply Ukraine with systems and weapons that it   
could use for self-defense against Russian aggression.   
Within the first year of the war, this support illumi­  
nated worrisome vulnerabilities in the U.S. and Eu­  
ropean defense industrial bases, especially in terms   
of preparedness for sustained conflict generally and   
in munitions production specifically.1 Russia similar­  
ly began the fight without understanding the likely   
strains on its industrial base and the need to ensure   
adequate stockpiles and production capacity. Along   
with limitations on defense production, the war has   
revealed constraints throughout the supply chain and   
in the production workforce. It has also demonstrat­  
ed the benefits of working with allies and partners,   
which has sustained both Ukraine and Russia during   
the long conflict. The risks of potential adversaries   
controlling key supply chain inputs, including Chi­  
na’s dominance of critical minerals processing, have   
become clearer. And the speed with which both sides   
have incorporated innovation in what they bring to   
the fight suggests that the industrial base, along with   
the government bureaucracies that set and fund   
requirements, must be agile enough to ensure that   
equipment delivered to the battlefield incorporates   
updated technology that refreshes at the rate of weeks   
or days, not years.  
A clear lesson has emerged: Defense industrial   
readiness needs to be in sync with the possibility of   
high-intensity, prolonged conflict in which there is   
rapid technical refresh.2 The industrial base needs   
to be robust, resilient, and ready to surge, especially   
given the risk of lengthy conflicts. There is a renewed   
understanding that “production is deterrence.”3   
Thus, investments in production and in surge capa­  
bility and capacity throughout the supply chain,   
especially for munitions, will be necessary to sup­  
port future war. The challenge of surging production   
means that nations must be willing to produce for   
stockpiles in times of peace to have the capabilities   
A rethink of industrial posture is necessary—  
not just to ensure peacetime readiness but   
to be able to sustain and surge to support   
combat operations against a near-peer   
adversary in the case of protracted war.  
photo: jean-francois monier/afp/getty images

**Page 136**

130  
Industrial Roadblocks  
they need ready in case of conflict. Equally important   
is working with allies and partners to build a more   
integrated and resilient industrial base through   
coproduction, shared stockpiles, and coordinated   
supply chains. A rethink of industrial posture is nec­  
essary—not just to ensure peacetime readiness but   
to be able to sustain and surge to support combat   
operations against a near-peer adversary in the case   
of protracted war. This posture needs to include con­  
siderations of the possibility of economic warfare,   
whereby potential adversaries control the produc­  
tion of and withhold inputs to necessary-to-manu­  
facturing defense components.  
Future war will require the industrial base to be   
responsive to the unprecedented, persistent inno­  
vation loop of technology on the battlefield. Russia’s   
war in Ukraine has showcased a level of technologi­  
cal integration whereby lessons from the front lines   
are shaping what is produced within days or weeks.   
The war has demonstrated the efficacy of dual-use   
technologies, such as drones that are widely avail­  
able on the commercial market and simple enough   
to build in small factories; an increased use of elec­  
tronic warfare, requiring the continual evolution of   
system technologies; and an increased availability   
of intelligence, surveillance, and reconnaissance   
(ISR) technologies (both drone- and space-based),   
removing the element of surprise. All of these factors   
will require updating acquisition approaches for any   
nation working to maintain its warfighting effective­  
ness. Slow and deliberate processes that prioritize   
cost efficiency will not deliver capabilities at the pace   
of warfighting necessity.  
Lessons from Current Wars   
The Importance of Production   
Russia’s war in Ukraine has resulted in staggering   
levels of materiel consumption. Both sides have   
burned through artillery shells, precision-guided   
munitions, drones, and other equipment at rates that   
dwarf peacetime forecasts. Similarly, Israel’s opera­  
tions in Gaza since late 2023 in response to Hamas’s   
October 7, 2023, attack have demonstrated the pace   
at which a modern military can expend munitions,   
even in a small geographic area, and risk depleting   
national munitions stocks.4   
The challenge of ensuring adequate stockpiles is   
also a significant finding from wargames, including   
those examining a potential conflict over Taiwan.   
In these simulations, forces often run out of critical   
munitions—particularly long-range precision weap­  
ons—within days.5 For the United States, demand   
in these scenarios often exceeds current industrial   
capacity, suggesting the need for a significant reimag­  
ining of stockpiles and surge capabilities. Analysis   
shows that rebuilding U.S. inventories for some sys­  
tems provided to Ukraine will take years.6 European   
industry has worked to build capacity, but it still faces   
supply constraints.7 Russia has invested in growing its   
industrial base to meet the demands of its war but has   
still benefited from imports of dual-use components.8   
Surging manufacturing is not merely a matter of   
sending orders to prime contractors, or of increas­  
ing orders at government owned factories. Entire   
defense supply chains need to be ready to expand   
production.9 Supply chain complexity muddles this   
effort, since prime contractors may not even know   
who supplies components at the lowest level of   
supply chains, with the additional risk that adversar­  
ies may control production of necessary inputs, such   
as critical minerals.10 The defense industrial bases of   
most major powers are not incentivized for resilience   
during peacetime and will face challenges surging   
during wartime, especially during initial phases. Mar­  
ket-based defense industries prioritize efficiency and   
profit, rather than excess capacity, which increases   
costs. Nations with centralized planning—like China   
and North Korea—are the most able to direct sus­  
tained defense production in peacetime.   
China’s industrial policy has supported its devel­  
opment into the world’s manufacturing powerhouse,   
with as much as 50 percent of its manufacturing poten­  
tially dual-use.11 It has invested heavily in its defense   
industrial base, including in munitions and shipbuild­  
ing, with some analysts assessing that the nation’s   
defense industrial base is on a “wartime footing.”12   
China also dominates in a number of necessary   
sub-tier parts of the supply chain, including critical

**Page 137**

131  
Cynthia R. Cook  
Most of the rest of the world has similarly underin­  
vested in production capacity over time. One analysis   
found that “the uncomfortable truth emerging from   
the ongoing war on European soil is that European   
countries have barely prepared for war at all. Russia’s   
war of aggression against Ukraine has revealed signif­  
icant shortcomings in the capacity of European NATO   
governments to supply and arm a neighbouring part­  
ner, much less fight a major war themselves.”19 Many   
European nations focused on social spending instead   
of investing in their national defenses at the NATO   
target of 2 percent developed in 2014, and only after   
Russia began its attack on Ukraine did the number of   
nations at that target increase from 6 in 2021 to 23 in   
2024.20 The European Union issued a defense indus­  
trial strategy in March 2024, with the goal of enhanc­  
ing defense industrial capacity by 2024, hoping to   
address challenges of “fragmentation and limited   
collaboration, exacerbated by EU Member States’   
dependency on non-EU defence equipment.”21   
The Australian government’s relatively small   
requirement has meant that maintaining consistent   
production over time has been difficult.22 It released   
a Defence Industry Development Strategy in 2024 to   
address long-standing production challenges.23 Until   
recently, Japan banned defense exports, which limited   
industry to Japan’s small defense market and made   
the country less well-postured to surge.24 In contrast,   
South Korea’s defense industry grown over time,   
with investments spurred by the proximity of nucle­  
ar-armed North Korea and enhanced by strong gov­  
ernment partnerships with industry.25 South Korea’s   
strong industrial base has postured the country to win   
contracts with new customers, such as Poland.26  
One nation has followed a dramatically differ­  
ent approach. Over the last decade, China has visi­  
bly expanded its defense industrial base and made   
investments in capabilities, such as shipbuilding,   
that have dual-use potential.27 Chinese production of   
key platforms and munitions now far outpaces that   
of the United States, reinforcing that planning for a   
short war is a gamble unless the U.S. industrial base   
is transformed.28   
Not all the industrial base lessons from Russia’s   
war in Ukraine are stories of persistent challenges   
minerals processing, which raises the question of   
supply chain security. Industrial readiness requires   
attention to a production ecosystem that includes   
both systems integrators and suppliers. Component,   
subcomponent, and material suppliers face the same   
challenges of expanding manufacturing as prime con­  
tractors, including workforce and facility constraints.   
Complex supply chains may have 10 levels or more,   
so it may be difficult to assess risks, including risks   
posed by single-source suppliers or dependencies   
on unreliable international sources.13 Investments in   
readiness must apply to the entire supply chain, and a   
consistent focus on supply chain illumination to iden­  
tify and remediate sources of risk needs to be part of   
an industrial base strategy.  
The Need to Overcome Inertia   
and Invest Consistently   
The importance of the defense industrial base is   
not a new concept, but many nations have under­  
invested in capability and capacity. Even before the   
end of the Cold War, one analyst offered that “the   
US defense industry in 1988 bears little resemblance   
to the ‘Arsenal of Democracy’ that turned out tanks   
and airplanes in legendary numbers during World   
War II. American industry today cannot meet surge   
or wartime mobilization needs. It even has difficulty   
with peacetime defense requirements.”14 The rea­  
sons stated then remain familiar today—increased   
outsourcing, workforce challenges, and smaller   
defense budgets.   
Recent U.S. administrations have highlighted   
industrial base and supply chain risks. The 2010 Qua­  
drennial DefenseReview included a call to revitalize   
the defense industrial base.15 During the first Trump   
administration, Executive Order 13806 called for an   
assessment on how to strengthen the defense indus­  
trial base, which was published in 2018.16 Even before   
Russia’s invasion of Ukraine, the Biden administration   
published a report on the security of defense-criti­  
cal supply chains, highlighting limitations in kinetic   
capabilities, among other inputs.17 Repeated warnings   
about defense industrial base challenges have yielded   
some action, including the development of the first   
ever National Defense Industrial Strategy in 2023.18

**Page 138**

132  
Industrial Roadblocks  
of military drones.34 Iran has also supplied Russia   
with short-range ballistic missiles.35 North Korea   
has provided millions of rounds of ammunition, at   
least 100 ballistic missiles, and “elements of three   
brigade sets of heavy artillery, including DPRK-ori­  
gin 170mm long range self-propelled artillery pieces,   
240mm long-range multiple rocket launchers, more   
than 200 total vehicles, self-propelled guns, multiple   
rocket launchers, and reload vehicles for both types   
of weapons,” according to an multilateral monitoring   
body.36 In return for this support, Russia has provided   
its more advanced military technologies to its part­  
ners.37 Along with insight into how their equipment   
performed on the battlefield, China may get advanced   
equipment and technology, including relating to aero­  
space; Iran is getting a range of equipment, including   
helicopters, radars, and fighter aircraft; and North   
Korea is accessing information on missiles and satel­  
lite technology.38  
The Role of Innovation  
Russia’s war in Ukraine has showcased a level of   
technological integration that marks a step change   
in modern warfare, with implications for the indus­  
trial base. Ukraine has pioneered a variety of inno­  
vations in what has been termed “the first full-scale   
drone war.”39 Even early in the war it was clear that   
“Ukraine’s widespread and successful use of newer   
systems [was] placing emerging tech into the mili­  
tary mainstream.”40 Ensuring that warfighters have   
capabilities that are keeping pace with the evolution   
of adversary systems requires an approach to acqui­  
sition that is fast, flexible, technically informed, and   
able to work with a range of defense contractors—  
from traditional primes focused on systems integra­  
tion to cutting-edge innovation providers. Ukraine’s   
distributed model of technology development has   
allowed for the emergence of new ideas from the pri­  
vate sector, with battlefield demands driving inno­  
vation, but has also made these innovations harder   
to scale.41 Russia has responded with investments in   
its own innovation ecosystem, with recent analysis   
suggesting that a more centralized planning and pro­  
duction approach has enabled it to outpace Ukraine   
in its ability to develop, scale production of, and field   
and unaddressed gaps. One takeaway is that conflict   
generates the urgency for putting an industrial base   
on a wartime footing. Russia has pivoted its econ­  
omy toward the production of weapons, and while   
its industrial base has been assessed as a continuing   
weakness, one recent analysis suggests that Russia’s   
economy has been resilient.29 Ukraine has vastly   
expanded its network of factories, drawing on the   
labor of women of all ages, along with some men who   
are able to work in defense factories rather than serv­  
ing on the front lines.  
Allies and Partners   
as Force Multipliers  
Even beyond offering second sources of supply and   
the potential for surge capacity, current conflicts have   
highlighted the importance of allies and partners. In   
Russia’s war in Ukraine, both sides have relied on   
material and technical know-how provided by other   
nations. Materiel provided by allies and partners   
sustained Ukraine in the early part of the war even   
more than its own industrial base, which had been   
underinvested in before the invasion.30 A Ukrainian   
economic nongovernmental organization reported   
that $118 billion of aid has come from abroad, with the   
United States and EU nations being the most import­  
ant sources.31 The United States and NATO allies have   
a wide range of offensive and defensive systems,   
including ammunition, artillery, bombs and rockets,   
air defense systems, ground vehicles, drones and air­  
craft (including F-16s), and a range of other systems.32   
Russia has also benefited from being able to access   
the industrial bases of other nations, following a more   
transactional approach. China, Iran, and North Korea   
have made components, capabilities, and other forms   
of support available to Russia, which has strength­  
ened its supply chain and its ability to sustain its war   
against Ukraine. A statement from U.S. Indo-Pacific   
Command in the spring of 2025 suggests that China   
has provided 70 percent of the machine tools and 90   
percent of the legacy chips that Russia needed to reset   
its industrial base and ramp up production.33 Iran   
initially supplied Russia with drones and then later   
provided Russia the technical and production knowl­  
edge necessary to expand its indigenous production

**Page 139**

133  
Cynthia R. Cook  
tion.48 This aligns with other analysis, including from   
wargames, which suggests that technological evo­  
lution puts a wider variety of systems at risk.49 The   
challenge going forward will be using these lessons   
to reshape larger acquisition programs, which have   
constituencies with other objectives including main­  
taining industrial production at current facilities and   
ensuring local employment levels. While these may   
be worthy goals, there needs to be balance to ensure   
that resources are available to invest in new types of   
systems with greater battlefield effectiveness.  
Conclusion  
Russia’s war in Ukraine has lasted three-and-a-half   
years as of this writing. It has become a grinding con­  
flict featuring the heavy expenditure of munitions   
and the adoption of new technology, including the   
increased use of drones. The defense industrial bases   
of both nations have been dramatically reshaped,   
moving to a wartime footing and incorporating more   
rapid innovation. Both nations have also relied on   
partners and allies for the provision of munitions and   
other capabilities as well as for supply chain inputs.   
Neither nation’s industrial base was prepared for   
protracted war, and support for Ukraine has strained   
allied production.   
In the Israel-Hamas conflict, Israel has much   
more robust military capabilities and has dominated   
the battlefield, but it has relied on its ally the United   
States for munitions, missiles, and other systems   
being used in the protracted fight.  
These conflicts, along with recent wargames,   
have highlighted concerns about the availability of   
capabilities necessary to stay in the fight in the case of   
protracted war. Even in times of peace, nations must   
focus on the industrial base to ensure they have the   
capabilities and capacity when needed in the case   
of a long conflict. This includes paying attention to   
risks in the entire supply chain, including by contin­  
ually investing in supply chain visibility to look for   
constraints and for chokeholds potential adversar­  
ies may have on the production of necessary inputs.   
A robust defense industrial base is expensive and   
must be defended even in times of peace in order   
to be ready in times of war. Working with allies and   
new systems.42 The ability to nimbly incorporate tech­  
nology evolution is important, but it does not out­  
weigh the ability to produce systems in the quantities   
needed for industrial war.   
The ability to nimbly incorporate   
technology evolution is important,   
but it does not outweigh the ability   
to produce systems in the quantities   
needed for industrial war.   
Drones offer a useful case study on the role inno­  
vation has played. Ukrainian forces have used drones   
for ISR and strike, with some analysis suggesting that   
over the first three years of the war, drone attacks   
were responsible for 70 percent of Russian casualties   
and 90 percent of equipment losses.43 These strikes   
were enabled by other capabilities, as Ukraine has   
taken commercially available drones and coupled   
them with electronic warfare and ISR systems. Over   
the course of the war, Ukraine has expanded its fac­  
tory network, and the production of drones has risen   
dramatically, reducing the nation’s import depen­  
dencies on commercially available drones.44 This   
has reduced Ukraine’s supply risk, given that China   
leads the world in commercial drone production and   
has also supported Russia in the war. Production in   
Ukraine has been decentralized, which has allowed   
for an increase in facilities and reduced risk from   
Russian precision attacks on defense factories.45   
Military units have maintained and repaired these   
systems on the front lines.46 This also brings an advan­  
tage because systems need to be updated rapidly to   
address changes in adversary capabilities, including   
in electronic warfare.   
The war has also cast some doubt on the util­  
ity—or at least the survivability—of expensive and   
exquisite weapons systems.47 The sinking of Russia’s   
Moskva cruiser by Ukrainian missiles early in the war   
offers a notable example of a strategy of cost imposi­

**Page 140**

134  
Industrial Roadblocks  
capabilities they need to win, or even to stay in the   
fight over the long term. The nations with the stronger   
industrial bases, with the more robust supply chains,   
and with the closer defense industrial ties with allies   
and partners will prevail, and those that do not delib­  
erately focus on these capabilities during peacetime   
will fail during war.  
partners is a strategy that strengthens ties and offers   
expanded production capacity while spreading the   
investment burden.   
These lessons are not new, and the risks of an   
inadequate defense industrial base have been high­  
lighted over the decades. In democratic nations with   
market economies, addressing industrial base chal­  
lenges will require considerable senior leadership   
support, funding, and efforts to identify and eliminate   
policies that limit flexibility. Nations with centralized   
planning—or ones that face ongoing threats, such as   
South Korea—are better able to support industrial   
base investment.  
Recent conflict, especially Russia’s war in   
Ukraine, has featured an increasingly rapid refresh   
of technology on the battlefield. More flexible   
acquisition approaches that partner operators with   
acquisition professionals will enable better access to   
innovation.50 Open-systems approaches that allow for   
the rapid refresh of subcomponents can offer advan­  
tages over large, “exquisite” systems that are more   
difficult to update.51 Rigid approaches where funders   
apply resources to specific programs limit the ability   
to move funds to new innovations as the need arises.   
During wartime, many of the more formalized acqui­  
sition regulations often are traded for the flexibility   
of “urgent operational needs,” but allowing and prac­  
ticing this flexibility in advance could create a more   
innovative defense sector, and one that is more rap­  
idly adaptable in case of conflict.  
As dramatically different as they are, Russia’s war   
in Ukraine and the Israel-Hamas conflict both show   
the likelihood of conflicts becoming protracted.   
Nations that are concerned about being pulled into   
combat must focus on strategies to ensure they have   
the weapons they need to compete on the battlefield.   
Munitions are a particularly important investment,   
yet one that has been harder to justify when nations   
are not drawing on stockpiles in their own defense   
or to support partners. Peacetime approaches to   
defense industrial production that prioritize manag­  
ing cost over ensuring capability will be insufficient to   
meet the needs of modern war. Planning and resourc­  
ing for conflict with the expectation that it will be over   
quickly creates the risk that nations will not have the

**Page 141**

Cynthia R. Cook  
CHAPTER 15  
Power Projection and the   
Logistics of Modern War

**Page 142**

136  
Power Projection and the Logistics of Modern War  
”  
“  
In future conflicts, robust logistics will   
continue to help win wars—and contested   
logistics will determine who can fight at all.  
W  
arfighting readiness and resilience have   
always been central to securing victory   
during conflict. Even as warfare evolves   
and the concepts, equipment, and supplies devel­  
op and change, there can be no success in warfare   
without the logistics enterprise. There is a persistent   
cliché that amateurs study strategy and experts talk   
logistics. A more exact formulation would be that   
experts understand the importance of logistics and   
readiness to their strategy, and plan and resource   
accordingly.   
There is increasing recognition of the possibility   
of protracted war requiring larger stockpiles of—or   
the ability to rapidly surge—a wide range of supplies.   
There are new challenges to power projection,   
including contested environments with persistent   
surveillance and adversaries with long-range, pre­  
cision-guided munitions. Resource challenges can   
lead to underinvestment in regular maintenance,   
limiting readiness. Whether nations are supporting   
an ally (e.g., the United States reinforcing Ukraine and   
Israel or China backing Russia) or are engaged directly   
in a major conflict, successfully addressing logistics   
challenges determines the feasibility and tempo of   
military operations.   
Technological change, including automation,   
advanced manufacturing, and AI, offers the potential   
to enhance planning and reduce logistical pressures.   
But these innovations cannot eliminate the funda­  
mental problem of sustaining high-intensity oper­  
ations across thousands of miles. Current conflicts   
show that nations continue to see the operational   
value in attacking each other’s logistics enterprises.   
Strong relationships with allies and partners allow for   
pre-positioning, industrial base support and mobi­  
lization, forward locations for sustainment, and   
enhanced transportation networks. In other words,   
these relationships are force multipliers.   
This chapter begins with a short overview of   
the components of the logistics enterprise to set   
the stage. It examines lessons from recent ongoing   
conflicts, including Russia’s war in Ukraine and the   
Israel-Gaza war, and evaluates their applicability to   
photo: john macdougall/afp/getty images

**Page 143**

137  
Cynthia R. Cook  
The Nature of the Power   
Projection Challenge  
Power projection is a function not only of capabilities,   
but also of context: Is the nation directly engaged, or is   
it supporting an ally? Is the theater permissive or con­  
tested? Is the objective short-term crisis response or   
sustained deterrence and warfighting? In almost every   
case, forward support is necessary. Transportation net­  
works must be defined and defended. Plans for weapon   
system maintenance and battle damage repair—pref­  
erably forward closer to the flight, to avoid the chal­  
lenge of contested logistics when sending equipment   
to be fixed—must be developed in advance, an effort   
which may include engaging with allies and partners   
and contracting with industry. Military logistics also   
encompasses the life-cycle management of necessary   
materiel; this includes requirements setting, acquisi­  
future war, drawing out readiness and sustainment   
implications. It concludes with recommendations   
for innovations specific to projecting and sustaining   
forces in a contested environment, with a focus on   
technological innovation, industrial cooperation, and   
allied partnerships.   
However, logistics enterprises by nature are   
very complicated and diverse, making a thorough   
review of lessons learned and insights for future war   
an impossible task. The literature on these conflicts   
is extensive. Even a subset of current experiences is   
enough to stress the imperative that operators and   
planners focusing on contested logistics ensure the   
enterprise is adequately resourced and available to   
support future plans. Assessing whether strategy   
leads logistics or logistics has the primacy over strat­  
egy is less important that taking the steps to invest in   
and ensure readiness.1   
Table 15.1: Class of Supply  
Class  
Description  
I  
Subsistence, including food and food-related supplies, including condiments, utensils, paper products and bottled   
water  
II  
Clothing, individual equipment, tentage, organizational tool kits, hand tools, and administrative and housekeeping   
supplies and equipment  
III  
Petroleum fuels, lubricants, hydraulic and insulating oils, preservatives, liquid and compressed gases, bulk chem­  
ical products, coolants, de-icing and antifreeze components, together with components and additives of such   
products, and coal  
IV  
Construction materials including installed equipment and all fortification or barrier materials  
V  
Ammunition, to include military munitions, of all types (including chemical, biological, radiological, and special   
weapons), bombs, explosives, mines, fuses, detonators, pyrotechnics, missiles, rockets, propellants, and other   
assorted items  
VI  
Personal demand items (non-military sales items)  
VII  
Major end items. A final combination of end products that is ready for its intended use (e.g., launchers, tanks, mo­  
bile machine shop, and vehicles)  
VIII  
Medical materiel, including medical-peculiar repair parts  
IX  
Repair parts and components, including kits, assemblies and subassemblies, and reparable and consumable   
items required for maintenance support of all equipment, excluding medical-peculiar repair parts  
X  
Materiel to support non-military programs, such as agricultural and economic development, not included in   
classes I through IX.  
Note: Taken directly from source. Bold formatting added.  
Source: Office of the Under Secretary of Defense for Acquisition and Sustainment, “DoD Supply Chain Management Procedures:   
Material Returns, Retention and Disposition,” DoD Manual 4140.01, vol. 6 (Washington, DC: U.S. Department of Defense, 2022), https://  
www.esd.whs.mil/Portals/54/Documents/DD/issuances/414001m/414001m\_vol06.PDF?ver=aF45YIqclvKJK3Z8Cu3GQw%3D%3D.

**Page 144**

138  
Power Projection and the Logistics of Modern War  
sight and management are critically important for the   
enterprise. Each of the aspects listed above requires   
different expertise, draws on different sources, and,   
above all, requires adequate resources, including   
funding. For example, the different U.S. military ser­  
vices have varying needs and individually engage in   
logistics planning and operations as they organize,   
train, and equip for the joint force, with additional   
joint organizations and concepts aimed at coordinat­  
ing support.2   
Joint concepts in the United States highlight the   
need for adequate resources, the ability to allocate   
those resources appropriately using information   
technology, the ability to manage and prioritize   
logistics capability, and the necessary transportation   
assets.3 These concepts call for a transportation net­  
work able to move people, equipment, and supplies   
to and within the theater, the capacity to pre-posi­  
tion supplies, and a worldwide network with multiple   
options.4 More realistically, the goal of speed is chal­  
lenged by the fact that movement frequently requires   
the use of large and relatively slow ships that transit   
through congested and vulnerable choke points.   
Lessons from Russia’s War in   
Ukraine and the Israel-Hamas   
Conflict  
Recent ongoing conflicts offer valuable insights into   
both logistics failures and successful adaptations.   
These lessons show that logistics must be tailored   
according to the nature of the conflict, with planning   
shaped by the realities of geographic and operational   
requirements.   
Russia-Ukraine  
Russia’s buildup on Ukraine’s border prior to its attack   
in February 2022 meant that the eventual invasion   
was not a surprise.5 The attack on Crimea eight years   
earlier created the opportunity and the will inside   
of Ukraine to invest in systems and the reforms that   
have contributed to its ability to sustain its self-de­  
fense over time, bolstered by allied support. Over the   
course of the current conflict, both sides have worked   
to expand sources of supply; maintain and repair   
equipment; move supplies, equipment and person­  
tion, distribution, maintenance, and disposition. Plan­  
ners must ensure warfighters and support personnel   
can make it to the conflict zone, where there needs to   
be adequate facilities, services, and medical support.   
Understanding the challenge of readiness begins   
with a recognition of the types of materiel necessary   
to support the fight. For reference, the United States   
military divides this into classes of supply, each of   
which has its own procurement challenges. Table   
15.1 lists the 10 classes of supply. Of particular note is   
Class V, or ammunition, which includes munitions of   
all types. The readiness enterprise thus overlaps with   
industrial base production considerations.  
This granular listing of the types of materiel   
needed in modern war is intended to ground the   
understanding of the logistics challenge. In any con­  
flict, the logistics enterprise must plan to acquire and   
deliver a very wide variety of materiel and equipment   
to the front lines.  
Along with the materiel necessary for the fight,   
the readiness challenge extends to maintenance,   
repair, and overhaul of existing systems. For any   
type of military capability, there are always trade-  
offs between the procurement of new equipment   
and the maintenance of existing equipment and   
production lines. Regulatory frameworks may limit   
where maintenance can occur, and who can do it.   
Forward-deployed assets need regular maintenance,   
and equipment that has suffered battle damage will   
need to be repaired. Ensuring adequate resources in a   
constrained environment—where funds too often pri­  
oritize new systems rather than sustaining the ones   
currently in the fleet—is an ongoing challenge.  
Logistics includes transportation to the point   
of need, which can vary from simple containeriza­  
tion for items such as clothing to complex handling   
requirements for munitions and medical supplies.   
Logistics also requires the transport of personnel.   
Transportation of equipment, supplies, and person­  
nel includes movement from the rear to the theater,   
and within the theater itself. Each of these layers has   
a different set of associated challenges.  
Finally, effective logistics includes a significant   
amount of planning and coordination. Capable over­

**Page 145**

139  
Cynthia R. Cook  
On the other side, U.S. and NATO support to   
Ukraine has been enabled by the proximity of allied   
territory and bases. Weapons and equipment have   
flowed overland from Poland and Romania, enabled   
by NATO’s secure rear area. Nonetheless, even this rel­  
atively favorable logistics environment has required   
planning, adaptation, and coordination. Moving   
munitions from the United States across the Atlan­  
tic to the European theater and within the theater is   
operationally complex. Ports have quantity limits for   
safety reasons, requiring careful pacing of deliveries,   
and transportation has to be smooth across vectors.13   
Allied support has not entirely made up for the fact   
that Ukraine is outmatched by Russia’s size and indus­  
trial capacity, and one of its responses has been to   
attack Russian infrastructure, including fuel storage   
facilities, munitions depots, and rail lines. These   
attacks have shown that constant pressure on supply   
chains can, in fact, help a smaller country compete   
with a bigger player’s industrial might.14   
To ensure the rapid flow of support, allies have   
provided Ukraine with existing rather than new sys­  
tems, with one benefit for the provider countries   
being the opportunity to update their own fleets and   
support their industrial bases.15 As a result, some of   
the drawdown equipment has needed to be repaired   
before it arrives in Ukraine, which has not always   
been completely carried out.16 Early in the conflict,   
Ukraine needed strategies to ensure repair and main­  
tenance of provided equipment, as well as to repair   
battle damage.   
Additionally, the diversity of equipment pro­  
vided to Ukraine by its allies means that there are a   
variety of repair approaches and supply chains, and   
sourcing adequate spare parts has been a challenge.17   
Advances in communications technology have enable   
tele-maintenance, with experts in the rear provid­  
ing guidance, but Ukraine still faces shortfalls.18 As   
one retired U.S. Army general put it, there is now a   
concern that Ukraine will face a situation “when the   
cumulative effect of sustainment shortfalls forces fun­  
damental changes in operational posture and battle­  
field decision-making.”19  
Logistics support also includes medical materiel.   
One analysis found that the scale of munitions used in   
nel to and around the battlefield; engage in protec­  
tion of their transportation nodes and supply depots;   
and adapt and update their planning in response to   
adversary activities. The prevalence of drones and   
improvements in intelligence, surveillance, and   
reconnaissance (ISR) have made fixed logistics net­  
works and nodes even more vulnerable than in the   
past, requiring ongoing adaptation. The war has rein­  
forced the importance of the logistics enterprise to   
operational success, including planning and reacting   
to change.  
Russia’s plan to immediately dominate Ukraine   
failed in part because of assumptions related to the   
expected length of the conflict, which led to a lack   
of preparation. Early analyses pointed to a variety of   
logistics challenges: Russian convoys stalled without   
fuel, tires failed due to poor maintenance, and logis­  
tical units lacked protection and flexibility.6 Images of   
stalled trucks on the road to Kyiv became iconic repre­  
sentations of Moscow’s failures. Russian forces experi­  
enced shortages of food, water, and medical supplies.7   
But Russia’s initial challenges were not simply features   
of its decision to attack in 2022. They were the result   
of long-standing issues for Russian logistics: systematic   
resource inefficiency, inadequate investments in sup­  
plies, and corruption in procurement.8   
The length of the war has given Russia the oppor­  
tunity to recover and adapt from its early misfires. The   
nation has mobilized its industrial base to support the   
war. Russian operational logistics now emphasize dis­  
persed logistics nodes, greater use of rail and civilian   
vehicles, and battlefield repair under fire. Motorcy­  
cles that can travel across open fields are being used   
for troop movement and logistics support.9 Russia is   
getting supplies from China and North Korea, with   
China supplying dual-use items such as microelec­  
tronics and machine tools that can be used for mili­  
tary production and North Korea notably supplying   
both troops and end-use items such as munitions.10   
Russia has addressed labor shortages in its industrial   
base in a variety of ways, including with programs to   
teach school children how to design, manufacture,   
and operate drones.11 Moscow has also worked to   
create a contested environment, attacking Ukrainian   
logistics using drones.12

**Page 146**

140  
Power Projection and the Logistics of Modern War  
Israel’s ability to respond rapidly and in force has   
been bolstered by its close alliance with the United   
States. Shortly after the October 7 attack, United   
States Transportation Command began delivering   
munitions, spare parts, and interceptors directly into   
Israeli air bases, demonstrating the logistical power   
of U.S. airlift.24 Attacks on ships by Houthi rebels in   
Yemen led the command to reach out to commercial   
sealift partners to plan how to mitigate such risk.25   
The United States’ simultaneous provision of   
munitions to Israel and Ukraine has led to questions   
as to whether the nation has sufficient stockpiles to   
support both conflicts while simultaneously prepar­  
ing for other potential wars.26 Israel has faced indus­  
trial base and stockpile challenges, including for its   
Iron Dome interceptors.27 Ensuring the adequacy of   
munitions stockpiles and being ready to mobilize the   
industrial base are difficult but necessary problems   
to solve.   
Hamas’s munitions supply chain has included   
scavenging materiel left behind on battlefields by   
Israeli soldiers and taking unexploded Israeli ord­  
nance, including bombs, missiles, and artillery shells,   
and remanufacturing them into improvised explo­  
sives, rockets, and missiles in factories in its under­  
ground tunnel network.28   
A related conflict has also showed the risk of   
supply chain attacks and the importance of protect­  
ing sources of supply from infiltration—a lesson that   
applies to information systems as well as the indus­  
trial base. Israel’s infiltration of Hezbollah’s pager   
supply chain enabled the inclusion of a small amount   
of explosives, which were then detonated in an oper­  
ation in September 2024.29 Information systems need   
to be protected to ensure that adversaries do not have   
access to sensitive information (e.g., where supplies   
are stored or transportation plans) and also cannot   
inject false data (e.g., inflating readiness numbers or   
misdirecting supplies).   
The particularities of Israel’s case reveal the   
limits of using specific lessons learned for other con­  
flicts. Israel is a small country with dense infrastruc­  
ture and has been able to use relatively permissive   
airspace in its attacks. Many of the engagements in   
the conflict has meant an increase in severe injuries,   
which has implications for the requirements for field   
hospitals, supplies like whole blood, and medical staff   
who can treat patients.20  
Constant drone surveillance by Russia has also   
complicated resupply, especially to soldiers in   
trenches on the front lines. Ukraine has adapted   
drones to deliver supply packages to its forces, to   
reduce the risk of being located and attacked. These   
deliveries include food, water, ammunition, and   
other supplies necessary for sojourns in trenches that   
may last for weeks.21  
Like Russia, Ukraine has adapted its own logis­  
tics enterprise through the course of the war and   
has worked to attack its adversary’s logistics net­  
works. The question now is which side will have the   
resources to sustain the fight longer. Adequate mate­  
riel (e.g., munitions), weapon systems sustainment,   
and transportation will be keys to victory.  
Israel-Gaza  
Unlike Russia’s full-scale invasion of Ukraine, which   
was signaled by a military buildup and Russian leader   
messaging, the October 7, 2023, attack on Israel by   
Hamas was a strategic surprise (in spite of intelligence   
analysts and border sentries trying to warn leadership   
that an attack was imminent).22 While Israel was not   
ready to immediately counter in the first few hours   
of the attack, it had the resources to begin extensive   
airstrikes on Gaza the next day and began a ground   
attack before the end of the month.   
Israel has a much more capable military than   
Hamas, with a much larger end strength and high-end   
equipment. It has continued to press the war after   
two years, with the goals of eliminating the threat that   
Hamas represents, retrieving the remaining living   
hostages captured on October 7, and recovering the   
bodies of the hostages that have died in captivity.   
Hamas has committed fighters and has the advantage   
of a hidden tunnel network underneath Gaza to hide   
in and fight from, as well as access to manufactur­  
ing and storage facilities. Hamas also benefits from a   
global response to the wider humanitarian suffering   
in Gaza, which has led some nations to limit exports   
to Israel.23

**Page 147**

141  
Cynthia R. Cook  
building.30 China is producing an increasing number   
of roll-on/roll off (Ro-Ro) ships that are used to trans­  
port vehicles, including military vehicles.31 The nation   
is also reportedly stockpiling commodities, including   
grain, oil, and gas, and is making global investments   
in logistics to allow for expeditionary operations.32   
Though the comparison is not one-to-one, several   
lessons from the ongoing conflicts should be taken   
into consideration by the United States:   
•   
Make logistics readiness an ongoing pri­  
ority. As seen by Russia’s initial experience   
in Ukraine, waiting for the test of war to iden­  
tify logistics gaps can have disastrous conse­  
quences. Investments in weapons systems   
readiness, stockpiles, industrial surge capacity,   
and appropriate planning capabilities must be   
developed and in place before the fight begins.   
Israel’s relative level of readiness led it to be   
able to respond to the attack quickly, although   
it has relied on support from an ally to have the   
materiel necessary to continue the fight. The   
challenge is in having adequate resources and   
managing the trade-offs between supporting   
existing systems and making plans to procure   
newer ones.  
•   
Assume supply lines will be targeted.   
Attacks on logistics and supply degrade oppo­  
nents’ ability to wage war, and these types   
of attacks have been and will continue to be   
a feature of modern war. Just as Ukraine has   
targeted Russian ammunition depots, trans­  
portation networks, and logistics hubs, and   
Russia has responded in kind, modern war   
will likely include strikes on fuel depots, ports,   
and airfields. Pre-positioning materiel in areas   
of potential conflict can help reduce this risk,   
although developing “iron mountains” of mate­  
riel offers valuable targets for adversaries.  
•   
Make partnerships a priority. Support from   
its partners has enhanced Ukraine’s ability to   
stay in the fight, and Russia has similarly bene­  
fited from supplies delivered by other nations,   
especially China. In a fight in the Indo-Pacific,   
Australia, Japan, and others could offer sup­  
Gaza have taken place in urban areas with an exten­  
sive underground tunnel network. These physical   
characteristics will not apply to other situations, par­  
ticularly those in the Indo-Pacific in any potential   
conflict with China. The distances would be vastly   
greater, the adversary more capable, and the logis­  
tics far more complex.   
Implications for the   
Future of Warfare  
While the Ukraine and Israel cases underscore the   
enduring centrality of logistics, they also demon­  
strate that each conflict is unique and that the les­  
sons from one may be only partially applicable to   
the other. For example, any Indo-Pacific conflict or   
war over Taiwan would be fought at sea and in the   
air, across thousands of nautical miles, and against a   
peer adversary with robust ISR and precision strike   
capabilities. Nations participating in that or any   
other conflict could not assume secure overflight   
rights, permissive air bases, or nearby overland   
supply routes. Logistics would be contested, and   
the persistence of satellite surveillance means that   
operating in secrecy is increasingly impossible.  
Along with the warfighting capabilities   
of potential adversaries, nations   
should look to understand an enemy’s   
logistics capabilities and investments   
as an indicator of how challenging   
any engagement might be.   
Along with the warfighting capabilities of poten­  
tial adversaries, nations should look to understand an   
enemy’s logistics capabilities and investments as an   
indicator of how challenging any engagement might   
be. China’s preeminent role in global shipbuilding   
and dual-use shipyards has enabled the People’s Lib­  
eration Army to draw on commercial infrastructure,   
investment, and intellectual property for naval ship­

**Page 148**

142  
Power Projection and the Logistics of Modern War  
•   
Additive Manufacturing: The 3D printing   
of spare parts can reduce dependence on   
long supply chains, reduce contested logistics   
related to getting the supplies to the fight, and   
speed the availability of spare parts. Intellec­  
tual property considerations relating to the   
ownership of design and approaches to qual­  
ify parts should be addressed in advance, as   
should the training of those expected to serve   
toward the front, to ensure effective mainte­  
nance and repair.  
•   
Tele-maintenance: Modern information   
systems can allow rear maintainers to deliver   
training and information to the front lines.  
•   
New Approaches to Resupply: Uncrewed   
ships and aircraft can deliver parts to the point   
of need, reducing the risk to personnel and   
allowing for a more distributed transportation   
network. Nontraditional systems like motor­  
cycles are smaller than trucks and can bring   
goods closer to the front lines in some contexts.  
•   
Alternative Energy and Energy Networks:   
Reducing fuel dependency by investing in   
hybrid platforms and renewable generation at   
forward bases will reduce the need to transport   
fuel to forward locations. It will also reduce the   
necessity to bring fuel transportation equipment   
such as tanker trucks and drivers, the additional   
security forces to protect those convoys, and   
the food, water, clothes, medical support, and   
other supplies that will be needed as part of that   
supply chain. Planning for energy availability,   
including developing contractual on-demand   
relationships with civilian suppliers in advance   
of conflict, can help ensure resiliency.  
•   
AI and Automation: The equation of logistics   
includes determining what and how much is   
needed, and how to transport it to the fight. AI   
has the potential to increase the efficiency of   
planning for supply and to dynamically route   
and reroute logistics flows in contested environ­  
ments. The concepts underpinning dynamic   
rerouting are not new, but the approach is facil­  
itated by the dramatic increases in information   
port for the United States—but only if plan­  
ning, access agreements, and co-location   
efforts occur in advance. These agreements   
can include pre-positioning materiel, includ­  
ing consumable supplies arrangements, to   
support weapons system sustainment. The   
United States has developed a variety of agree­  
ments along these lines, including the Regional   
Sustainment Framework, the Partnership for   
Indo-Pacific Industrial Resilience, and the   
Defense Industrial Cooperation Framework   
between the United States and Japan.33 China,   
Iran, and North Korea have supported Russia   
in a variety of ways, including by bolstering the   
country’s logistics and readiness enterprise   
with materiel such as spare parts. Those rela­  
tionships seem to be more transactional, with   
each of Russia’s supporters receiving funding,   
technology, or other kinds of information or   
access in return for assistance.   
•   
Partner with industry to ensure adequate   
capacity—including surge—of all aspects of   
logistics support. In a conflict, industry will   
likely need to mobilize to surge production   
of all classes of supply, along with expanding   
transportation. Stockpiles of consumables and   
spare parts will provide the initial ability to fight   
back and allow time to engage the industry   
base. Creating agreements in advance to surge   
when necessary, rather than scrambling to do   
so in the hour of need, will enable smoother   
and more effective support. In one example,   
the United States’ Civil Reserve Air Fleet can   
be tapped to transport personnel and cargo if   
necessary, with airlines getting payments to   
participate in the program on an ongoing basis.   
Additionally, the Defense Production Act offers   
a set of authorities to engage the industrial   
base for national defense purposes.34 These   
and similar laws and arraignments should be   
reauthorized when necessary and adequately   
resourced.  
There are also several emerging technologies that   
the United States should engage with that offer path­  
ways to reduce vulnerability and enhance readiness:

**Page 149**

143  
Cynthia R. Cook  
technology. But these approaches also expand   
the digital attack surface of logistics, which   
requires further investments in cybersecurity.  
•   
Cybersecure Logistics: The information tech­  
nology used in logistics planning and systems   
is critical. Nations must assume that cyberat­  
tacks will aim to cripple sustainment networks,   
either by limiting access to logistics systems or   
by injecting false information that can nega­  
tively impact planning and outcomes.  
Investment in logistics innovation will not elimi­  
nate challenges, but it can reduce the necessary foot­  
print, complicate adversary targeting, and increase   
responsiveness.  
Conclusion  
The importance of logistics and readiness is not a new   
lesson from the conflicts of this decade. The impor­  
tance of sustainment and the need for effective logis­  
tics and supply are the lessons of every war. In future   
conflicts, robust logistics will continue to help win   
wars—and contested logistics will determine who can   
fight at all. Thus, readiness and sustainment should   
not be considered as back-office support functions,   
but as critical to operational readiness and to the   
fight. Lessons from recent conflicts are not propri­  
etary, nor are they necessarily pertinent to all future   
scenarios. Competitors around the world are watch­  
ing the same failures and adaptations, drawing their   
own conclusions. Relying on legacy assumptions of   
uncontested movement, protected infrastructure,   
and industrial dominance will be a recipe for failure.   
Industrial capacity, logistics resilience, and allied   
coordination take years to build. Nations cannot   
wait until war is imminent to invest in sustainment   
technologies, forward partnerships, and stockpiling   
strategies. For future wars, states should consider the   
following actions:  
1.   
Continue to invest in approaches that   
address the issue of contested logistics.   
• Expand pre-positioning of key consum­  
ables in likely conflict zones, with redun­  
dancy and deception built in.  
• Harden and disperse logistics nodes,   
including through mobile and sea-based   
systems. Ensure these are flexible rather   
than fixed. Trains can quickly transport   
large quantities of goods but are easier to   
target than motorcycles.  
• Develop and scale allied sustainment   
frameworks, with joint training and   
common standards. Build and strengthen   
these frameworks in times of peace so   
they are ready in times of war.  
2.   
Enhance planning for logistics, sustain­  
ment, and resilience.   
• Make industrial base investments to   
ensure adequate access to munitions and   
spare parts. Engage industry in planning   
for sustainment in advance of conflict.  
• Invest in AI-enabled logistics planning,   
with resilience against cyber disruption.  
• Ensure that operators and planners are   
focused on logistics, not just the fight.   
Fund wargames and exercises focused on   
contested logistics as part of the warfight­  
ing framework. Ensure that these warga­  
mes can include the possibility of losing   
based on logistics shortfalls to ensure   
operators understand their importance.  
3.   
Plan for change during the conflict.   
• Expect adversaries to adapt during the   
fight. Plan to capture lessons and insights   
on an ongoing basis to be able to adapt as   
effectively.  
The future of deterrence and warfighting hinges   
not just on the operational concepts underpinning   
the fight and the capabilities that are used in it, but   
also on whether competitors can get to the fight at all.   
The lessons from Russia’s war in Ukraine and the Isra­  
el-Gaza conflict suggest that protracted war should be   
part of planning scenarios. As a result, states should   
plan to sustain readiness through a conflict that may   
drag out for years, and where investments in logistics,   
readiness, and resilience determine the winner.

**Page 150**

Conclusion

**Page 151**

The Next Offset  
Winning the Fight Before It Starts  
Seth G. Jones

**Page 152**

146  
The Next Offset  
”  
“  
The United States is not adequately   
prepared for the future of warfare.  
a growing democratization of space that is shifting tra­  
ditional notions of who can wield space capabilities in   
war, creating new motivations for adversaries to deny   
the advantages that space provides, and increasing   
counterspace capabilities.  
Despite these developments, the United States is   
not adequately prepared for the future of warfare. It   
is not prepared to fight and win two or more major   
theater wars at the same time, its defense industrial   
base is not ready for a protracted conflict, and its   
defense budget is significantly lower than at any   
point during the Cold War as a percentage of gross   
domestic product.   
One of the most urgent priorities—and the focus   
of this chapter—is the need to develop an offset to   
defeat and deter China, which has some advantages   
over the United States in mass and scale. An offset   
refers to an effort to affordably counter—or offset—  
an adversary’s advantages through a combination of   
operational concepts and technology.3 The focus on   
emerging technology, such as autonomous systems,   
A  
s the chapters in this volume highlight, the   
United States and its allies face one of the   
most dangerous international security envi­  
ronments in recent history, with war raging in Europe   
and the Middle East and tensions high in the Taiwan   
Strait, South China Sea, East China Sea, and Korean   
Peninsula. In this environment, some aspects of war­  
fare are largely unchanged. As the Prussian general   
and military theorist Carl von Clausewitz argues, war   
is still at its core “an act of violence intended to com­  
pel our opponent to fulfill our will.”1   
Yet the character of warfare is evolving. There   
is an expansion of unmanned and autonomous sys­  
tems—air, undersea, surface, and ground—that can be   
used for “precise mass,” in which large numbers of   
inexpensive, accurate, and technologically advanced   
systems can be deployed together to target an oppo­  
nent.2 There will likely continue to be an explosion of   
open-source intelligence, and AI, quantum, and other   
technologies may be increasingly important on the   
battlefield. Thanks to commercial technology, there is   
photo: sheng kiapeng/china news service/vcg/getty images

**Page 153**

147  
Seth G. Jones  
cheap precision-guided missiles, and AI, has crowded   
out the development of a sound operational concept.   
Technology is important, but it has never been suffi­  
cient to win wars. Successful warfighting has required   
the establishment of an effective operational concept,   
which is then supported by relevant technologies. As   
Andrew Marshall, the long-time head of the Penta­  
gon’s Office of Net Assessment argued, “technology   
makes possible the revolution, but the revolution   
itself takes place only when new concepts of opera­  
tion develop.”4   
A joint U.S. operational concept against a rapidly   
modernizing China should focus on preventing the   
People’s Liberation Army (PLA) from conducting a   
successful invasion of Taiwan by swiftly striking at   
the center of gravity of the PLA’s invasion force. Spe­  
cific examples include PLA amphibious assault ships,   
landing craft, air assault helicopters, and airborne   
delivery planes carrying PLA soldiers, weapons sys­  
tems, and equipment as part of an invasion. Based on   
this concept, the United States needs several types   
of capabilities: a mix of large nuclear-powered attack   
submarines and cheap underwater drones, since the   
PLA is relatively weak in the undersea domain; suf­  
ficient quantities of long-range missiles and cheap   
unmanned and autonomous systems to sink PLA   
ships and destroy other targets; and a combination   
of bombers and stealthy fifth- and sixth-generation   
aircraft to conduct penetrating attacks. But there is   
a lot the United States will not need in the quantities   
it has required in the past, such as large, expensive   
surface vessels and heavy land systems.   
The rest of this chapter is divided into seven sec­  
tions. The first examines Eisenhower’s New Look and   
the first offset in the 1950s. The second section shifts   
to Air-Land Battle and the second offset, which began   
in the 1970s. The third provides a brief overview of   
the third offset in the mid-2010s. The fourth section   
explores the China challenge, including PLA modern­  
ization and an industrial base that is on a wartime   
footing. The fifth outlines a new offset and an opera­  
tional concept designed to defeat a PLA amphibious   
invasion. The sixth section discusses the key capabil­  
ities needed for a new offset. And the seventh section   
provides a brief conclusion.  
New Look  
The first offset took place during the Eisenhower   
administration in the 1950s, when the United States   
faced a major Soviet threat in Europe. The Soviet   
Union had nearly three times the number of ground   
forces in Europe as the United States and its allies, and   
it was building a formidable industrial base. As the   
Eisenhower administration’s top-secret policy paper   
NSC 162/2 concluded, “The USSR has sufficient bombs   
and aircraft, using one-way missions, to inflict serious   
damage on the United States, especially by surprise   
attack. The USSR soon may have the capability of   
dealing a crippling blow to our industrial base and   
our continued ability to prosecute a war.”5  
President Eisenhower concluded that deploy­  
ing and sustaining a large U.S. force in Europe would   
likely weaken the U.S. economy, which at the time was   
recovering from the Korean War. Instead, his adminis­  
tration developed an offset strategy called New Look,   
which was designed to counter Soviet advantages in   
conventional forces. New Look involved building an   
overwhelming nuclear advantage and, in a war, using   
tactical nuclear weapons against Red Army troops—  
including inside West Germany. As described in NSC   
162/2, the United States would develop the capability   
to inflict “massive retaliatory damage by offensive   
striking power,” including with tactical and strategic   
nuclear weapons.6 For officials like Secretary of State   
John Foster Dulles, this doctrine of “massive retal­  
iation” meant that the United States would respond   
disproportionately to a conventional attack.7 The U.S.   
Army fielded infantry and airborne divisions, including   
the Pentomic Division, that were designed to fight and   
win a nuclear war. The goal was to strengthen deter­  
rence and persuade the Soviet Union not to start a war,   
but to nevertheless be prepared in case of a conflict.   
Consequently, New Look led to a major invest­  
ment in two areas: nuclear weapons and long-range   
bombers. The first involved a rapid increase in the   
development and production of nuclear weapons and   
delivery vehicles, especially intercontinental ballis­  
tic missiles (ICBMs). The U.S. Air Force ramped up   
development of the liquid-fueled Atlas ICBM and mul­  
tistage Titan I, as well as two types of guided missiles:

**Page 154**

148  
The Next Offset  
against the Soviet military in three areas: close (at the   
front line of troops), rear (immediately behind the   
front line of troops), and deep.11 As Air-Land Battle   
doctrine stated, “Successful attack will require iso­  
lation of the battle area in great depth as well as the   
defeat of enemy forces in deeply echeloned defensive   
areas. Successful defense will require early detection   
of attacking forces, prompt massing of fires, interdic­  
tion of follow-on forces, and the containment of large   
formations by fire and maneuver.”12  
One of the most significant complementary   
concepts was Assault Breaker, which was devel­  
oped under the oversight of the Defense Advanced   
Research Projects Agency (DARPA).13 Assault Breaker   
focused on offsetting Soviet capabilities by destroying   
waves of Soviet forces that broke through U.S. and   
other NATO defenses. Implementing Assault Breaker   
involved the research, development, production, and   
deployment of sensors, computer programs, stealth   
capabilities, high-speed digital communications, and   
precision weapons to strike hardened mobile targets,   
such as tanks.14 As Perry noted in a memo to Brown   
in August 1978, “In order to stop the second and third   
echelons [of a Soviet and broader Warsaw Pact attack   
against Western Europe] with conventional weapons,   
we need to ‘see deep’ and ‘shoot deep’; that is, detect   
and place precision weapons on targets 30 to 50 KM   
behind the FEBA [forward edge of the battle area].”15  
The efforts of Brown, Perry, and other Pentagon   
officials led to the production of an array of smart   
weapons, such as stealth platforms like the F-117 attack   
aircraft; artillery shells, such as the Copperhead 155   
mm caliber cannon-launched guided projectile; pre­  
cision-guided bombs and missiles, such as Paveway   
and Maverick; and long-range cruise missiles, such as   
the air-launched cruise missile and Tomahawk Land   
Attack Missile.16 The United States also developed a   
series of satellite-based systems, such as the Global   
Positioning System (GPS), and smart sensors, such   
as the Joint Surveillance Target Attack Radar System.   
President Reagan continued the efforts to support   
Assault Breaker and other concepts—including Air-  
Land Battle. The U.S. defense budget rose by almost   
$100 billion between 1981 and January 1985, defense   
sales increased by 60 percent in real terms in the early   
the subsonic, ground-launched Snark cruise missile   
and the supersonic Navaho cruise missile. Testifying   
before Congress in 1956, Chairman of the Joint Chiefs   
of Staff General Nathan Twining explained that the   
Pentagon gave “the very highest priority” to Atlas   
production to offset Soviet military capabilities.8 The   
United States also developed several other missiles   
capable of carrying nuclear warheads: the Polaris   
submarine-launched ballistic missile, the Thor inter­  
mediate-range ballistic missile, and the Jupiter medi­  
um-range ballistic missile.9  
The second priority was long-range bombers   
that could carry nuclear weapons. The backbone   
was the B-52, a long-range bomber capable of flying   
at subsonic speeds that could carry nuclear and con­  
ventional ordnance. The B-52 could also perform a   
range of missions, including strategic attack, close air   
support, air interdiction, and offensive counter-air   
operations. In 1956, President Eisenhower and Sec­  
retary of Defense Charles E. Wilson asked Congress   
for an additional $248.5 million to increase B-52 pro­  
duction from 17 aircraft per month to 20 per month.   
They also requested another $128 million to expand   
air base infrastructure necessary for the B-52 force.10   
The result was impressive. The Soviet Union was   
deterred in Central Europe, and the United States   
held a commanding lead over the Soviet Union in   
missiles by the 1960s—including nuclear missiles.  
Air-Land Battle  
By the 1970s, however, the United States was in   
danger of losing deterrence in Central Europe, thanks   
to U.S. defense cuts and Soviet advancements. The   
Soviet Union had reached nuclear parity with the   
United States and also had a three-to-one advantage   
in conventional capabilities in Central Europe.  
U.S. Department of Defense officials sparked a   
fundamental shift in U.S. defense policy during the   
Carter administration—a second offset—led by such   
individuals as Secretary of Defense Harold Brown   
and Undersecretary of Defense for Research and   
Engineering William Perry. The U.S. Army was also   
pivotal, including such individuals as General Donn   
Starry. At the core of Air-Land Battle was the concept   
of integrating land and air forces to conduct attacks

**Page 155**

149  
Seth G. Jones  
States began to invest in new space capabilities,   
advanced sensors, missile defense, cyber capabilities,   
and a range of promising technologies: unmanned   
underwater systems, advanced sea mines, high-speed   
strike weapons, AI, advanced aeronautics, electro­  
magnetic rail guns, and high-energy lasers. The third   
offset, as Work described it, was a “combination of   
technology, operational concepts, and organizational   
constructs—different ways of organizing our forces—to   
maintain our ability to project combat power into any   
area at the time and place of our own choosing.”19  
Despite these efforts, however, there was no actual   
offset. Neither China nor Russia possessed a signifi­  
cant military advantage over the United States—at least   
not yet. The United States enjoyed a preponderance   
of military power. It spent $647.8 billion on defense   
in 2014, compared to $182.1 billion for China and a   
measly $84.7 billion for Russia.20 This reality made the   
situation fundamentally different from the first and   
second offsets, when the Soviet Union had consider­  
able advantages that the United States needed to offset   
or risk losing deterrence. In many ways, Work’s third   
offset was a decade ahead of its time.  
The China Challenge  
But the situation is different today. China has become   
a formidable military challenger of the United States.   
Its defense industrial base is on a wartime footing   
and is producing a growing number of highly capa­  
ble surface and subsurface vessels, aircraft, missiles   
(including those capable of carrying nuclear war­  
heads), space-based and offensive cyber capabilities,   
and land systems. China’s long-range missile capabil­  
ities have significantly expanded over the past two   
decades, creating a major challenge for the United   
States in parts of the Indo-Pacific. Commensurate   
with its burgeoning land attack capacity, China has   
grown its inventory of ballistic and cruise missiles   
that can engage surface ships. As a result, U.S. for­  
ward-based forces on land and at sea are now vulner­  
able to being damaged or destroyed before they even   
get to the fight. The PLA’s ballistic and cruise missiles   
can be launched from a broad spectrum of air, land,   
and maritime platforms. The concepts that emerged   
from the third offset envisioned China as a potential   
1980s, and the aerospace workforce grew by 15 per­  
cent from 1983 to 1986.17  
Moscow viewed Assault Breaker and the U.S.   
development of sensors, stealth, and precision weap­  
ons with alarm. General Nikolai Ogarkov and other   
Soviet leaders conducted a massive exercise in 1981,   
called Zapad-81, to respond to Assault Breaker and   
became increasingly concerned that the Soviet Union   
was falling behind. Minister of Defense Dmitri Usti­  
nov told a meeting of the Warsaw Pact Committee of   
Defense Ministers that the military balance between   
NATO and the Warsaw Pact was “at the moment not   
in our favor” because of Assault Breaker and other   
U.S. defense efforts.18 Yet again, U.S. defense leaders   
combined concepts of operation with advanced tech­  
nologies to defeat (and ultimately deter) Soviet forces   
in Europe.  
Third Offset  
By the mid-2010s, Pentagon officials led by Deputy   
Secretary of Defense Bob Work developed the “third   
offset.” One of Work’s most significant concerns   
was that China and Russia had made progress in   
achieving parity with the United States in such areas   
as theater-level battle networks, precision-guided   
munitions, and long-range, ground-based fires. Work   
was particularly concerned about China, which he   
assessed was trying to achieve military technical   
parity with the United States. China had developed   
the DF-21D, an antiship ballistic missile with a range of   
nearly 1,000 miles, dubbed the “carrier killer,” which   
posed a serious threat to U.S. surface ships—including   
aircraft carriers—in the Pacific. China and Russia were   
also investing in cyber, space and counterspace, and   
electronic warfare capabilities.  
The solution for Work and others, including   
Secretary of Defense Ashton Carter, was to identify   
and develop operational concepts and technology to   
ensure that the United States could win a war. One   
critical component was the development of new   
warfighting operational concepts, such as the U.S.   
Navy’s Distributed Maritime Operations, U.S. Marine   
Corps’ Expeditionary Advanced Base Operations, U.S.   
Army’s Multi-Domain Operations, and U.S. Air Force’s   
Agile Combat Employment. In addition, the United

**Page 156**

150  
The Next Offset  
chain due to logistical constraints, corruption, and   
inexperience in blue-water operations. More broadly,   
the PLA suffers from “peace disease” (和平病), a lack   
of combat experience since the 1979 Sino-Vietnamese   
War.21 With no serious combat experience for over 50   
years, PLA soldiers, equipment, and doctrine are not   
battle-tested.  
These weaknesses suggest opportunities for the   
United States.  
A New Offset   
A U.S. offset needs to be based on solving a specific   
operational problem.22 A PLA amphibious invasion   
of Taiwan offers a useful test case since reuniting the   
island nation is a major priority for Xi Jinping and   
a war so close to the Chinese mainland would be a   
major challenge for the U.S. military. The primary   
goal of a U.S. operational concept should be stopping   
such an invasion.   
An operational concept to defeat the PLA in the   
Taiwan Strait would also be relevant to conflicts in   
other areas, including in the South China Sea, East   
China Sea, and Yellow Sea. An offset that focuses on   
China does not exclude preparing for contingencies   
elsewhere, such as against Russia in Eastern Europe,   
Iran in the Middle East, or North Korea on the Korean   
Peninsula. But it does mean that the United States   
needs to prioritize defeating and deterring China,   
much like the United States focused primarily on the   
Soviet Union during the Cold War.  
A successful PLA invasion would require quickly   
moving massive amounts of troops, weapons, and   
materiel onto Taiwan or another territory through   
an amphibious landing, air assault, or airborne land­  
ings, or most likely a combination of these means,   
in the shortest time possible. The PLA would likely   
need hundreds of thousands of soldiers—from the   
PLA Army (PLAA), PLAN Marine Corps, and PLAAF   
Airborne Corps—and vast amounts of materiel.23   
It would then need to bring those forces to Taiwan   
using amphibious assault ships, landing craft, civilian   
roll-on/roll-off (Ro-Ro) ferries, air assault helicopters,   
and transport aircraft.24 These platforms would trans­  
port first echelon troops to seize and hold a lodgment,   
future challenge, but now China presents a near-term   
challenge with some advantages in mass and scale.  
China has also invested in advanced surface-to-air   
missile systems with powerful tracking and guidance   
radars equipped with electronic countermeasures and   
missiles able to engage fighter aircraft at long ranges.   
The radars and missile launchers can be mounted   
on vehicles, making them challenging to locate,   
target, and destroy. Suppressing China’s integrated   
air defense systems would be difficult and time con­  
suming for U.S. pilots, especially if deployed in dense   
arrays and aided by survivable C2 facilities. China   
complements its surface-based air defenses with sub­  
stantial numbers of fourth- and fifth-generation fighter   
aircraft, such as the J-20 and J-35 fighters, along with   
H-6J, H-6K, and H-6N bombers. China has also fielded   
the KJ-500, the country’s most advance airborne early   
warning and control aircraft, which enables the PLA   
Air Force (PLAAF) to detect, track, and target U.S. and   
partner capabilities at greater ranges.  
The PLA Navy (PLAN) has made major strides in   
modernizing its surface and subsurface fleets. As a   
result of these investments, China’s surface fleet fea­  
tures growing numbers of destroyers and frigates with   
modern combat management systems and sensors, as   
well as long-range SAMs and surface-to-surface mis­  
siles. Similarly, the PLAN is modernizing its submarine   
fleet with growing numbers of nuclear-powered vessels   
and more capable antiship cruise missiles. Further­  
more, the PLAN has embarked on a long-term effort   
to develop and deploy several aircraft carriers, includ­  
ing the Type 003 carrier Fujian. The result is that the   
United States is losing deterrence in the Indo-Pacific,   
particularly around such areas as the Taiwan Strait,   
where the PLA can gain advantages in mass and scale.   
Like the Soviet Union during the Cold War, how­  
ever, China has vulnerabilities that can be exploited   
which need to be integrated into an offset strategy.   
One major weakness is antisubmarine warfare, where   
the PLAN still struggles to detect, identify, and track   
U.S. submarines. While China has made significant   
improvements in antisubmarine warfare, the United   
States remains dominant in the undersea domain. In   
addition, the PLAN and PLAAF would likely face chal­  
lenges extending operations outside the first island

**Page 157**

151  
Seth G. Jones  
To quickly target the heart of the PLA’s invasion   
force, the United States would need to generate   
combat power that can operate both inside and out­  
side the reach of China’s strike systems. As Admiral   
Samuel Paparo, commander of Indo-Pacific Com­  
mand, remarked, “I want to turn the Taiwan Strait   
into an unmanned hellscape using a number of clas­  
sified capabilities so I can make their lives utterly mis­  
erable for a month, which buys me the time for the   
rest of everything.”30  
In the short run, the United States would need   
to ensure that U.S. and allied forces could withstand   
initial PLA attacks; blind PLA battle networks and   
command, control, communications, computers,   
cyber, intelligence, surveillance, and reconnaissance   
systems (C5ISR); execute a suppression campaign   
against PLA long-range missiles; and target PLA air   
defense systems. As Admiral Paparo acknowledged,   
the U.S. military badly needs “counter-C5ISR capabil­  
ities in cyber, space, counterspace, to ensure that the   
United States can see, understand, decide, act, assess,   
learn faster than the PRC can, to enhance our ability   
to blind, to deceive, and to destroy the adversary’s   
ability to see and sense.”31  
In the long run, the United States would need to be   
prepared for a protracted campaign, maintain oper­  
ational logistics, and increase defense industrial pro­  
duction for critical munitions and weapons systems,   
including air defense and long-range strike. Allies such   
as Japan, Australia, South Korea, and the Philippines   
would be helpful, though not necessarily assured.  
A Mix of Capabilities  
Several types of capabilities are important to defeat   
PLA forces as part of this operational concept—and   
should drive research, development, and production   
of the U.S. defense industrial base.   
The first includes capabilities that allow the   
United States to maintain its undersea advantage. Of   
particular value are attack submarines, such as Virgi­  
na-class nuclear-powered submarines, and relatively   
cheap underwater drones. PLA capabilities are still   
relatively weak in antisubmarine warfare, and the   
PLA has serious difficulties finding U.S. submarines.   
allowing follow-on PLA forces to flow into Taiwan.   
The PLAA would likely take the lead in attempting to   
break through Taiwan’s coastal defenses, establishing   
one or more beachheads, overrunning entrenched   
defenders, and establishing conditions for sec­  
ond-echelon PLA forces.25 In addition, the PLA would   
likely need thousands of ballistic and cruise missiles,   
rockets, drones, and strike aircraft capable of hitting   
enemy forces and infrastructure, supported by cyber,   
space, and air defense capabilities. The initial phases   
of a PLA campaign would also likely involve a block­  
ade and cyber and space operations.26 Throughout   
the process, the PLA’s joint logistics and national   
defense mobilization systems would play key roles.27  
Consequently, a U.S. operational concept needs   
to include several components.  
The first is to preposition equipment to move   
with urgency and speed, which is beginning to occur.   
The United States would need to act within hours or   
days to prevent a territorial fait accompli. There may   
not be sufficient time for a slow and steady build-up   
of forces, much like the United States did before Oper­  
ation Desert Storm in 1991. Consequently, the United   
States needs to posture its forces, munitions, and   
equipment today for a rapid engagement. Examples   
include deploying sufficient bombers to Australia and   
Alaska, hardening shelters for aircraft, establishing   
active defenses for missiles, and stockpiling sufficient   
quantities of fuel, spare parts, munitions, and other   
materiel that can be used for a fight now.28  
Second, U.S. forces would need to rapidly strike   
at the center of gravity of the PLA’s invasion force   
and cripple its offensive. This would require identify­  
ing high-value targets, including amphibious assault   
ships, landing craft, air assault helicopters, and air­  
borne delivery planes carrying PLA soldiers, weap­  
ons systems, and equipment. It would also involve   
precisely hitting and destroying PLA air defenses,   
air and missile bases, artillery, and operational C2   
centers supporting the invasion force.29 While many   
of these strikes might occur in transit from the main­  
land to Taiwan, the United States would also need to   
weigh striking targets in ports, airfields, and bases   
on the Chinese mainland, raising important ques­  
tions about escalation.

**Page 158**

152  
The Next Offset  
the B-21 Raider presents China with a particularly   
daunting challenge. They can be based beyond the   
range of Chinese ballistic missiles, and they can carry   
substantial bombs to attrit Chinese forces. Some fifth-   
and sixth-generation stealth aircraft are also helpful   
because their speed, sensor packages, and strike   
capabilities will likely allow them to operate inside   
the PLA’s anti-access/area denial (A2/AD) areas for air-  
to-air engagements, some air-to-ground missions, and   
overall battle management.  
Other capabilities are also important, such as   
all-domain C2 capabilities and software that leverages   
next-generation AI, which allows the U.S. military to   
operate a battle network. So are space, cyber, elec­  
tronic warfare, and some land capabilities, such as   
air defense systems and long-range fires. But other   
capabilities are not likely to be as critical for this pri­  
oritized operational concept. For example, surface   
ships are less likely to be useful in a war because of   
their vulnerability. Destroyers are highly exposed in   
a war, as are aircraft carriers. Many U.S. land systems,   
such as heavy tanks, are not helpful for this fight.  
Conclusion  
There is a growing chorus of voices who argue that   
the future of warfare hinges on the production and   
use of emerging technology, such as autonomous   
systems, cheap precision-guided missiles, and AI.   
As one article concludes, “Future wars will no longer   
be about who can mass the most people or field the   
best jets, ships, and tanks. Instead, they will be   
dominated by increasingly autonomous weapons   
systems and powerful algorithms.”37 Some contend   
that the era of large, expensive platforms is dead. As   
Elon Musk pronounced, the F-35 aircraft is “obso­  
lete” and “manned fighter jets are outdated in the   
age of drones and only put pilots’ lives at risk.”38   
Another skeptic referred to these large platforms,   
such as bombers and fighter aircraft, as “old legacy   
zombie programs.”39  
But U.S. military capabilities need to be grounded   
in a viable joint operational concept. Inventing tech­  
nologies or being the first country to use a technology   
in warfare does not guarantee a significant advantage   
on the battlefield—militaries still have to integrate the   
In multiple iterations of CSIS wargames, U.S. subma­  
rines wreak havoc against Chinese ships, including   
large amphibious vessels, escorts, and logistics ves­  
sels. Submarines are also needed to screen against   
Chinese submarines exiting the first island chain.32  
The United States should also prioritize auton­  
omous underwater drones. There will be substan­  
tial U.S. submarine attrition in a fight against China,   
such as in the relatively shallow waters of the Taiwan   
Strait.33 Each loss would be tough, since a Virgin­  
ia-class submarine has a crew of roughly 132 sailors   
and costs approximately $4.5 billion each.34 While   
underwater drones are not yet as capable as attack   
submarines, they can be programmed to fulfill some   
critical missions, such as minelaying and strike   
against PLA submarines and surface vessels.  
Second is a major increase in the U.S. inventory   
of precision-guided, long-range missiles—including   
antiship missiles—that can strike PLA vessels and air­  
craft. Munition usage is likely to be high in a protracted   
conflict with the PLA. Long Range Anti-Ship Missiles   
(LRASMs) are effective against PLA targets. But they are   
expensive at over $3 million per missile, and the United   
States does not have enough of them.35 The Joint Air-  
to-Surface Missile-Extended Range (JASSM-ER) is also   
effective and comes with a price of roughly $1.5 million   
per missile.36 The United States needs to ramp up the   
research, development, and production of long-range   
missiles—especially antiship missiles to strike PLA sur­  
face vessels—and do so at a lower cost.  
Large numbers of relatively cheap unmanned air­  
craft systems, or drones, are also critical for defeating   
the PLA, particularly drones that do not need run­  
ways to launch. They can perform valuable missions   
in a war—such as intelligence, surveillance, reconnais­  
sance, battle damage assessment, electronic warfare,   
and strike—within range of PLA missiles and drones.   
They are also expendable since they are cheaper than   
fourth- and fifth-generation aircraft and do not endan­  
ger a pilot or crew.  
Third, manned aircraft are still important in this   
operational concept, especially bombers and stealthy   
fifth- and sixth-generation fighters. The range and   
high ordnance throughput of stealth bombers like

**Page 159**

153  
Seth G. Jones  
technology into combat.40 British engineers at Wil­  
liam Foster & Company developed and produced the   
tank, including one dubbed the “Little Willie,” with   
the support of senior British officers such as Sir John   
French and Douglas Haig.41 But it was German mili­  
tary officers such as Heinz Guderian that effectively   
used the tank to devastating effect during blitzkrieg   
operations in World War II.   
Bold pronouncements about obsolete and anti­  
quated platforms and systems—such as fifth-genera­  
tion aircraft and bombers—are largely meaningless   
unless they are connected to a joint operational   
concept against a specific adversary. Technology   
needs to support the joint concept, not the other   
way around. And this is exactly why it is important   
to develop an offset to deter and—if deterrence fails—  
defeat a rising China.

**Page 160**

About the Contributors

**Page 161**

155  
War and the Modern Battlefield  
Kari A. Bingen is the director of the Aerospace Security Project and a   
senior fellow in the Defense and Security Department at the Center for   
Strategic and International Studies (CSIS). She joined CSIS from HawkEye   
360, an innovative space technology company creating a new class of   
radio frequency (RF) data and analytics, where she was the chief strategy   
officer. Prior to the private sector, Kari served as the deputy undersec­  
retary of defense for intelligence and security, overseeing the defense   
intelligence and security enterprises, comprising more than 120,000 per­  
sonnel and an annual budget of over $54 billion. Before that, Kari served   
as the policy director on the House Armed Services Committee and staff   
lead for its Strategic Forces Subcommittee, advising members of Congress   
on defense policy, program, and budget matters. Prior to entering gov­  
ernment, Kari specialized in national security space issues, working with   
U.S. defense and intelligence community clients, first as a space systems   
analyst at SRA International’s Adroit C4ISR Center, and then as a senior   
space policy analyst at the Aerospace Corporation. In addition to her work   
at CSIS, Kari is an adjunct assistant professor at Georgetown University.   
She is a member of the U.S. Strategic Command Strategic Advisory Group,   
was a commissioner on the CSIS Technology and Intelligence Task Force,   
and serves on a number of corporate and nonprofit advisory boards. She   
graduated from the Massachusetts Institute of Technology with a degree   
in aeronautics and astronautics and was a 2002 National Reconnaissance   
Office technology fellow.  
Daniel Byman is the director of the Warfare, Irregular Threats, and Ter­  
rorism Program at CSIS. He is also a professor at Georgetown University’s   
School of Foreign Service and director of the Security Studies Program. He   
is the foreign policy editor for Lawfare and has served as a senior adviser   
to the Department of State on the International Security Advisory Board.   
He has held positions at the Brookings Institution, the RAND Corporation,   
the U.S. intelligence community, the 9/11 Commission, and the Joint 9/11   
Inquiry Staff of the House and Senate Intelligence Committees. Dr. Byman   
is a leading researcher and has written widely on a range of topics related   
to terrorism, insurgency, intelligence, social media, artificial intelligence,   
and the Middle East. He is the author of nine books, including Spreading   
Hate: The Global Rise of White Supremacist Terrorism (Oxford, 2022); Road   
Warriors: Foreign Fighters in the Armies of Jihad (Oxford, 2019); Al Qaeda,   
the Islamic State, and the Global Jihadist Movement: What Everyone Needs to   
Know (Oxford, 2015); and A High Price: The Triumphs and Failures of Israeli   
Counterterrorism (Oxford, 2011). He is the author or coauthor of almost 200   
academic and policy articles, monographs, and book chapters as well as   
numerous opinion pieces in the New York Times, Wall Street Journal, Wash­  
ington Post, and other leading journals. Dr. Byman is a graduate of Amherst   
College and received his PhD in political science from the Massachusetts   
Institute of Technology.

**Page 162**

156  
A Report of the CSIS Defense and Security Department  
Mark Cancian (Colonel, USMCR, ret.) is a senior adviser with the CSIS   
Defense and Security Department. He joined CSIS in April 2015 from the   
Office of Management and Budget, where he spent more than seven years   
as chief of the Force Structure and Investment Division, working on issues   
such as Department of Defense budget strategy, war funding, and procure­  
ment programs, as well as nuclear weapons development and nonprolifer­  
ation activities in the Department of Energy. Previously, he worked on force   
structure and acquisition issues in the Office of the Secretary of Defense   
and ran research and executive programs at Harvard University’s Kennedy   
School of Government. In the military, Colonel Cancian spent over three   
decades in the U.S. Marine Corps, active and reserve, serving as an infantry,   
artillery, and civil affairs officer and on overseas tours in Vietnam, Desert   
Storm, and Iraq (twice). Since 2000, he has been an adjunct faculty member   
at the Johns Hopkins School of Advanced International Studies, where he   
teaches a course on the connection between policy and analysis. A prolific   
author, he has published over 40 articles on military operations, acqui­  
sition, budgets, and strategy and received numerous writing awards. He   
graduated with high honors (magna cum laude) from Harvard College and   
with highest honors (Baker scholar) from Harvard Business School.  
Eliot A. Cohen is the Arleigh A. Burke Chair in Strategy at CSIS and pro­  
fessor emeritus at Johns Hopkins School of Advanced International Studies   
(SAIS), where he has taught since 1990. He received his BA and PhD degrees   
from Harvard and taught there and at the U.S. Naval War College before   
going to SAIS, where he has also served as the school’s ninth dean. His books   
include, most recently, The Hollow Crown: Shakespeare on How Leaders Rise,   
Rule, and Fall (Basic Books, 2023), as well as The Big Stick: The Limits of   
Soft Power and the Necessity of Military Force (Basic Books, 2017), Conquered   
into Liberty: Two Centuries of Battle Along the Great Warpath that Made the   
American Way of War (FreePress, 2011) and Supreme Command: Soldiers,   
Statesmen, and Leadership in Wartime (Anchor, 2002), among others. He   
served in the U.S. Army Reserve, was a director in the Defense Department’s   
policy planning staff, led the U.S. Air Force’s multivolume study of the first   
Gulf War, and has served in various official advisory positions. From 2007 to   
2009 he was counselor of the Department of State, serving as Secretary Con­  
doleezza Rice’s senior adviser, focusing chiefly on issues of war and peace,   
including Iraq and Afghanistan. He is a contributing writer at The Atlantic,   
and his commentary has also appeared in the Washington Post, Wall Street   
Journal, New York Times, and on major television networks.  
Cynthia R. Cook is a senior fellow with the Center for the Industrial Base   
in the Defense and Security Department at CSIS. She is widely published on   
defense acquisition policy and organization, the defense industrial base,   
new technology development, and weapon systems production and sustain­  
ment. Dr. Cook is a member of the editorial board for the Defense Acquisition   
Research Journal and is an adjunct professor at the Pardee RAND Graduate

**Page 163**

157  
War and the Modern Battlefield  
School. From 1997 to 2021, Dr. Cook worked as a senior management scientist   
at RAND, where she served as the director of the Acquisition and Technology   
Policy Center and managed a wide range of studies for components across   
the U.S. Department of Defense, along with the Australian Department of   
Defense and the UK Ministry of Defense. Previously, Dr. Cook was a research   
specialist at the Massachusetts Institute of Technology, working on the Lean   
Aerospace Initiative. Before her graduate studies, Dr. Cook worked in New   
York as an investment banker, specializing in high-yield finance. She holds   
a PhD in sociology from Harvard University and a BS in management from   
the Wharton School of the University of Pennsylvania.  
Seamus P. Daniels is a fellow for Defense Budget Analysis in the Defense   
and Security Department at CSIS, where he researches issues related to   
U.S. and global defense funding, force structure, and military readiness. He   
has authored publications on trends in the overall U.S. defense budget, the   
legislative process surrounding defense appropriations, defense strategy   
and force structure, and NATO burden sharing. Prior to joining CSIS, Mr.   
Daniels worked for Government Executive Media Group. He holds an MA in   
international relations from Johns Hopkins University School of Advanced   
International Studies and an AB from Princeton University’s School of   
Public and International Affairs with minors in Near Eastern studies and   
Arabic language and culture.  
Hannah Freeman is a program coordinator and research assistant with   
the Missile Defense Project at CSIS. Before joining CSIS, she worked as a   
research assistant at the Freeman Spogli Institute for International Studies   
and as an intern with the U.S. House of Representatives and the Department   
of State’s Bureau of Arms Control, Deterrence, and Stability. She holds a BA   
in political science from Stanford University.  
Emily Harding is director of the Intelligence, National Security, and   
Technology (INT) Program and vice president of the Defense and Secu­  
rity Department (DSD) at CSIS. As the head of the INT Program, Harding   
provides thought leadership on the most critical issues facing intelligence   
professionals and on the future of intelligence work. In her capacity as vice   
president of DSD, she is responsible for leading a team of world-renowned   
scholars providing policy solutions that shape national security. Drawing   
on her decades of experience in national security, Harding has established   
herself as an expert on how technology is revolutionizing national secu­  
rity work. She has also served in a series of high-profile national security   
positions at critical moments. While serving as deputy staff director on the   
Senate Select Committee on Intelligence, she led the committee’s investiga­  
tion into Russian interference in the 2016 elections, which was lauded for   
its bipartisanship. At the Central Intelligence Agency, she led analysts and   
analytic programs through moments of crisis, including shepherding the   
Iraq Group during the attempted Islamic State takeover. During a tour at the

**Page 164**

158  
A Report of the CSIS Defense and Security Department  
National Security Council, she served as director for Iran. After leaving the   
White House, her team ran the first Office of the Director of National Intelli­  
gence–led presidential transition, where she was responsible for briefing the   
incoming administration. Harding is an adjunct lecturer at the Johns Hop­  
kins School of Advanced International Studies. Her analysis has appeared in   
the Wall Street Journal, BBC, NPR, Bloomberg, and other outlets. She holds a   
master’s degree from Harvard University’s Kennedy School of Government   
and a bachelor’s degree from the University of Virginia.  
Benjamin Jensen is director of the Futures Lab and a senior fellow for the   
Defense and Security Department at CSIS. At CSIS, Dr. Jensen leads research   
initiatives on applying data science and AI and machine learning to study   
the changing character of war and statecraft. Under his leadership, Futures   
Lab has pioneered building AI applications into wargames and innovative   
scenario exercises. The exercise topics range from major war, competitive   
strategy, and national mobilization to economic security, energy politics,   
and national resilience. He is also the Frank E. Petersen Chair for Emerging   
Technology and a professor of strategic studies at the Marine Corps Univer­  
sity School of Advanced Warfighting (MCU). At MCU, he leads a research pro­  
gram on future war and teaches seminars on modern operational art and   
joint-all domain operations. Dr. Jensen has authored five books including   
Information at War: Military Innovation, Battle Networks, and the Future of   
Artificial Intelligence (Georgetown University Press, 2022), Military Strategy   
in the 21st Century: People, Connectivity, and Competition (Cambria, 2018),   
Cyber Strategy: The Evolving Character of Power and Coercion (Oxford Univer­  
sity Press, 2018), and Forging the Sword: Doctrinal Change in the U.S. Army   
(Stanford University Press 2016). He also served as senior research director   
for the U.S. Cyberspace Solarium Commission and is a reserve officer in   
the U.S. Army, with command experience from platoon to battalion. Dr.   
Jensen graduated from the University of Wisconsin-Madison and earned his   
MA and PhD from the American University School of International Service.  
Seth G. Jones is president of the Defense and Security Department and   
Harold Brown Chair at the Center for Strategic and International Studies   
(CSIS). He focuses on defense strategy, military operations, the defense   
industrial base, and irregular warfare. He leads a bipartisan team of over   
150 resident and non-resident staff that conduct policy-relevant research   
and analysis on defense and national security issues. Dr. Jones currently   
serves as a Commissioner on the Congressionally established Afghanistan   
War Commission. He also teaches at the Center for Homeland Defense and   
Security (CHDS) at the U.S. Naval Postgraduate School.  
Prior to CSIS, Dr. Jones was director of the International Security and   
Defense Policy Center at the RAND Corporation. Before that, he served in   
several positions in the Office of the Secretary of Defense and U.S. Special   
Operations Command. He served as representative for the commander, U.S.

**Page 165**

159  
War and the Modern Battlefield  
Special Operations Command, to the assistant secretary of defense for spe­  
cial operations. He was also a plans officer and adviser to the commanding   
general, U.S. Special Operations Forces, in Afghanistan (Combined Forces   
Special Operations Component Command–Afghanistan). Dr. Jones served   
on a congressionally mandated panel that reviewed the FBI’s implementa­  
tion of counterterrorism recommendations contained in the 9/11 Commis­  
sion Report. He is author of The American Edge: The Military Tech Nexus and   
the Sources of Great Power Dominance (Oxford, 2025), Three Dangerous Men:   
Russia, China, Iran, and the Rise of Irregular Warfare (W.W. Norton, 2021),   
A Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland (W.W.   
Norton, 2018), Waging Insurgent Warfare: Lessons from the Vietcong to the   
Islamic State (Oxford University Press, 2016), Hunting in the Shadows: The   
Pursuit of al Qa’ida since 9/11 (W.W. Norton, 2012), and In the Graveyard of   
Empires: America’s War in Afghanistan (W.W. Norton, 2009). Dr. Jones has   
published articles in a range of journals, including Foreign Affairs, Foreign   
Policy, and International Security, and news outlets like the New York Times,   
Washington Post, and Wall Street Journal. He is a graduate of Bowdoin Col­  
lege and received his MA and PhD from the University of Chicago.  
Thomas Karako is the director of the Missile Defense Project and a senior   
fellow with the Defense and Security Department at CSIS, where he arrived   
in 2014. His research focuses on national security, missile defense, nuclear   
deterrence, and public law. In 2010–2011, he was an American Political Sci­  
ence Association congressional fellow, working with the professional staff   
of the House Armed Services Committee and the Subcommittee on Strate­  
gic Forces on U.S. strategic forces policy, nonproliferation, and NATO. Dr.   
Karako received his PhD from Claremont Graduate University and his BA   
from the University of Dallas.  
Elizabeth Kos is a former program manager and research associate with   
the CSIS Project on Nuclear Issues.  
Aosheng Pusztaszeri is a research assistant with the Intelligence, National   
Security, and Technology Program at CSIS, where he focuses on emerging   
technologies and their implications for national security. Before joining   
CSIS, he interned in the U.S. Senate and the U.S. House of Representatives   
and served as an undergraduate research assistant in Cornell University’s   
Department of Government. Aosheng holds a BA in government and history   
from Cornell University.  
Joseph Rodgers is deputy director and fellow with the Project on Nuclear   
Issues in the International Security Program at CSIS. His research focuses   
on the nuclear non-proliferation regime, U.S. nuclear modernization, and   
open-source intelligence. Joseph has led research projects on nuclear arms   
control, deterrence, and disarmament. He is a PhD student in the biodefense   
program at George Mason University. Previously, Joseph worked as a graduate   
research assistant at the James Martin Center for Nonproliferation Studies

**Page 166**

160  
A Report of the CSIS Defense and Security Department  
and interned with the United Nations Institute for Disarmament Research.   
Joseph holds an MA in nonproliferation and terrorism from the Middlebury   
Institute for International Studies and a BA in politics from the University of   
California, Santa Cruz.  
Clayton Swope is the deputy director of the Aerospace Security Proj­  
ect and a senior fellow in the Defense and Security Department at CSIS.   
Before joining CSIS, Swope led national security and cybersecurity public   
policy for Amazon’s Project Kuiper, an initiative to increase global broad­  
band access through a constellation of satellites in low Earth orbit. While at   
Amazon, he also worked on cloud policy issues. Prior to his time at Amazon,   
Swope served as a senior adviser on national security, space, foreign affairs,   
and technology policy issues for a member of the U.S. House of Represen­  
tatives. He also worked for more than 14 years at the Central Intelligence   
Agency, serving largely in the Directorate of Science and Technology. He   
holds a bachelor of science in mechanical engineering from the University   
of Notre Dame.  
Sofia Triana is a program coordinator for the Warfare, Irregular Threats,   
and Terrorism Program at CSIS. Before joining CSIS, she worked on U.S.   
Department of State public diplomacy programs at World Learning and   
served as an associate at a DC-based political communications and adver­  
tising firm. Sofia graduated Phi Beta Kappa from the University of North   
Carolina at Chapel Hill, where she earned a BA in U.S. history and peace,   
war, and defense.  
Heather Williams is the director of the Project on Nuclear Issues and   
a senior fellow in the Defense and Security Department at CSIS. She is a   
member of the Defense Science Board, an associate fellow with the Project   
on Managing the Atom in the Belfer Center for Science and International   
Affairs at the Harvard Kennedy School, and a senior associate with the Royal   
United Services Institute in London. Before joining CSIS, Dr. Williams was a   
visiting fellow with the Project on Managing the Atom and a Stanton nuclear   
security fellow in the Security Studies Program at MIT. Until 2022, she was a   
senior lecturer (associate professor) at King’s College London and served as   
a specialist adviser to the House of Lords International Relations Commit­  
tee. Dr. Williams has a PhD in war studies from King’s College London, an   
MA in security policy studies from the George Washington University, and   
a BA in international relations and Russian studies from Boston University.

**Page 167**

Endnotes

**Page 168**

162  
A Report of the CSIS Defense and Security Department  
INTRODUCTION: HOW TO THINK ABOUT MODERN WARFARE  
1   
For more on this theme, see Cyril Falls, One Hundred Years of War, 1850-1950 (New York:   
Collier, 1953); Williamson Murray, The Dark Path: The Structure of War and the Rise of the   
West (New Haven, CT: Yale University Press, 2024).  
2   
Brent M. Eastwood, “Russia’s Black Sea Fleet Is Now ‘Functionally Inactive’,”   
19FortyFive, February 3, 2025, https://www.19fortyfive.com/2025/02/russias-black-sea-  
fleet-is-now-functionally-inactive/.  
3   
U.S. Government Accountability Office, In-Space Servicing, Assembly, and   
Manufacturing: Benefits, Challenges, and Policy Options, GAO-25-107555 (Washington,   
DC: U.S. Government Accountability Office, July 2025), https://www.gao.gov/products/  
gao-25-107555.  
ADVERSARIES AND THE FUTURE OF COMPETITION  
1   
While this chapter focuses on China, Russia, Iran, and North Korea, it assumes that   
cooperation with other countries could also increase.  
2   
Andrew Radin and Clint Reach, Russian Views of the International Order (Santa Monica:   
RAND, May 2017), https://www.rand.org/pubs/research\_reports/RR1826.html; and   
Ruonan Liu and Songpo Yang, “China and the Liberal International Order: A Pragmatic   
and Dynamic Approach,” International Affairs 99, no. 4 (July 2023): 1383–1400, https://  
doi.org/10.1093/ia/iiad169.  
3   
Philip Zelikow, “Confronting Another Axis? History, Humility, and Wishful Thinking,”   
Texas National Security Review 7, no. 3 (Summer 2024): 90, https://tnsr.org/2024/05/  
confronting-another-axis-history-humility-and-wishful-thinking/.   
4   
Xi Jinping, “Speech at ‘The Road to Rejuvenation’,” China Copyright and Media,   
November 29, 2012, https://chinacopyrightandmedia.wordpress.com/2012/11/29/  
speech-at-the-road-to-rejuvenation/.   
5   
Senior U.S. and European government officials, in discussion with the author, 2025;   
and U.S. Department of the Treasury, “Treasury Targets Actors Involved in Drone   
Production for Russia’s War Against Ukraine,” press release, October 17, 2024, https://  
home.treasury.gov/news/press-releases/jy2651.  
6   
Steve Holland and Susan Heavey, “US Says China Is Boosting Russia’s War Machine in   
Ukraine,” Reuters, April 15, 2024, https://www.reuters.com/world/us-says-china-is-  
boosting-russias-war-machine-ukraine-2024-04-12/.   
7   
See, for example, U.S. Department of the Treasury, “U.S. Continues to Degrade Russia’s   
Military-Industrial Base and Target Third-Country Support with Nearly 300 New   
Sanctions,” press release, May 1, 2024, https://home.treasury.gov/news/press-releases/  
jy2318/.   
8   
U.S. government officials, in discussion with the author, 2025; and Office of the Director   
of National Intelligence, Support Provided by the People’s Republic of China to Russia   
(Washington, DC: Office of the Director of National Intelligence, July 2023), https://  
democrats-intelligence.house.gov/uploadedfiles/odni\_report\_on\_chinese\_support\_to\_  
russia.pdf.   
9   
U.S. Department of the Treasury, “U.S. Continues.”  
10   
See, for example, Omar Al-Ghusbi and Conrad Rousseau, Airborne Axis: Inside the   
Deal That Brought Iranian Drone Production to Russia (Washington, DC: C4ADS, May   
2025), https://c4ads.org/reports/airborne-axis/; U.S. Defense Intelligence Agency, “DIA   
Releases Updated Report on Russia’s Use of Lethal Iranian Unmanned Aerial Vehicles   
(UAVs) in Ukraine,” press release, August 25, 2023, https://www.dia.mil/News-Features/  
Articles/Article-View/Article/3504948/dia-releases-updated-report-on-russias-use-  
of-lethal-iranian-unmanned-aerial-ve/; and C. Todd Lopez, “Iran Gives Russia Short-  
Range Missiles, While U.S., Partners Expect to Keep Bolstering Ukrainian Air Defense,”   
U.S. Department of Defense, September 10, 2024, https://www.defense.gov/News/  
News-Stories/Article/Article/3901774/iran-gives-russia-short-range-missiles-while-us-

**Page 169**

163  
War and the Modern Battlefield  
partners-expect-to-keep-bolster/.   
11   
Mary Ilyushina, “Russia’s Deadly Drone Industry Upgraded with Iran’s Help,   
Report Says,” Washington Post, May 29, 2025, https://www.washingtonpost.com/  
world/2025/05/29/russia-iran-drone-cooperation-industry/; and Al-Ghusbi and   
Rousseau, Airborne Axis.  
12   
“Iran’s Revolutionary Guards Commander Says Iran Purchased Russian-Made Sukhoi   
35 Fighter Jets,” Reuters, January 27, 2025, https://www.reuters.com/business/  
aerospace-defense/irans-revolutionary-guards-commander-says-iran-purchased-  
russian-made-sukhoi-35-2025-01-27/; and Maya Carlin, “Iran Finally Admits to Buying   
Russian Su-35 Fighters,” National Interest, January 28, 2025, https://nationalinterest.  
org/blog/buzz/iran-finally-admits-to-buying-russian-su-35-fighters.   
13   
Justin McCurry, “From Ammunition to Ballistic Missiles: How North Korea Arms Russia   
in the Ukraine War,” The Guardian, April 25, 2025, https://www.theguardian.com/  
world/2025/apr/25/how-north-korea-arms-russia-in-ukraine-war; Tom Balmforth   
and Mariano Zafra, “Thousands of Troops, Millions of Shells,” Reuters, April 15,   
2025, https://www.reuters.com/graphics/UKRAINE-CRISIS/NORTHKOREA-RUSSIA/  
lgvdxqjwbvo/; Dasl Yoon and Matthew Luxmoore, “Satellite Images Show North Korea   
Boosting Arms Flow to Russia,” Wall Street Journal, December 23, 2024, https://www.  
wsj.com/world/russia-north-korea-weapons-shipment-676d7f52; and U.S. Defense   
Intelligence Agency, North Korea: Enabling Russian Missile Strikes Against Ukraine   
(Washington, DC: Defense Intelligence Agency, May 2024), https://www.dia.mil/  
Portals/110/Documents/News/Military\_Power\_Publications/DPRK\_Russia\_NK\_Enabling\_  
Russian\_Missile\_Strikes\_Against\_Ukraine.pdf.   
14   
See, for example, Brian Spegele, “The Chinese Satellite Firm Washington Accuses of   
Helping U.S. Foes,” Wall Street Journal, April 26, 2025, https://www.wsj.com/world/  
china/the-chinese-satellite-firm-washington-accuses-of-helping-u-s-foes-b5e68d2e; and   
Sudarsan Raghavan, Saleh al-Batati, and Benoit Faucon, “U.S. Accuses China of Helping   
the Houthis Target Their Attacks,” Wall Street Journal, April 18, 2025, https://www.wsj.  
com/world/middle-east/u-s-accuses-china-of-helping-the-houthis-target-their-attacks-  
e56264da.   
15   
Christy Lee, “Analysts: Russia–North Korea Military Ties Pose Dilemma for China,”   
Voice of America, February 1, 2024, https://www.voanews.com/a/analysts-russia-north-  
korea-military-ties-pose-dilemma-for-china/7467749.html; and Lingling Wei, Ann M.   
Simmons, and Timothy W. Martin, “Behind Putin Visit, Unease in Beijing over His   
Potential Next Stop: North Korea,” Wall Street Journal, May 19, 2024, https://www.wsj.  
com/world/behind-putin-visit-unease-in-beijing-over-his-potential-next-stop-north-  
korea-28b82cf5.   
16   
Bruce W. Bennett, “North Korea and China Aren’t the Allies You Think They   
Are,” RAND, Commentary, September 27, 2023, https://www.rand.org/pubs/  
commentary/2023/09/north-korea-and-china-arent-the-allies-you-think-they.html.   
17   
Reuters, “China Maintains Stance on Disputed Gulf Islands Despite Iran’s Anger,”   
Reuters, June 3, 2024, https://www.reuters.com/world/china-maintains-stance-  
disputed-gulf-islands-despite-irans-anger-2024-06-03/; Associated Press, “Iran   
Summons Russian Envoy over Statement on Persian Gulf Disputed Islands,” Reuters,   
December 24, 2023, https://www.voanews.com/a/iran-summons-russian-envoy-over-  
statement-on-persian-gulf-disputed-islands-/7410524.html; and Tala Taslimi, “Iran   
Grows Wary of Russia amid Moscow’s Support for UAE in Island Spat,” Nikkei Asia, July   
23, 2023, https://asia.nikkei.com/Politics/International-relations/Iran-grows-wary-of-  
Russia-amid-Moscow-s-support-for-UAE-in-island-spat.   
18   
Stephen M. Walt, The Origins of Alliances (Ithaca: Cornell University Press, 1987), 17–49.   
Also see John J. Mearsheimer, The Tragedy of Great Power Politics (New York: W. W.   
Norton, 2001), 48, 156, 269.  
19   
As used here, “ideologies” refers to the principles of governance to which   
policymakers are dedicated, including the core institutional, economic, or social goals   
they attempt to implement in their countries. Examples include whether leaders   
support authoritarian or democratic political institutions, capitalist or socialist

**Page 170**

164  
A Report of the CSIS Defense and Security Department  
economic systems, or religious or secular values. See, for example, Mark L. Haas,   
“When Do Ideological Enemies Ally?,” International Security 46, no. 1 (Summer 2021):   
104–46, https://doi.org/10.1162/isec\_a\_00413.  
20   
Hans J. Morgenthau, Politics Among Nations: The Struggle for Power and Peace, Fourth   
Edition (New York: Alfred A. Knopf, 1967), 177–78.   
21   
See, for example, Kenneth N. Waltz, Man, the State, and War: A Theoretical Analysis   
(New York: Columbia University Press, 2001).  
22   
Christopher S. Chivvis and Jack Keating, “How Evil? Deconstructing the New Russia–  
China–Iran–North Korea Axis,” Survival 66, no. 6 (December 2024): 51–66, https://doi.  
org/10.1080/00396338.2024.2432198.  
23   
See, for example, Walt, Origins.  
24   
Mathew George et al., Trends in International Arms Transfers, 2024 (Stockholm: SIPRI,   
March 2025), 7, https://www.sipri.org/sites/default/files/2025-03/fs\_2503\_at\_2024\_0.pdf.   
25   
Derek Solen, The Truth About the Sino-Russian Combined Patrols (Tokyo: JASDF Air   
and Space Institute, July 2025), https://www.mod.go.jp/asdf/meguro/center/Eimg/  
EJASIreport20250630.pdf.  
26   
“Iran, Russia, China Conduct Joint Naval Drills in Gulf of Oman,” Al Jazeera, March 12,   
2025, https://www.aljazeera.com/news/2025/3/12/iran-russia-china-conduct-joint-  
naval-drills-in-gulf-of-oman.   
27   
Brian G. Carlson, “The Growing Significance of China-Russia Defense Cooperation,”   
Strategic Studies Institute, U.S. Army War College, September 18, 2024, https://ssi.  
armywarcollege.edu/SSI-Media/Recent-Publications/Display/Article/3908561/the-  
growing-significance-of-china-russia-defense-cooperation/.   
28   
Antoni Slodkowski and Laurie Chen, “China’s Xi Affirms ‘No Limits’ Partnership with   
Putin in Call on Ukraine War Anniversary,” Reuters, February 24, 2025, https://www.  
reuters.com/world/xi-putin-hold-phone-call-ukraine-war-anniversary-state-media-  
says-2025-02-24/.   
29   
“Iran and China Sign 25-Year Cooperation Agreement,” Reuters, March 27, 2021,   
https://www.reuters.com/world/china/iran-china-sign-25-year-cooperation-  
agreement-2021-03-27/.   
30   
Hyonhee Shin, “Key Points of North Korea, Russia Landmark Strategic Partnership   
Treaty,” Reuters, June 20, 2024, https://www.reuters.com/world/asia-pacific/key-  
points-north-korea-russia-landmark-strategic-partnership-treaty-2024-06-20/.   
31   
“Treaty on the Comprehensive Strategic Partnership between the Islamic Republic of   
Iran and the Russian Federation,” President of the Islamic Republic of Iran, January 17,   
2025, https://president.ir/en/156874.   
32   
Marc Santora, “With Drones and North Korean Troops, Russia Pushes Back Ukraine’s   
Offensive,” New York Times, March 8, 2025, https://www.nytimes.com/2025/03/08/  
world/europe/ukraine-russia-north-korea-kursk.html; and Lex Harvey, “North Korea   
Has Sent 3,000 More Soldiers to Bolster Russia’s War on Ukraine, South Korea Says,”   
CNN, March 27, 2025, https://www.cnn.com/2025/03/27/europe/north-korea-russia-  
ukraine-soldiers-intl-hnk.   
33   
Stephen Hadley, “Xi Jinping’s Axis of Losers,” Foreign Affairs, November 1, 2024,   
https://www.foreignaffairs.com/china/xi-jinpings-axis-losers.   
34   
As used here, an alliance is a formal or informal relationship of security cooperation   
between two or more sovereign states. This definition assumes some level of   
commitment and an exchange of benefits for the parties; severing the relationship or   
failing to honor the agreement would presumably cost something. Walt, Origins, 1.  
35   
Morgenthau, Politics, 177. Another potential example is the Treaty of the Arab League of   
1945.  
36   
See, for example, Director of Central Intelligence, Eastern Europe and the Warsaw

**Page 171**

165  
War and the Modern Battlefield  
Pact, National Intelligence Estimate No. 12-65 (Washington, DC: CIA, August 26, 1965),   
https://www.cia.gov/readingroom/docs/DOC\_0000273191.pdf; and Joan Bird and   
John Bird, eds., CIA Analysis of the Warsaw Pact Forces: The Importance of Clandestine   
Reporting (Langley, VA: CIA, 2012), https://www.cia.gov/static/CIA-Analysis-of-the-  
Warsaw-Pact-Forces-The-Importance-of-Clandestine-Reporting.pdf.   
37   
Fenella McGerty and Karl Dewey, “Global Defense Spending Soars to New High,”   
Military Balance Blog, International Institute for Strategic Studies, February 12,   
2025, https://www.iiss.org/online-analysis/military-balance/2025/02/global-defence-  
spending-soars-to-new-high/.  
38   
“How Much Will Rising Defense Spending Boost Europe’s Economy?,” Goldman Sachs,   
March 6, 2025, https://www.goldmansachs.com/insights/articles/how-much-will-rising-  
defense-spending-boost-europes-economy.  
39   
Mark Rutte, “Building a Better NATO,” NATO, June 9, 2025, https://www.nato.int/cps/  
en/natohq/opinions\_235867.htm.  
40 McGerty and Dewey, “Global Defense Spending Soars to New High.”  
41   
Andrea Kendall-Taylor and Richard Fontaine, “The Axis of Upheaval: How America’s   
Adversaries Are Uniting to Overturn the Global Order,” Foreign Affairs 103, no. 3 (May/  
June 2024), 50–63, https://www.foreignaffairs.com/china/axis-upheaval-russia-iran-  
north-korea-taylor-fontaine.   
42   
See, for example, David S. Cloud and Aresu Eqbali, “Iran’s Supreme Leader Ali   
Khamenei Emerges in Public amid Health Speculation,” Wall Street Journal, September   
17, 2022, https://www.wsj.com/articles/irans-supreme-leader-ali-khamenei-emerges-in-  
public-amid-health-speculation-11663414072.   
43   
RAND, Commission on the National Defense Strategy (Santa Monica, CA: RAND, July   
2024), vii, https://www.rand.org/nsrd/projects/NDS-commission.html; Raphael S.   
Cohen, The History and Politics of Defense Reviews (Santa Monica, CA: RAND, April   
2018), https://www.rand.org/pubs/research\_reports/RR2278.html.  
44   
U.S. Department of Defense, “Sustaining U.S. Global Leadership: Priorities for 21st   
Century Defense,” January 2012, 4, https://apps.dtic.mil/sti/pdfs/ADA554328.pdf.  
WILL, COHESION, RESILIENCE, AND THE WARS OF THE FUTURE  
1   
Carl von Clausewitz, On War (London: Penguin Group, 2003).  
2   
Shelby Butt and Daniel Byman, “Right-wing extremism: the Russian   
connection,=” Survival 62, no. 2 (April-May 2020), 137–151, https://www.tandfonline.  
com/toc/tsur20/62/2.  
3   
Dmytro Basmat, “Over 45,000 Ukrainian Soldiers Killed Since Start of War, Zelensky   
Says,” Kyiv Independent, February 5, 2025, https://kyivindependent.com/over-45-  
000-ukrainian-soldiers-killed-since-start-of-war-zelensky-says/; Bojan Pancevski,   
“One Million Are Now Dead or Injured in the Russia-Ukraine War,” Wall Street Journal,   
September 17, 2024, https://www.wsj.com/world/one-million-are-now-dead-or-injured-  
in-the-russia-ukraine-war-b09d04e5; and Anatoly Kurmanaev and Constant Meheut,   
“Ukraine Is Losing Fewer Soldiers Than Russia—but It’s Still Losing the War,” New York   
Times, January 23, 2025, https://www.nytimes.com/2025/01/23/world/europe/ukraine-  
russia-soldiers-loss.html.   
4   
“Number of Civilian Casualties in Ukraine During Russia’s Invasion Verified by OHCHR   
from February 24, 2022 to March 31, 2025,” Statista, April 11, 2025, https://www.statista.  
com/statistics/1293492/ukraine-war-casualties/.  
5   
Jyri Raitasalo, “Finnish Defense ‘Left of Bang’,” PRISM 10, no. 2 (March 10, 2023): 86,   
https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323915/finnish-  
defense-left-of-bang/.   
6   
Seth G. Jones, “Russia’s Shadow War Against the West,” CSIS, CSIS Briefs, March 18,   
2025, https://www.csis.org/analysis/russias-shadow-war-against-west.

**Page 172**

166  
A Report of the CSIS Defense and Security Department  
7   
Jakub Przetacznik and Linda Tothova, Russia’s War on Ukraine: Military Balance of   
Power (Brussels: European Parliamentary Research Service, March 2022), 1, https://  
www.europarl.europa.eu/RegData/etudes/ATAG/2022/729292/EPRS\_ATA(2022)729292\_  
EN.pdf; Constantine Atlamazoglou, “After a Year of Heavy Losses, Ukraine’s Military Is   
Juggling a ‘Very Uneven’ Force as It Prepares for Major Fighting, Expert Says,” Business   
Insider, April 28, 2023, https://www.businessinsider.com/ukraines-military-balances-  
uneven-training-levels-after-year-of-war-2023-4; and “Ukraine War Latest: Ukraine’s   
Military Now Totals 880,000 Soldiers, Facing 600,000 Russian Troops, Kyiv Claims,”   
Kyiv Independent, January 15, 2025, https://kyivindependent.com/ukraine-war-latest-  
ukraines-military-now-totals-880-000-soldiers-facing-600-000-russian-troops-kyiv-  
claims/.  
8   
Jennifer Hassan and Adam Taylor, “Israel’s Massive Mobilization of 360,000 Reservists   
Upends Lives,” Washington Post, October 10, 2023, https://www.washingtonpost.  
com/world/2023/10/10/israel-military-draft-reservists/; and Joel Gunter, “‘A Lot of   
Adrenaline, A Lot of Unknowns’: Reservists Flock to Join Israel’s Fight,” BBC, October   
10, 2023, https://www.bbc.com/news/world-middle-east-67067595.   
9   
Hassan and Taylor, “Israel’s Massive Mobilization.”  
10   
Gunter, “‘A Lot of Adrenaline’”; and Dan Williams, “Israel to Pull Some Troops from   
Gaza as War Enters New Phase,” Reuters, January 1, 2024, https://www.reuters.com/  
world/middle-east/israel-pull-some-troops-gaza-war-enters-new-phase-2024-01-01/.   
11   
Bar Peleg, “Third of Israeli Reservists Have Served More Than 150 Days Since War’s   
Start,” Haaretz, November 8, 2024, https://www.haaretz.com/israel-news/2024-11-08/  
ty-article/.premium/third-of-israeli-reservists-have-served-more-than-150-days-since-  
wars-start/00000193-0b6d-d599-a7f7-0b7f0a960000.   
12   
 “Ukraine Deploys over One Million Drones in Active Support of Its Forces Since 2022,”   
lobal Defense News, December 19, 2024, https://armyrecognition.com/focus-analysis-  
conflicts/army/analysis-defense-and-security-industry/ukraine-deploys-over-one-  
million-drones-in-active-support-of-its-forces-since-2022.   
13   
“Ukraine Can and Will Create the Best Weapons—President’s Speech at the Second   
International Defense Industries Forum,” President of Ukraine, October 1, 2024,   
https://www.president.gov.ua/en/news/ukrayina-mozhe-j-bude-stvoryuvati-najkrashi-  
zrazki-zbroyi-vi-93613.   
14   
Graeme Baker, “Ukraine Claims Drone Strike on Russian Oil Refinery,” BBC, January 24,   
2025, https://www.bbc.com/news/articles/cvg84r5g8d0o.   
15   
Emily Rose, “Israeli Startups Make Global Plans After Key Role in War,” Reuters,   
January 31, 2025, https://www.reuters.com/world/middle-east/israeli-startups-make-  
global-plans-after-key-role-war-2025-01-31/.   
16   
Ibid.  
17   
Ibid.  
18   
Raphael S. Cohen, “Israel’s ‘People’s Army’ at War,” Foreign Policy, January 13, 2024,   
https://foreignpolicy.com/2024/01/13/israel-hamas-war-gaza-idf-october-7-military/.   
19   
Steven Scheer, “Israeli Tech Sector Resilient but Faces Funding Uncertainty amid   
War with Hamas,” Reuters, September 23, 2024, https://www.reuters.com/world/  
middle-east/israeli-tech-sector-resilient-faces-funding-uncertainty-amid-war-with-  
hamas-2024-09-23/.   
20   
David E. Sanger, Julian E. Barnes, and Kate Conger, “As Tanks Rolled into Ukraine, So   
Did Malware. Then Microsoft Entered the War,” New York Times, February 28, 2022,   
https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.   
21   
Nate Ostiller, “Minister: Microsoft to Provide Free Cloud Services to Ukrainian   
Government for Another Year,” Kyiv Independent, November 29, 2023, https://  
kyivindependent.com/minister-microsoft-to-provide-free-cloud-services-to-ukrainian-  
government-for-another-year/.

**Page 173**

167  
War and the Modern Battlefield  
22   
Keren Setton, “Despite Constant Rocket Threat, Many Israelis Remain Without   
Shelters,” Jerusalem Post, May 19, 2023, https://www.jpost.com/israel-news/  
article-743572.   
23   
Yahya Abou-Ghazala, “In Gaza, Palestinians Have No Safe Place from Israel’s Bombs,”   
CNN, October 12, 2023, https://www.cnn.com/2023/10/12/middleeast/gaza-airstrikes-  
warnings-invs/index.html.   
24   
International Criminal Court, “Situation in the State of Palestine: ICC Pre-Trial   
Chamber I Rejects the State of Israel’s Challenges to Jurisdiction and Issues Warrants of   
Arrest for Benjamin Netanyahu and Yoav Gallant,” press release, November 21, 2024,   
https://www.icc-cpi.int/news/situation-state-palestine-icc-pre-trial-chamber-i-rejects-  
state-israels-challenges.   
25   
Anna Gordon, “New Polling Shows How Much Global Support Israel Has Lost,” Time,   
January 17, 2024, https://time.com/6559293/morning-consult-israel-global-opinion/.   
26   
Jeffrey M. Jones, “Majority in U.S. Now Disapprove of Israeli Action in Gaza,” Gallup,   
March 27, 2024, https://news.gallup.com/poll/642695/majority-disapprove-israeli-  
action-gaza.aspx; and Laura Silver, “Younger Americans Stand Out in Their Views of   
the Israel-Hamas War,” Pew Research Center, April 2, 2024, https://www.pewresearch.  
org/short-reads/2024/04/02/younger-americans-stand-out-in-their-views-of-the-israel-  
hamas-war/.   
27   
Silver, “Younger Americans.”  
28   
Brandon Boatwright, “How Ukraine’s Savvy Official Social Media Rallied the World and   
Raised the Bar for National Propaganda,” Clemson News, August 18, 2023, https://news.  
clemson.edu/how-ukraines-savvy-official-social-media-rallied-the-world-and-raised-  
the-bar-for-national-propaganda/.   
29   
“General Assembly Holds Emergency Special Session on Ukraine,” UN News, February   
28, 2022, https://news.un.org/en/story/2022/02/1112912; and “General Assembly   
Overwhelmingly Adopts Resolution Demanding Russian Federation Immediately End   
Illegal Use of Force in Ukraine, Withdraw All Troops,” United Nations, March 2, 2022,   
https://press.un.org/en/2022/ga12407.doc.htm.   
30   
Mary Blankenship and Aloysius Uche Ordu, “Russia’s Narratives About Its Invasion of   
Ukraine Are Lingering in Africa,” Brookings, June 27, 2022, https://www.brookings.edu/  
articles/russias-narratives-about-its-invasion-of-ukraine-are-lingering-in-africa/.   
31   
“Mapping a Surge of Disinformation in Africa,” Africa Center for Strategic Studies,   
March 13, 2024, https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-  
in-africa/.   
32   
Charles Millon, “Russia Will Unleash Chaos in the Sahel,” GIS Reports, March 29, 2024,   
https://www.gisreportsonline.com/r/russia-africa-propaganda/.   
33   
Mari Saito et al., “Russia-Linked Propaganda Campaign Pushes to Undercut German   
Support for Ukraine,” Reuters, February 18, 2025, https://www.reuters.com/  
investigations/russia-linked-propaganda-campaign-pushes-undercut-german-support-  
ukraine-2025-02-18/.   
34   
Jamie Dettmer, “Netanyahu Trapped by Clashing Demands from War Cabinet and   
Hawks,” Politico, January 21, 2024, https://www.politico.eu/article/israel-prime-  
minister-benjamin-netanyahu-trapped-clash-demands-war-gaza-palestine-cabinet-  
hawks/.   
35   
Jaroslav Lukiv, “Israeli Ministers Threaten to Quit over Ceasefire Plan,” BBC, June 2,   
2024, https://www.bbc.com/news/articles/cz55y6k0p5go.   
36   
Jim Garamone, “Russian Forces Invading Ukraine Suffer Low Morale,” U.S. Department   
of Defense, March 23, 2022, https://www.defense.gov/news/news-stories/article/  
article/2975508/russian-forces-invading-ukraine-suffer-low-morale/.   
37   
Roberto Foa and Roula Nezi, Piercing the Fog of War: Measuring Russian Public Opinion   
via Online Search Data (Cambridge, UK: Bennett Institute for Public Policy, April 2023),

**Page 174**

168  
A Report of the CSIS Defense and Security Department  
3, https://www.bennettinstitute.cam.ac.uk/publications/piercing-the-fog-of-war/.   
38   
Adam Rasgon, “Hamas After Cease-Fire: Weakened, Isolated but Still Standing,” New   
York Times, January 17, 2025, https://www.nytimes.com/2025/01/16/world/middleeast/  
hamas-gaza-cease-fire-palestinian-future.html.   
RETURNING TO AN ERA OF COMPETITION AND NUCLEAR RISK  
1   
Heather Williams et al., “Deter and Divide: Russia’s Nuclear Rhetoric and Escalation   
Risks in Ukraine,” CSIS, January 11, 2024, https://features.csis.org/deter-and-divide-  
russia-nuclear-rhetoric/.   
2   
U.S. Department of Defense, Military and Security Developments Involving the People’s   
Republic of China 2024 (Washington, DC: Department of Defense, 2024), https://  
media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-  
DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF; and   
Chris Andrews and Justin Anderson, China’s Theater-Range, Dual-Capable Delivery   
Systems: Integrated Deterrence and Risk Reduction Approaches to Counter a Growing   
Threat (Washington, DC: NDU INSS Center for the Study of WMD, August 2024), https://  
inss.ndu.edu/Portals/82/HDTRA1344728\_NDU%20INSS%20CSWMD\_TECREP\_unclass\_  
Final.pdf.   
3   
Lolita C. Baldor and Didi Tang, “Chinese and Russian Bombers Patrolling off Alaska   
Raise Concerns About Growing Military Cooperation,” Associated Press, July 25, 2024,   
https://apnews.com/article/china-russia-us-military-planes-norad-alaska-4994b489e  
75ae636b4a4cd5bb40f91ac; Jonathan Tirone, “China’s Imports of Russian Uranium   
Spark Fear of New Arms Race,” Bloomberg News, February 28, 2023, https://www.  
bloomberg.com/news/articles/2023-03-01/china-nuclear-trade-with-russia-risks-  
tipping-military-balance; and “Security Council Fails to Extend Mandate for Expert   
Panel Assisting Sanctions Committee on Democratic People’s Republic of Korea,”   
United Nations, March 28, 2024, https://press.un.org/en/2024/sc15648.doc.htm.   
4   
 Joseph Ataman and Jessie Yeung, “France to Consider Protecting European Allies   
ith Its Nuclear Arsenal, Macron Says,” CNN, March 6, 2025, https://www.cnn.  
com/2025/03/05/europe/macron-france-nuclear-arsenal-ukraine-intl-hnk/index.html.   
5   
“Poland’s Leader Says His Country Is Ready to Host NATO Members’ Nuclear Weapons   
to Counter Russia,” Associated Press, April 22, 2024, https://apnews.com/article/  
poland-nuclear-weapons-nato-russia-ukraine-d92c508d6ff53683a25f1bc62d256f86.   
6   
Kyu-Jin Shin, “72.8% of Koreans Support S. Korea’s Nuclear Weapon   
Development,” Dong-A Ilbo, February 6, 2024, https://www.donga.com/en/article/  
all/20240206/4731163/1.   
7   
William Burr, ed., “Preoccupations with West Germany’s Nuclear Weapons Potential   
Shaped Kennedy-Era Diplomacy,” National Security Archive, George Washington   
University, February 2, 2018, https://nsarchive.gwu.edu/briefing-book/nuclear-  
vault/2018-02-02/german-nuclear-question-nonproliferation-treaty; and William   
Burr, ed., “The U.S. Nuclear Presence in Western Europe, 1954–1962, Part I,” National   
Security Archive, George Washington University, July 21, 2020, https://nsarchive.  
gwu.edu/briefing-book/nuclear-vault/2020-07-21/us-nuclear-presence-western-  
europe-1954-1962.   
8   
W. J. Hennigan, “The Price,” New York Times, October 10, 2024, https://www.nytimes.  
com/interactive/2024/10/10/opinion/nuclear-weapons-us-price.html.   
9   
U.S. Department of Defense, Military and Security Developments Involving the People’s   
Republic of China 2024.   
10   
Williams et al., “Deter and Divide.”  
11   
Heather Williams, “What Trump’s Submarine Threat and Russia’s INF Exit Really   
Mean,” CSIS, Commentary, August 7, 2025, https://www.csis.org/analysis/what-trumps-  
submarine-threat-and-russias-inf-exit-really-mean.  
12   
Yoonjung Seo and Lex Harvey, “North Korea’s Kim Jong Un Threatens to Destroy the

**Page 175**

169  
War and the Modern Battlefield  
South with Nuclear Weapons If Provoked,” CNN, October 4, 2024, https://www.cnn.  
com/2024/10/04/asia/north-korea-kim-jong-un-nuclear-weapons-intl-hnk/index.html.   
13   
James H. Anderson, “The Next Taiwan Crisis Will (Almost) Certainly Involve Nuclear   
Threats,” U.S. Naval Institute, Proceedings 150, no. 3 (March 2024), https://www.usni.  
org/magazines/proceedings/2024/march/next-taiwan-crisis-will-almost-certainly-  
involve-nuclear-threats.   
14   
Office of the Director of National Intelligence, Annual Threat Assessment of the U.S.   
Intelligence Community (Washington, DC: Office of the Director of National Intelligence,   
February 2023), 14, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-  
Unclassified-Report.pdf.   
15   
Andrews and Anderson, China’s Theater-Range, 4.  
16   
ODNI, Annual Threat Assessment, 21.  
17   
Björn Hagelin, “Swords into Daggers: The Origins of the SS-20 Missiles,” Bulletin of   
Peace Proposals 15, no. 4 (1984): 341–53, https://www.jstor.org/stable/44481156.   
18   
“Special Meeting of Foreign and Defence Ministers (The ‘Double-Track’ Decision on   
Theatre Nuclear Forces) Chairman: Mr. J. Luns,” NATO, December 12, 1979, https://  
www.nato.int/cps/en/natolive/official\_texts\_27040.htm.   
19   
“Treaty Between the United States of America and the Union of Soviet Socialist   
Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles   
(INF Treaty),” U.S. Department of State, December 8, 1987, https://2009-2017.state.  
gov/t/avc/trty/102360.htm.   
20   
U.S. Naval Institute Staff, “Report to Congress on Nuclear-Armed Sea-Launched Cruise   
Missile,” USNI News, October 18, 2024, https://news.usni.org/2024/10/18/report-to-  
congress-on-nuclear-armed-sea-launched-cruise-missile.   
21   
Office of the Spokesperson, “Russia’s Violation of the Intermediate-Range Nuclear   
Forces (INF) Treaty,” U.S. Department of State, December 4, 2018, https://2017-2021.  
state.gov/russias-violation-of-the-intermediate-range-nuclear-forces-inf-treaty/.   
22   
Sydney J. Freedberg Jr., “Sub-Launched Nuclear Cruise Missile Will Need ‘An Entirely   
New Industrial Base,’ Warns Navy Admiral,” Breaking Defense, November 15, 2024,   
https://breakingdefense.com/2024/11/sub-launched-nuclear-cruise-missile-will-need-  
an-entirely-new-industrial-base-warns-navy-admiral/.   
23   
DOD, Military and Security, 107.  
24   
Dzirhan Mahadzir, “Joint Russian, Chinese Pacific Bomber Flight Prompts Japan and   
South Korea to Scramble Fighters,” U.S. Naval Institute, December 1, 2024, https://  
news.usni.org/2024/11/29/joint-russian-chinese-pacific-bomber-flight-prompts-japan-  
and-south-korea-to-scramble-fighters.   
25   
Helen Regan et al., “Blinken Warns Russia Is Close to Sharing Advanced Satellite   
Technology with North Korea,” CNN, January 6, 2025, https://www.cnn.  
com/2025/01/06/asia/blinken-russia-satellite-technology-north-korea-intl-hnk.   
26   
Dan Sabbagh, “Alarm in UK and US over Possible Iran-Russia Nuclear Deal,” The   
Guardian, September 14, 2024, https://www.theguardian.com/politics/2024/sep/14/  
alarm-in-uk-and-us-over-possible-iran-russia-nuclear-deal.   
27   
John Lewis Gaddis, Strategies of Containment: A Critical Appraisal of American National   
Security Policy During the Cold War (New York: Oxford University Press, 2005), 100.  
28   
Neal H. Petersen et al., ed., Foreign Relations of the United States, 1950, vol. 1, National   
Security Affairs; Foreign Economic Policy (Washington, DC: Government Publishing   
Office, 1977), Document 85.   
29   
Richard L. Kugler, Laying the Foundations: The Evolution of NATO in the 1950s (Santa   
Monica, CA: RAND, 1990), 75, https://www.rand.org/pubs/notes/N3105.html.   
30   
Francis P. Sempa, “Is Kissinger’s Triangular Diplomacy the Answer to Sino-Russian

**Page 176**

170  
A Report of the CSIS Defense and Security Department  
Rapprochement?,” The Diplomat, August 2, 2016, https://thediplomat.com/2016/08/  
is-kissingers-triangular-diplomacy-the-answer-to-sino-russian-rapprochement/.   
31   
Jaroslaw Adamowski, “Polish President Wants NATO Nukes for Deterring   
Russia,” Defense News, April 22, 2024, https://www.defensenews.com/global/  
europe/2024/04/22/polish-president-wants-nato-nukes-for-deterring-russia/.   
32   
Choe Sang-Hun, “Doubting America’s ‘Nuclear Umbrella,’ Some South Koreans Want   
their Own,” New York Times, August 19, 2024, https://www.nytimes.com/2024/08/17/  
world/asia/south-korea-nuclear-arsenal.html.   
33   
Aurelien Breeden, “France Open to Discussing Extension of Nuclear Deterrence,   
Macron Says,” New York Times, March 5, 2025, https://www.nytimes.com/2025/03/05/  
world/europe/france-nuclear-europe.html.   
34   
In 1957, West German Defense Minister Franz Josef Strauss stated that West Germany   
“too must be so equipped” with nuclear weapons to ensure its security. Marc   
Trachtenberg, History and Strategy (Princeton, NJ: Princeton University Press, 1991),   
182–83.   
35   
Burr, “U.S. Nuclear Presence.”  
36   
This solution also reflected a desire, which Eisenhower articulated even before 1957, to   
create “a third great power bloc” in Western Europe. Trachtenberg, History, 186.  
37   
Doreen Horschig and Heather Williams, “The Crumbling Nuclear Order: How to Save   
the Norms Against Testing, Building, and Using the Ultimate Weapon,” Foreign Affairs,   
September 16, 2024, https://www.foreignaffairs.com/china/crumbling-nuclear-order.   
38   
Williams et al., “Deter and Divide.”  
OPERATIONAL ART IN THE AGE OF BATTLE NETWORKS  
1   
Hugo Bachega and James Gregory, “‘Massive’ Drone Attack on Black Sea Fleet—Russia,”   
BBC News, October 29, 2022, https://www.bbc.com/news/world-europe-63437212;   
Mariano Zafra and Jon McClure, “Sea Drones and the Counteroffensive in Crimea,”   
Reuters, July 17, 2023, https://www.reuters.com/graphics/UKRAINE-CRISIS/CRIMEA/  
gdvzwrmrlpw/; and H. I. Sutton, “Uncrewed Platforms Have Been Critical to Ukraine’s   
Success in the Black Sea,” Royal United Services Institute, April 20, 2024, https://www.  
rusi.org/explore-our-research/publications/commentary/uncrewed-platforms-have-  
been-critical-ukraines-success-black-sea.   
2   
Sean J. A. Edwards, Swarming on the Battlefield: Past, Present, and Future (Santa Monica,   
CA: RAND, 2000), https://doi.org/10.7249/MR1100; and John Arquilla and David F.   
Ronfeldt, Swarming and the Future of Conflict (Santa Monica, CA: RAND, 2000), https://  
www.rand.org/pubs/documented\_briefings/DB311.html.   
3   
Benjamin Jensen, “Operational Art for the Replicator Initiative: Confessions of a   
Swarming Addict,” War on the Rocks, October 25, 2023, https://warontherocks.  
com/2023/10/operational-art-for-the-replicator-initiative-confessions-of-a-swarming-  
addict/; Benjamin Jensen, “Bringing the Swarm to Life: Roles, Missions, and   
Campaigns for the Replicator Initiative,” War on the Rocks, February 13, 2024,   
https://warontherocks.com/2024/02/bringing-the-swarm-to-life-roles-missions-and-  
campaigns-for-the-replicator-initiative/; Benjamin Jensen and John Paschkewitz,   
“Mosaic Warfare: Small and Scalable Are Beautiful,” War on the Rocks, December   
23, 2019, http://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-  
are-beautiful/; and Bryan Clark, Dan Patt, and Harrison Schramm, Mosaic Warfare:   
Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-  
Centric Operations (Washington, DC: CSBA, 2020), https://csbaonline.org/research/  
publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-  
systems-to-implement-decision-centric-operations.   
4   
Benjamin M. Jensen, Christopher Whyte, and Scott Cuomo, Information in War:   
Military Innovation, Battle Networks, and the Future of Artificial Intelligence (Washington,   
DC: Georgetown University Press, 2022); Todd Harrison, “Battle Networks and the

**Page 177**

171  
War and the Modern Battlefield  
Future Force: Part 1: A Framework for Debate,” CSIS, CSIS Briefs, August 5, 2021, https://  
www.csis.org/analysis/battle-networks-and-future-force; and John Stillion and Bryan   
Clark, What It Takes to Win: Succeeding in 21st Century Battle Network Competitions   
(Washington, DC: CSBA, 2015), https://csbaonline.org/research/publications/what-it-  
takes-to-win-succeeding-in-21st-century-battle-network-competitions.  
5   
Carl von Clausewitz, On War, ed. Michael Howard and Peter Paret (Princeton, NJ:   
Princeton University Press, 2008), https://doi.org/10.1515/9781400837403; William   
H. McNeill, The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000   
(Chicago: University of Chicago Press, 1993), 7; and Azar Gat, A History of Military   
Thought: From the Enlightenment to the Cold War (Oxford, UK: Oxford University Press,   
2001).  
6   
Paul R. Norwood, Benjamin M. Jensen, and Justin Barnes, “Capturing the Character of   
Future War,” Parameters 46, no. 2 (June 1, 2016): 81–91, https://doi.org/10.55540/0031-  
1723.2922. On operational art, see U.S. Department of the Army, ADP 3-0: Operations   
(Washington, DC: Department of the Army, July 2019), https://armypubs.army.mil/  
epubs/DR\_pubs/DR\_a/ARN18010-ADP\_3-0-000-WEB-2.pdf; Chairman of the Joint   
Chiefs of Staff, Joint Publication 3-0: Joint Campaigns and Operations (Arlington, VA:   
Joint Chiefs of Staff, 2022), https://www.benning.army.mil/mssp/security%20topics/  
Potential%20Adversaries/content/pdf/JP%203-0.pdf; Michael D. Krause and R. Cody   
Phillips, Historical Perspective of the Operational Art (Washington, DC: U.S. Army   
Center of Military History, 2005); Wilson C. Blythe Jr., “A History of Operational Art,”   
Military Review, November–December 2018, 37–49, https://www.armyupress.army.  
mil/Portals/7/military-review/Archives/English/ND-18/Blythe-Operational-Art.pdf;   
Georgii Samoilovich Isserson, The Evolution of Operational Art (Fort Leavenworth, KS:   
Combat Studies Institute Press, 2013), https://www.armyupress.army.mil/Portals/7/  
combat-studies-institute/csi-books/OperationalArt.pdf; Huba Wass de Czege, “Thinking   
and Acting Like an Early Explorer: Operational Art Is Not a Level of War,” Small Wars   
Journal, March 14, 2011, 4, http://smallwarsjournal.com/jrnl/art/operational-art-is-not-  
a-level-of-war; and Justin Kelly and Mike James Brennan, Alien: How Operational Art   
Devoured Strategy (Carlisle, PA: U.S. Army War College, September 2009), https://press.  
armywarcollege.edu/cgi/viewcontent.cgi?article=1619&context=monographs.   
7   
Gordon R. Sullivan and Michael V. Harper, Hope Is Not a Method: What Business Leaders   
Can Learn from America’s Army (New York: Broadway Books, 1997); Benjamin M.   
Jensen, Forging the Sword: Doctrinal Change in the U.S. Army (Stanford, CA: Stanford   
Security Studies, 2016); U.S. Department of the Army, Force XXI Operations: A Concept   
for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early   
Twenty-First Century, Tradoc Pamphlet 525-5 (Fort Monroe, VA: U.S. Army Training   
and Doctrine Command, August 1, 1994), https://apps.dtic.mil/sti/tr/pdf/ADA314276.  
pdf; Milan Vego, Recce-Strike Complexes in Soviet Theory and Practice, AD-A231 900   
(Fort Leavenworth, KS: Department of the Army, 1990), https://apps.dtic.mil/sti/tr/pdf/  
ADA231900.pdf; Andrew F. Krepinevich, The Origins of Victory: How Disruptive Military   
Innovation Determines the Fates of Great Powers (New Haven, CT: Yale University Press,   
2023); Michael J. Sterling, Soviet Reactions to NATO’s Emerging Technologies for Deep   
Attack, N-2294-AF (Santa Monica, CA: RAND, 1985), https://www.rand.org/pubs/notes/  
N2294.html; and Jensen et al., Information in War.  
8   
John Antal, Next War: Reimagining How We Fight (New York: Casemate Publishers,   
2023).  
9   
Jensen, Forging the Sword, 25.   
10   
Thomas R. Ryan Jr., “Warfighting: A Function of Combat Power,” Military Review,   
September–October 2022, 61–71, https://www.armyupress.army.mil/Journals/Military-  
Review/English-Edition-Archives/September-October-2022/Ryan/; Benjamin Jensen   
and Matthew Strohmeyer, “The Changing Character of Combined Arms,” War on the   
Rocks, May 23, 2022, https://warontherocks.com/2022/05/the-changing-character-of-  
combined-arms/; and Jeffrey R. Cares, An Information Age Combat Model (Newport, RI:   
Alidade, 2004), http://www.dodccrp.org/events/9th\_ICCRTS/CD/papers/166.pdf.  
11   
Stephen D. Biddle, Military Power: Explaining Victory and Defeat in Modern Battle   
(Princeton, NJ: Princeton University Press, 2006); Clint Reach, Vikram Kilambi, and

**Page 178**

172  
A Report of the CSIS Defense and Security Department  
Mark Cozad, Russian Assessments and Applications of the Correlation of Forces and Means   
(Santa Monica, CA: RAND, 2020), https://doi.org/10.7249/RR4235; Shawn Woodford,   
“How Does the U.S. Army Calculate Combat Power? ¯\\_(ツ)\_/¯,” The Dupuy Institute,   
December 7, 2017, https://dupuyinstitute.org/2017/12/07/how-does-the-u-s-army-  
calculate-combat-power-%c2%af\_%e3%83%84\_-%c2%af/; Ryan Vest, “Understanding   
Relative Combat Power Analysis: How Planners Can Make the Most of a Powerful Tool,”   
MOC Warfighter 1, no. 10 (May 2017): Article 3, https://digital-commons.usnwc.edu/  
moc-warfighter/vol1/iss10/3; Joshua M. Epstein, “The 3:1 Rule, the Adaptive Dynamic   
Model, and the Future of Security Studies,” International Security 13, no. 4 (Spring   
1989): 90–127, https://doi.org/10.2307/2538781; Joshua M. Epstein, The Calculus of   
Conventional War: Dynamic Analysis Without Lanchester Theory (Washington, DC:   
Brookings Institution Press, 1985); John J. Mearsheimer, “Assessing the Conventional   
Balance: The 3:1 Rule and Its Critics,” International Security 13, no. 4 (Spring 1989):   
54–89, https://doi.org/10.2307/2538780; John W. R. Lepingwell, “The Laws of Combat?   
Lanchester Reexamined,” International Security 12, no. 1 (Summer 1987): 89–134,   
https://doi.org/10.2307/2538918; Barry R. Posen, “Is NATO Decisively Outnumbered?,”   
International Security 12, no. 4 (Spring 1988): 186–202, https://doi.org/10.2307/2539002;   
and Trevor N. Dupuy, Analysis of Factors That Have Influenced Outcomes of Battles and   
Wars: A Data Base of Battles and Engagements, vol. 1, Main Report (Bethesda, MD: U.S.   
Army Concepts Analysis Agency, September 1984).  
12   
Michael C. Horowitz, “Battles of Precise Mass: Technology Is Remaking War—and   
America Must Adapt,” Foreign Affairs, October 22, 2024, https://www.foreignaffairs.  
com/world/battles-precise-mass-technology-war-horowitz.   
13   
This process is separate from neorealist theory and Waltz’s conceptualization of   
socialization by undifferentiated units in an anarchic system and from the English   
School’s definition of anarchical society. Rather, it conforms to the notion of   
epistemic communities, definitions of professions from sociology, and work on   
programmatic actors. See Kenneth Waltz, Theory of International Politics (Reading,   
MA: Addison-Wesley, 1979); João Resende-Santos, Neorealism, States, and the   
Modern Mass Army (New York: Cambridge University Press, 2007); Hedley Bull, The   
Anarchical Society: A Study of Order in World Politics (New York: Columbia University   
Press, 2002); Emanuel Adler, “The Emergence of Cooperation: National Epistemic   
Communities and the International Evolution of the Idea of Nuclear Arms Control,”   
International Organization 46, no. 1 (Winter 1992): 101–45, https://doi.org/10.1017/  
S0020818300001466; and Peter M. Haas, “Introduction: Epistemic Communities and   
International Policy Coordination,” International Organization 46, no. 1 (Winter 1992):   
1–35, https://doi.org/10.1017/S0020818300001442.   
14   
Harjeet Singh, The Kautilya Arthaśāstra: A Military Perspective (New Delhi: KW   
Publishers, 2013); R. Shamasastry, Kautilya’s Arthasastra (Mysore, India: Sri Raghuveer   
Printing Press, 1951), http://archive.org/details/in.gov.ignca.900; Sun Tzu, The Art   
of War, trans. Ralph Sawyer (New York: Basic Books, 1994); and Derek M. C. Yuen,   
Deciphering Sun Tzu: How to Read The Art of War (New York: Oxford University Press,   
2022).   
15   
Niccolò Machiavelli, Art of War (Chicago: University of Chicago Press, 2005).  
16   
Henri I. Rohan (Duc De), Capitaine (le parfait) ou abrégé des guerres, des commentaires de   
César (Paris: Legare Street Press, 2023); Patrick Speelman, Henry Lloyd and the Military   
Enlightenment of Eighteenth Century (London: Praeger, 2002); John L. Alger, The Quest   
for Victory: The History of the Principles of War (Ann Arbor: University of Michigan   
Press, 1982); and Azar Gat, The History of Military Thought: From the Enlightenment to   
the Cold War (New York: Oxford University Press, 2001).  
17   
J. F. C. Fuller, The Foundations of the Science of War (London: Hutchinson and Company,   
1926); and Alger, Quest for Victory.  
18   
Department of the Army, ADP 3-0: Operations, A-1–A-5.  
19   
Harrison, “Battle Networks”; Stillion and Clark, What It Takes; and Jensen et al.,   
Information in War. For additional explorations of how information changes warfare,   
see Jon R. Lindsay, Information Technology and Military Power, Cornell Studies in

**Page 179**

173  
War and the Modern Battlefield  
Security Affairs (Ithaca: Cornell University Press, 2020), and Jeremy Black, The Power   
of Knowledge: How Information and Technology Made the Modern World (New Haven, CT:   
Yale University Press, 2015).  
20   
U.S. Government Accountability Office, Defense Command and Control: Further Progress   
Hinges on Establishing a Comprehensive Framework, GAO-25-106454 (Washington,   
DC: GAO, April 2025), https://www.gao.gov/assets/gao-25-106454.pdf; and U.S.   
Department of Defense, Summary of the Joint All-Domain Command and Control   
(JADC2) Strategy (Washington, DC: DOD, March 2022), https://media.defense.gov/2022/  
Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-  
CONTROL-STRATEGY.pdf.   
21   
Christian Brose, The Kill Chain: Defending America in the Future of High-Tech Warfare   
(New York: Grand Central Publishing, 2022).  
22   
Stillion and Clark, What It Takes; ibid.; and Jensen and Paschkewitz, “Mosaic Warfare.”   
23   
China Aerospace Studies Institute, In Their Own Words: Science of Military Strategy   
2020 (Montgomery, AL: China Aerospace Studies Institute, January 2022), https://  
www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%20  
2020%20Science%20of%20Military%20Strategy.pdf; Dmitry (Dima) Adamsky,   
“Russian Lessons from the Syrian Operation and the Culture of Military Innovation,”   
George C. Marshall European Center for Security Studies, February 2020, https://www.  
marshallcenter.org/en/publications/security-insights/russian-lessons-syrian-operation-  
and-culture-military-innovation; and Randy Noorman, “The Russian Way of War in   
Ukraine: A Military Approach Nine Decades in the Making,” Modern War Institute,   
June 15, 2023, https://mwi.westpoint.edu/the-russian-way-of-war-in-ukraine-a-military-  
approach-nine-decades-in-the-making/. On military diffusion, see Michael Horowitz,   
The Diffusion of Military Power: Causes and Consequences for International Politics   
(Princeton, NJ: Princeton University Press, 2010).  
24   
Lester W. Grau and Charles K. Bartles, “The Russian Reconnaissance Fire Complex   
Comes of Age,” Changing Character of War Centre, May 30, 2018, https://www.ccw.  
ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age.   
25   
Delta COP is Ukraine’s digital command and control platform that integrates battlefield   
intelligence from drones, satellites, electronic intercepts, and frontline observers into   
a real-time situational awareness tool, enabling rapid targeting and decentralized   
decisionmaking across units. On Delta, see Kateryna Bondar, Does Ukraine Already   
Have Functional CJADC2 Technology? (Washington, DC: CSIS, December 2024), https://  
www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology.   
26   
 Thomas A. Walsh and Alexandra L. Huber, “A Symphony of Capabilities: How the Joint   
Warfighting Concept Guides Service Force Design,” Joint Force Quarterly, October 2023,   
4–15, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3568312/a-  
symphony-of-capabilities-how-the-joint-warfighting-concept-guides-service-for/.   
27   
Curt Taylor, “Preparing to Win the First Fight of the Next War,” Modern War Institute,   
February 23, 2024, https://mwi.westpoint.edu/preparing-to-win-the-first-fight-of-the-  
next-war/; Timothy J. Rizza and Michel Wyss, “Hider-Finder Competition, Deception,   
and Ground Manoeuvre on the ‘Transparent Battlefield’,” Defence Horizon Journal,   
February 20, 2025, https://tdhj.org/blog/post/deception-transparent-battlefield/;   
and David Barno and Nora Bensahel, “The Other Big Lessons That the U.S. Army   
Should Learn from Ukraine,” War on the Rocks, June 27, 2022, https://warontherocks.  
com/2022/06/the-other-big-lessons-that-the-u-s-army-should-learn-from-ukraine/. On   
diminishing marginal returns as an economic lens to analyze battles, see Jurgen Brauer   
and Hubert van Tuyll, Castles, Battles, and Bombs: How Economics Explains Military   
History (Chicago: University of Chicago Press, 2008).  
28   
Antal, Next War, 10.  
29   
Matthew Savill and Burcu Ozcelik, “Operation Days of Repentance: The Impact of   
Israel’s Strikes on Iran,” Royal United Services Institute, October 28, 2024, https://www.  
rusi.org/explore-our-research/publications/commentary/operation-days-repentance-  
impact-israels-strikes-iran; and Carrie Keller-Lynn, Rory Jones, and Dov Lieber, “How

**Page 180**

174  
A Report of the CSIS Defense and Security Department  
Israel Pulled Off Its Largest-Ever Strike on Iran,” Wall Street Journal, October 26, 2024,   
https://www.wsj.com/world/middle-east/how-israel-pulled-off-its-largest-ever-strike-  
on-iran-689022ca.   
30   
Thomas Newdick, “Israeli Strikes Knocked Out All of Iran’s S-300 Air Defense Systems:   
Officials,” The War Zone, October 28, 2024, https://www.twz.com/news-features/  
israeli-strikes-knocked-out-all-of-irans-s-300-air-defense-systems-officials.   
31   
Ronen Bergman, Mark Mazzetti, and Farnaz Fassihi, “Bomb Smuggled into Tehran   
Guesthouse Months Ago Killed Hamas Leader,” New York Times, August 1, 2024, https://  
www.nytimes.com/2024/08/01/world/middleeast/how-hamas-leader-haniyeh-killed-  
iran-bomb.html.   
32   
Wyatte Grantham-Philips, Michael Biesecker, Sarah El Deeb, and Sarah Parvini, “What   
to Know About the Two Waves of Deadly Explosions That Hit Lebanon and Syria,” AP   
News, September 19, 2024, https://apnews.com/article/lebanon-israel-hezbollah-pager-  
explosion-e9493409a0648b846fdcadffdb02d71e.   
33   
Newdick, “Israeli Strikes.”  
34   
Annika Ganzeveld, The Consequences of the IDF Strikes into Iran (Washington, DC:   
Institute for the Study of War, November 2024), https://www.understandingwar.org/  
backgrounder/consequences-idf-strikes-iran.   
THE EVOLUTION OF LANDPOWER  
1   
Oksana Torop and Svyatoslav Khomenko, “The Fight for Hostomel Airfield. How the   
Gates to Kyiv Stayed Locked,” The Best of BBC News Russian - in English (blog), February   
29, 2024, https://bbcrussian.substack.com/p/ukraine-war-the-fight-for-hostomel-  
airfield.  
2   
CPT Rick Chersicla, “What Free Men Can Do: The Winter War, the Use of Delay, and   
Lessons for the 21st Century,” Infantry Magazine (January–March 2017), https://www.  
benning.army.mil/infantry/magazine/issues/2017/JAN-MAR/pdf/Chersicla\_WinterWar.  
pdf.  
3   
Georgij S. Isserson, The Evolution of Operational Art, 2nd ed., trans. Bruce W. Menning   
(Fort Leavenworth, KS: Combat Studies Institute Press, 2013), https://www.armyupress.  
army.mil/Portals/7/combat-studies-institute/csi-books/OperationalArt.pdf; and Paul R.   
Norwood, Benjamin M. Jensen, and Justin Barnes, “Capturing the Character of Future   
War,” Parameters 46, no. 2 (June 2016), https://doi.org/10.55540/0031-1723.2922.  
4   
Jack D. Kem, ed., Deep Operations: Theoretical Approaches to Fighting Deep, The US   
Army Large-Scale Combat Operations Series (Fort Leavenworth, KS: Army University   
Press, 2021), https://www.armyupress.army.mil/Portals/7/combat-studies-institute/  
images/LSCO%20DeepOps%20book%20interactive%20with%20cover%20spread%20  
12Nov21.pdf.  
5   
John F. Schmitt, “Understanding Maneuver as the Basis for a Doctrine,” Marine Corps   
Association, August 1, 1990, https://www.mca-marines.org/gazette/understanding-  
maneuver-as-the-basis-for-a-doctrine/; Peter J. Vlakancic, “Marshal Tukhachevsky   
and the ‘Deep Battle’: An Analysis of Operational Level Soviet Tank and Mechanized   
Doctrine, 1935-1945,” Institute of Land Warfare, Land Warfare Paper no. 14, November   
1992, https://www.ausa.org/sites/default/files/LWP-14-Marshal-Tukhachevsky-and-  
the-Deep-Battle-An-Analysis-of-Operational-Level-Soviet-Tank-and-Mechanized-  
Doctrine-1935-1945.pdf; and Alex Danchev, “Liddell Hart and Manoeuvre,” RUSI Journal   
143, no. 6 (December 1998): 33–35, https://doi.org/10.1080/03071849808446325.  
6   
Benjamin M. Jensen, Forging the Sword: Doctrinal Change in the U.S. Army (Stanford,   
CA: Stanford University Press, 2016); Benjamin M. Jensen, Christopher Whyte,   
and Scott Cuomo, Information in War: Military Innovation, Battle Networks, and the   
Future of Artificial Intelligence (Washington, DC: Georgetown University Press, 2022);   
Department of the Army, “A Concept for the Evolution of Full-Dimensional Operations   
for the Strategic Army of the Early Twenty-First Century,” Force Operations: Tradoc   
Pamphlet 525-5, August 1, 1994; and Steven Metz and Raymond Millen, Future War/

**Page 181**

175  
War and the Modern Battlefield  
Future Battlespace: The Strategic Role of American Landpower (Carlisle, PA: U.S. Army   
War College Press, March 2003), https://press.armywarcollege.edu/cgi/viewcontent.  
cgi?article=1800&context=monographs.  
7   
Alexander Gale, “On Ukraine’s ‘Transparent Battlefield,’ There Are Few Places Left to   
Hide,” 19FortyFive, April 18, 2024, https://www.19fortyfive.com/2024/04/on-ukraines-  
transparent-battlefield-there-are-few-places-left-to-hide/; and Timothy J. Rizza and   
Michel Wyss, “Hider-Finder Competition, Deception, and Ground Manoeuvre on the   
‘Transparent Battlefield’,” Defence Horizon Journal, February 20, 2025, https://tdhj.org/  
blog/post/deception-transparent-battlefield/.  
8   
Marco J. Lyons and David E. Johnson, “People Who Know, Know MDO: Understanding   
Army Multi-Domain Operations as a Way to Make It Better,” Association of the United   
States Army, November 14, 2022, https://www.ausa.org/publications/people-who-  
know-know-mdo-understanding-army-multi-domain-operations-way-make-it-better;   
U.S. Army Futures Command Futures and Concepts Center, The U.S. Army Concept for   
Maneuver in Multi-Domain Operations, 2028-2040 (Washington, DC: U.S. Department   
of the Army, July 2020), https://apps.dtic.mil/sti/pdfs/AD1118627.pdf; Steven Metz,   
Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare   
(Carlisle, PA: U.S. Army War College Press, 2000); and U.S. Department of the Army,   
Field Manual (FM) 3-0 (Washington, DC: U.S. Department of Defense, October 2022),   
https://irp.fas.org/doddir/army/fm3-0.pdf.   
9   
Thomas A. Walsh and Alexandra L. Huber, “A Symphony of Capabilities: How the Joint   
Warfighting Concept Guides Service Force Design,” Joint Force Quarterly 111, October   
30, 2023, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3568312/a-  
symphony-of-capabilities-how-the-joint-warfighting-concept-guides-service-for/.  
10   
“Strategic Landpower: Winning the Clash of Wills,” Strategic Landpower Task Force,   
2014, https://api.army.mil/e2/c/downloads/310007.pdf; and Charles Cleveland et al.,   
Military Strategy for the 21st Century: People, Connectivity, and Influence, Cambria Rapid   
Communications in Conflict and Security Series (Amherst, NY: Cambria Press, 2018).  
11   
Philip Howard, Fen Lin, and Viktor Tuzov, “Computational Propaganda: Concepts,   
Methods, and Challenges,” Communication and the Public 8, no. 2 (June 2023): 47–53,   
https://doi.org/10.1177/20570473231185996; Grace B. Mueller et al., “Cyber Operations   
during the Russo-Ukrainian War,” CSIS, July 13, 2023, https://www.csis.org/analysis/  
cyber-operations-during-russo-ukrainian-war; and Benjamin Jensen, “The Cyber   
Character of Political Warfare,” Brown Journal of World Affairs 24, no. 1 (2017): 159–72,   
https://www.jstor.org/stable/27119085.  
12   
Michael Allen Hunzeker and Alexander Lanoszka, “Landpower and American   
Credibility,” Parameters 45, no. 4 (December 2015), https://doi.org/10.55540/0031-  
1723.2983; Christopher G. Pernin et al., Chasing Multinational Interoperability: Benefits,   
Objectives, and Strategies (Santa Monica, CA: RAND Corporation, April 2020), https://  
doi.org/10.7249/RR3068; and Timothy M. Bonds et al., What Role Can Land-Based,   
Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?   
(Santa Monica, CA: RAND Corporation, May 2017), https://doi.org/10.7249/RR1820.  
13   
Abby Doll et al., The Backbone of U.S. Joint Operations: Army Roles in the Indo-Pacific   
(Santa Monica, CA: RAND Corporation, May 2023), https://doi.org/10.7249/RRA1784-1.  
14   
Julian Stafford Corbett, Some Principles of Maritime Strategy (1911; Project Gutenberg,   
2005), https://www.gutenberg.org/files/15076/15076-h/15076-h.htm.  
15   
Corbett, Some Principles; Michael Romero and Kevin D. McCranie, “Mahan, Corbett,   
and the Foundations of Naval Strategic Thought,” Naval War College Review 76,   
no. 1 (May 9, 2023), https://digital-commons.usnwc.edu/nwc-review/vol76/iss1/16;   
A. T. Mahan, The Influence of Sea Power Upon History, 1660-1783 (1890; Project   
Gutenberg, 2004), https://www.gutenberg.org/files/13529/13529-h/13529-h.htm;   
Kevin D. McCranie, Mahan, Corbett, and the Foundations of Naval Strategic Thought,   
Studies in Naval History and Sea Power (Annapolis, MD: Naval Institute Press, 2021);   
and Barry M. Gough, “Maritime Strategy: The Legacies of Mahan and Corbett as   
Philosophers of Sea Power,” RUSI Journal 133, no. 4 (December 1988): 55–62, https://doi.  
org/10.1080/03071848808445330.

**Page 182**

176  
A Report of the CSIS Defense and Security Department  
16   
Jason Rivera, “A Theory of Cyberwarfare: Political and Military Objectives, Lines of   
Communication, and Targets,” Georgetown Security Studies Review, June 10, 2014,   
https://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyberwarfare-  
political-and-military-objectives-lines-of-communication-and-targets/; John J. Klein,   
“Corbett in Orbit: A Maritime Model for Strategic Space Theory,” Brookings Institution,   
January 1, 2004, https://www.brookings.edu/articles/corbett-in-orbit-a-maritime-  
model-for-strategic-space-theory/; and C. Alan Meadows, “A Cyber Fleet In Being:   
Considering Maritime Strategy as a Basis for Cyber Strategy,” Air Command and Staff   
College, April 2014, https://apps.dtic.mil/sti/tr/pdf/AD1023608.pdf.  
17   
Andrew Dorman, Mike Lawrence Smith, and Matthew R. H. Uttley, eds., The   
Changing Face of Maritime Power (London: Palgrave Macmillan, 1999), https://doi.  
org/10.1057/9780230509610.  
18   
Nicholas E. Bixby, “Joint All-Domain Operations (JADO): The Maneuver Concept for   
Future Conflict,” Over The Horizon Journal, November 22, 2024, https://othjournal.  
com/2024/11/22/joint-all-domain-operations-jado-the-maneuver-concept-for-future-  
conflict/; and “Understanding a Joint All Domain Operational Concept,” NATO   
Headquarters Rapid Deployable Corps Italy, accessed April 24, 2025, https://www.  
nrdc-ita.nato.int/newsroom/insights/creating-competitive-space-through-a-framework-  
of-joint-all-domain-maneuver.aspx.  
19   
Clay Bartels, Tim Tormey, and Jon Hendrickson, “Multidomain Operations and Close   
Air Support,” Military Review (March–April 2017), https://www.armyupress.army.mil/  
Journals/Military-Review/English-Edition-Archives/March-April-2017/ART-011/.  
20   
Brian J. Dunn, “The Tyranny of the Shores: Army Planning for the Asia-Pacific Theater,”   
Military Review (March–April 2018), https://www.armyupress.army.mil/Portals/7/  
military-review/Archives/English/Dunn-Tyranny-of-Shores.pdf.  
21   
Andrew F. Krepinevich Jr, “How to Deter China,” Foreign Affairs, February 16, 2015,   
https://www.foreignaffairs.com/articles/china/2015-02-16/how-deter-china; Benjamin   
Jensen, “Distributed Maritime Operations: Back to the Future?,” War on the Rocks,   
April 9, 2015, https://warontherocks.com/2015/04/distributed-maritime-operations-  
an-emerging-paradigm/; Andrew F. Krepinevich, Jr., Archipelagic Defense: The Japan-  
U.S. Alliance and Preserving Peace and Stability in the Western Pacific (Washington,   
DC: Sasakawa Peace Foundation, August 2017), https://www.spf.org/global-data/  
SPF\_20170810\_03.pdf; Art Corbett, “Expeditionary Advanced Base Operations (EABO)   
Handbook : Considerations for Force Development and Employment,” Marine Corps   
Warfighting Lab, Concepts & Plans Division, June 1, 2018, https://www.mca-marines.  
org/wp-content/uploads/Expeditionary-Advanced-Base-Operations-EABO-handbook-  
1.1.pdf; and Andrew F. Krepinevich Jr., “Archipelagic Defense 2.0,” Hudson Institute,   
September 14, 2023, https://www.hudson.org/archipelagic-defense-2-taiwan-china-  
japan-australia-deterrence-us-navy-andrew-krepinevich-jr.  
22   
Isaac B. Kardon, “Combating the Gray Zone: Examining Chinese Threats to the   
Maritime Domain,” Carnegie Endowment for International Peace, June 4, 2024, https://  
carnegieendowment.org/posts/2024/06/combating-the-gray-zone-examining-chinese-  
threats-to-the-maritime-domain?lang=en; and Brent Sadler and Elizabeth Lapporte,   
“China’s Evolving Risk Tolerance and Gray-Zone Operations: From the East China Sea   
to the South Pacific,” Heritage Foundation, September 9, 2024, https://www.heritage.  
org/defense/report/chinas-evolving-risk-tolerance-and-gray-zone-operations-the-east-  
china-sea-the-south.  
23   
Office of Naval Intelligence, The PLA Navy: New Capabilities and Missions for the 21st   
Century (Washington, DC: Office of Naval Intelligence, 2015), https://apps.dtic.mil/  
sti/pdfs/ADA616040.pdf; and U.S. Department of Defense, Military and Security   
Developments Involving the Peoples Republic of China 2024 (Washington, DC: U.S.   
Department of Defense, 2024), https://media.defense.gov/2024/Dec/18/2003615520/-  
1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-  
REPUBLIC-OF-CHINA-2024.PDF.   
24   
Collin Koh, “Beijing’s “Swiss Army Knife” in the South China Sea” in Beijing’s ‘Swiss   
Army Knife’ in the South China Sea, ed. Collin Koh (London: Routledge, 2024), https://

**Page 183**

177  
War and the Modern Battlefield  
doi.org/10.4324/9781003307365; and Aybars Oztuna, “Assessing The Chinese Naval   
Infrastructure Changes In The South China Sea Using Geospatial Intelligence” (master’s   
capstone, Johns Hopkins University, 2024), https://jscholarship.library.jhu.edu/server/  
api/core/bitstreams/9a61c029-3a11-44c5-bbd4-430b94216319/content.  
25   
Wei-Chung Chen et al., “China’s Gray Zone Actions in the East China Sea, Taiwan   
Strait, and South China Sea: A Comparative Study and Impact on Fisheries,” Marine   
Policy 167 (September 2024): 106246, https://doi.org/10.1016/j.marpol.2024.106246;   
Hongzhou Zhang, “The South China Sea Fishing Crisis: The Overlooked Role of   
Chinese Subnational Governments,” Pacific Review 37, no. 6 (November 2024):   
1090–1119, https://doi.org/10.1080/09512748.2024.2304805; Alison McCook and Donald   
R. Rothwell, “Territorial Disputes and Deep-Sea Mining in the South China Sea,”   
Melbourne Journal of International Law 25, no. 1 (July 2024): 95–131; Mohd Haris Abdul   
Rani, “Energy Dominance in the South China Sea: Legal and Geopolitical Battles over   
Strategic Resources,” International Journal of Research and Innovation in Social Science   
VIII, no. XII (2025): 3308–16, https://doi.org/10.47772/IJRISS.2024.8120275.  
26   
Shaleen Khanal and Hongzhou Zhang, “Ten Years of China’s Belt and Road Initiative: A   
Bibliometric Review,” Journal of Chinese Political Science 29, no. 2 (June 2024): 361–95,   
https://doi.org/10.1007/s11366-023-09873-z; Daniel Lindley, “Assessing China’s Motives:   
How the Belt and Road Initiative Threatens US Interests,” Air University, August 1, 2022,   
https://www.airuniversity.af.edu/JIPA/Display/Article/3111114/assessing-chinas-motives-  
how-the-belt-and-road-initiative-threatens-us-interests/; “Weaponizing the Belt and   
Road Initiative,” Asia Society Policy Institute, September 8, 2020, https://asiasociety.  
org/policy-institute/weaponizing-belt-and-road-initiative; and “China’s Belt and Road   
Initiative,” National Bureau of Asian Research, n.d., https://www.nbr.org/program/  
chinas-belt-and-road-initiative-military-and-security-implications/.  
27   
Fakhar Hussain et al., “The Digital Rise and Its Economic Implications for   
China through the Digital Silk Road under the Belt and Road Initiative,”   
Asian Journal of Comparative Politics 9, no. 2 (June 2024): 238–53, https://doi.  
org/10.1177/20578911231174731; and Robert Greene and Paul Triolo, “Will China Control   
the Global Internet Via Its Digital Silk Road?,” Carnegie Endowment for International   
Peace, May 8, 2020, https://carnegieendowment.org/posts/2020/05/will-china-control-  
the-global-internet-via-its-digital-silk-road?lang=en.  
28   
 Tony Roberts and Marjoke Oosterom, “Digital Authoritarianism: A Systematic iterature   
Review,” Information Technology for Development, November 24, 2024, 1–25, https://doi.  
org/10.1080/02681102.2024.2425352.  
29   
“China Regional Snapshot: Space,” House Committee on Foreign Affairs; and Malcolm   
Davis, “The Coming of China’s Space Silk Road,” Australian Strategic Policy Institute,   
August 11, 2017, https://www.aspistrategist.org.au/coming-chinas-space-silk-road/.  
30   
Gareth Jennings, “Ukraine Reportedly Strikes Russian Airbase,” Janes, February 25,   
2022, https://www.janes.com/osint-insights/defence-news/defence/ukraine-reportedly-  
strikes-russian-airbase.  
31   
“Half of Russia’s Black Sea Fleet’s Combat Jets out of Operation, Western Official Says,”   
Reuters, August 19, 2022, https://www.reuters.com/world/europe/half-russias-black-  
sea-fleets-combat-jets-out-operation-western-official-2022-08-19/.  
32   
Mark Trevelyan, “Moscow Says Three Killed in Ukrainian Drone Attacks on Air Bases   
Deep Inside Russia,” Reuters, December 5, 2022, https://www.reuters.com/world/  
europe/three-killed-fuel-tanker-explosion-russian-airfield-2022-12-05/.  
33   
Andrew Osborn, “UK Says a Supersonic Russian Bomber Likely to Have Been   
Destroyed in Drone Attack,” Reuters, August 22, 2023, https://www.reuters.com/  
world/europe/uk-says-supersonic-russian-bomber-likely-have-been-destroyed-drone-  
attack-2023-08-22/.  
34   
Benjamin Jensen, “Relative Superiority in the Drone Age: McRaven’s Playbook Meets   
Ukraine’s Airfield Assaults,” CSIS, Commentary, June 2, 2024, https://www.csis.org/  
analysis/relative-superiority-drone-age-mcravens-playbook-meets-ukraines-airfield-  
assaults; Benjamin Jensen “Ukraine’s Operation Spider Web destroyed more than

**Page 184**

178  
A Report of the CSIS Defense and Security Department  
aircraft – it tore apart the old idea that bases far behind the front lines are safe,” The   
Conversation June 5, 2025: https://theconversation.com/ukraines-operation-spider-  
web-destroyed-more-than-aircraft-it-tore-apart-the-old-idea-that-bases-far-behind-the-  
front-lines-are-safe-258056  
35   
Andrzej Wilk and Piotr Żochowski, “Ukraine Attacks with ATACMS Missiles. Day 603 of   
War,” OSW Centre for Eastern Studies, October 20, 2023, https://www.osw.waw.pl/en/  
publikacje/analyses/2023-10-20/ukraine-attacks-atacms-missiles-day-603-war.   
36   
Igor Delanoë, “Russia’s Black Sea Fleet in the ‘Special Military Operation’ in   
Ukraine,” Foreign Policy Research Institute, February 7, 2024, https://www.fpri.org/  
article/2024/02/russias-black-sea-fleet-in-the-special-military-operation-in-ukraine/.  
37   
George Allison, “Ukraine Has ‘Significantly Degraded’ Russian Black Sea Fleet,” UK   
Defence Journal, February 28, 2025, https://ukdefencejournal.org.uk/ukraine-has-  
significantly-degraded-russian-black-sea-fleet/.  
38   
Ibid.  
39   
“Space Wars Continue: Ukraine Hits Russian Satellite Communication Center in   
Yevpatoria,” Defense Express, June 24, 2024, https://en.defence-ua.com/news/  
space\_wars\_continue\_ukraine\_hits\_russian\_satellite\_communication\_center\_in\_  
yevpatoria-10950.html.  
40 Andrew Feickert, “The Army’s Multi-Domain Task Force (MDTF),” Congressional   
Research Service, IF 11797, April 14, 2025, https://www.congress.gov/crs-product/  
IF11797; U.S. Naval Institute Staff, “Report to Congress on The Army’s Multi-Domain   
Task Force,” USNI News, March 18, 2025, https://news.usni.org/2025/03/18/report-  
to-congress-on-the-armys-multi-domain-task-force; “Multi-Domain Task Forces: A   
Glimpse at the Army of 2035,” Association of the United States Army, March 2, 2022,   
https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035;   
Justin Katz, “Marines to Formally Stand up Second of 3 Marine Littoral Regiments in   
November,” Breaking Defense, October 17, 2023, https://breakingdefense.com/2023/10/  
marines-to-formally-stand-up-second-of-3-marine-littoral-regiments-in-november/;   
“Inside the Marine Corps’ First-Ever Littoral Regiment,” Defense One, October 6, 2024,   
https://www.defenseone.com/threats/2024/10/inside-marine-corps-first-ever-littoral-  
regiment/400084/; and Andrew Feickert, “The U.S. Marine Corps Marine Littoral   
Regiment (MLR),” Congressional Research Service, IF 12200, April 23, 2025, https://  
www.congress.gov/crs-product/IF12200.  
41   
Andrew Feickert, “The U.S. Army’s Typhon Mid-Range Capability (MRC) System,”   
Congressional Research Service, IF 12145, April 22, 2025, https://www.congress.gov/  
crs-product/IF12135.  
42   
Jen Judson, “Here’s How the US Army’s Multidomain Task Force Is Contributing to   
AUKUS,” Defense News, May 17, 2024, https://www.defensenews.com/land/2024/05/17/  
heres-how-the-us-armys-multidomain-task-force-is-contributing-to-aukus/.  
43   
Joe Mroszczyk, “Multi-Domain Effects Battalion: Space Integration and Effects in   
Multidomain Operations,” Military Review (Space & Missile Defense 2024), https://www.  
armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-2024/  
Multi-Domain-Effects-Battalion/.  
44   
Jen Judson, “US Army Buys Long-Flying Solar Drones to Watch over Pacific Units,”   
Defense News, October 30, 2024, https://www.defensenews.com/land/2024/10/30/  
us-army-buys-long-flying-solar-drones-to-watch-over-pacific-units/; and “US Army to   
Launch High Altitude Balloons,” U.S. Army Pacific, June 6, 2024, https://www.usarpac.  
army.mil/Our-Story/Our-News/Article-Display/Article/3798814/us-army-to-launch-high-  
altitude-balloons/.  
45   
Jensen, “Distributed Maritime Operations”; and United States Marine Corps, Tentative   
Manual for Expeditionary Advanced Base Operations, 2nd ed. (Washington, DC:   
Department of the Navy, May 2023), https://www.marines.mil/Portals/1/Docs/230509-  
Tentative-Manual-For-Expeditionary-Advanced-Base-Operations-2nd-Edition.  
pdf?ver=05KvG8wWlhI7uE0amD5uYg%3D%3D.

**Page 185**

179  
War and the Modern Battlefield  
46   
Todd South, “US Marines and Japanese Military Put New Radar on Taiwan’s Doorstep,”   
Marine Corps Times, August 8, 2024, https://www.marinecorpstimes.com/news/  
your-marine-corps/2024/08/08/us-marines-and-japanese-military-put-new-radar-on-  
taiwans-doorstep/.  
47   
U.S. Marine Corps Training and Education Command, Information in Marine Corps   
Operations, MCWP 8-10 (Arlington, VA: United States Marine Corps, February   
2024); Mark Pomerleau, “Marines Experimenting with Defensive Cyber Teams for   
Reconnaissance,” DefenseScoop, May 6, 2022, https://defensescoop.com/2022/05/06/  
marines-experimenting-with-defensive-cyber-teams-for-reconnaissance/; Mark   
Pomerleau, “Here’s What the Marines’ Information Command Centers Will   
Do,” C4ISRNet, December 6, 2019, https://www.c4isrnet.com/information-  
warfare/2019/12/06/heres-what-the-marines-information-command-centers-will-do/;   
and Mark Pomerleau, “The Navy and Marines Want an Integrated Force for Information   
Warfare,” C4ISRNet, December 5, 2019, https://www.c4isrnet.com/information-  
warfare/2019/12/05/the-navy-and-marines-want-an-integrated-force-for-information-  
warfare/.  
48   
Walsh and Huber, “A Symphony of Capabilities”; Bixby, “Joint All-Domain Operations”;   
and U.S. Department of the Army, Field Manual (FM) 3-0.  
THE ENDURING ROLE OF FIRES ON THE MODERN BATTLEFIELD  
1   
David Johnson, “The Tank is Dead: Long Live the Javelin, the Switchblade, the . . . ?,”   
War on the Rocks, April 18, 2022, https://warontherocks.com/2022/04/the-tank-is-  
dead-long-live-the-javelin-the-switchblade-the/.   
2   
Joseph Trevithick and Tyler Rogoway, “How the Houthis’ Rickety Air Defenses   
Threaten Even the F-35,” The War Zone, May 14, 2025, https://www.twz.com/air/how-  
the-houthis-rickety-air-defenses-can-threaten-the-stealthy-f-35; John Grady, “Black Sea   
Conflict Informing U.S. Navy Unmanned Systems, Says Admiral,” USNI News, February   
28, 2025, https://news.usni.org/2025/02/28/black-sea-conclifct-informing-u-s-navy-  
unmanned-systems-says-admiral; Joe Cowen, “The Rise of Uncrewed Surface Vessels:   
How Ukraine Is Rewriting the Rules of Naval Warfare,” Forces News, March 10, 2025,   
https://www.forcesnews.com/ukraine/rise-uncrewed-surface-vessels-how-ukraine-  
rewriting-rules-naval-warfare; and Brandon Weichert, “The Navy Is Freaked: The   
Age of Big Warships Is Just About Done,” National Interest, October 18, 2024, https://  
nationalinterest.org/feature/navy-freaked-age-big-warships-just-about-done-209999.  
3   
Japan Ministry of Defense, National Security Strategy of Japan (Tokyo: Ministry of   
Defense, December 2022), 18–19, https://www.mod.go.jp/j/policy/agenda/guideline/  
pdf/security\_strategy\_en.pdf; and Japan Ministry of Defense, Defense Buildup Program   
(Tokyo: Ministry of Defense, December 2022), 6–7, https://www.mod.go.jp/j/policy/  
agenda/guideline/plan/pdf/program\_en.pdf; and Australia Department of Defense,   
2024 National Defence Strategy (Canberra: Department of Defense, 2024), 38–39,   
https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-  
2024-integrated-investment-program.   
4   
“mitto,” Wiktionary, Accessed July 28, 2025, https://en.wiktionary.org/wiki/mitto.   
5   
“missilis,” Numen: The Latin Lexicon, https://latinlexicon.org/definition.  
php?p1=2036372&p2=m.   
6   
Henry Fairlie, “An Ambassador Must Be Free to Lie,” Washington Post, August 18, 1979,   
https://www.washingtonpost.com/archive/opinions/1979/08/19/an-ambassador-must-  
be-free-to-lie/596d2de2-da64-49bb-b431-eb775577b32c/.   
7   
38th Commandant of the Marine Corps, Commandant’s Planning Guidance   
(Washington, DC: Headquarters Marine Corps, 2019), 14, https://www.hqmc.marines.  
mil/Portals/142/Docs/%2038th%20Commandant%27s%20Planning%20Guidance\_2019.  
pdf.   
8   
Chairman of the Joint Chiefs of Staff, JP 3-30: Joint Air Operations (Arlington, VA: Joint   
Chiefs of Staff, July 2019), https://irp.fas.org/doddir/dod/jp3\_30.pdf; and “Shahed-136,”   
Army Recognition, March 12, 2025, https://armyrecognition.com/military-products/

**Page 186**

180  
A Report of the CSIS Defense and Security Department  
army/unmanned-systems/unmanned-aerial-vehicles/shahed-136-loitering-munition-  
kamikaze-suicide-drone-technical-data.  
9   
U.S. Department of Defense, 2022 National Defense Strategy of the United States of   
America Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review   
(Washington, DC: U.S. Department of Defense, October 2022), https://media.defense.  
gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.  
pdf; and Tom Karako, “The 2022 Missile Defense Review: Still Seeking Alignment,”   
CSIS, Commentary, October 27, 2022, https://www.csis.org/analysis/2022-missile-  
defense-review-still-seeking-alignment.   
10   
Sean Gainey, “Countering Uncrewed Aerial Systems: A Conversation with General   
Sean Gainey,” CSIS, transcript, November 14, 2023, https://www.csis.org/analysis/  
countering-uncrewed-aerial-systems-conversation-general-sean-gainey.   
11   
Ian Williams, Putin’s Missile War: Russia’s Strike Campaign in Ukraine (Washington, DC:   
CSIS, May 2023), 8, https://www.csis.org/analysis/putins-missile-war.   
12   
Ibid., 2.  
13   
Yasir Atalan and Benjamin Jensen, “Breaking Down Russian Missile Salvos: What Drives   
Neutralization?,” CSIS, Commentary, February 24, 2025, https://www.csis.org/analysis/  
breaking-down-russian-missile-salvos-what-drives-neutralization.   
14   
Ibid.   
15   
Williams, Putin’s Missile War, 15.  
16   
Frederik Mertens et al., Lessons from Land Warfare: One Year of War in Ukraine (The   
Hague: Hague Centre for Strategic Studies, February 2023), https://hcss.nl/wp-content/  
uploads/2023/02/Lessons-Learned-Paper-English-Version-Final.pdf.  
17   
Wes Rumbaugh, “Cost and Value in Air and Missile Defense Intercepts,” CSIS,   
Commentary, February 13, 2024, https://www.csis.org/analysis/cost-and-value-air-and-  
missile-defense-intercepts.   
18   
James Holmes, “The U.S. Navy Could Soon Get Patriot Missiles,” National Interest,   
October 28, 2024, https://nationalinterest.org/feature/us-navy-could-soon-get-patriot-  
missiles-213419.   
19   
Lauren Frias, “See the 2 Anti-Drone Missiles the US Navy Is Using to Defend Aircraft   
Carriers,” Business Insider, May 18, 2025, https://www.businessinsider.com/anduril-  
roadrunner-raytheon-coyote-drones-us-navy-carriers-2025-5; and Daniel M. Gettinger,   
Department of Defense Counter Unmanned Aircraft Systems: Background and Issues for   
Congress, CRS Report No. R48477 (Washington, DC: Congressional Research Service,   
March 31, 2025), https://www.congress.gov/crs-product/R48477.   
20   
“Operations in the Red Sea: Lessons for Surface Warfare,” CSIS, transcript, May 14,   
2024, https://www.csis.org/analysis/operations-red-sea-lessons-surface-warfare.  
21   
Ibid.  
22   
Shaan Shaikh, “The Iran-Israel Air Conflict, One Week In,” CSIS, Critical Questions,   
April 19, 2024, https://www.csis.org/analysis/iran-israel-air-conflict-one-week.  
23   
C. Todd Lopez, “U.S. Assets in the Mediterranean Again Helped Defend Israel Against   
Iranian Missiles,” U.S. Department of Defense, October 1, 2024, https://www.defense.  
gov/News/News-Stories/Article/Article/3923123/us-assets-in-mediterranean-again-  
helped-defend-israel-against-iranian-missiles/.   
24   
Ria Reddy, Ben Rezaei, Johanna Moore, Annika Ganzeveld, and Brian Carter, “Iran   
Update Special Report,” Institute for the Study of War and American Enterprise   
Institute Critical Threats Project, June 12, 2025, https://www.understandingwar.org/  
sites/default/files/Iran%20Nuclear%20Strikes%2C%20June%2012%2C%202025%20  
1%20PDF.pdf.  
25   
Emanuel Fabian, “The Israel-Iran war by the numbers, after 12 days of fighting,” The   
Times of Israel, June 24, 2025, https://www.timesofisrael.com/the-israel-iran-war-by-

**Page 187**

181  
War and the Modern Battlefield  
the-numbers-after-12-days-of-fighting/.  
26   
Bilal Y. Saab and Darren D. White, “Lessons Observed from the War Between Israel   
and Iran,” War on the Rocks, July 16, 2025, https://warontherocks.com/2025/07/  
lessons-observed-from-the-war-between-israel-and-iran/; Zvi Smith and Benoit Faucon,   
“Through Trial and Error, Iran Found Gaps in Israel’s Storied Air Defenses,” Wall Street   
Journal, July 15, 2025, https://www.wsj.com/world/middle-east/iran-israel-air-defense-  
362826e3; and Shelby Holiday, “U.S. Races to Defend Israel as It Burns Through Missile   
Interceptors,” Wall Street Journal, June 20, 2025, https://www.wsj.com/world/middle-  
east/u-s-races-to-defend-israel-as-it-burns-through-missile-interceptors-2909e49d.  
27   
Shelby Holliday, Anat Peled, and Drew FitzGerald, “Israel’s 12-Day War Revealed   
Alarming Gap in America’s Missile Stockpile,” Wall Street Journal, July 24, 2025, https://  
www.wsj.com/world/israel-iran-us-missile-stockpile-08a65396?mod=hp\_lead\_pos9.  
28   
Patrick Kingsley et al., “Will Israel’s Interceptors Outlast Iran’s Missiles? The   
Answer May Shape the War,” New York Times, June 19, 2025, https://www.nytimes.  
com/2025/06/19/world/middleeast/israel-interceptors-iran-missiles-war-length.html.  
29   
Chris Gordon, “Iranian Ballistic Missile Hit US Air Base in Qatar in June, Pentagon   
Reveals,” Wall Street Journal, July 11, https://www.airandspaceforces.com/iranian-  
ballistic-missile-hit-al-udeid-air-base-qatar/.  
30   
Ibid.  
31   
“Israel’s Missile Defense Engagements Since October 7th,” CSIS, Transcript, July 12,   
2024, https://www.csis.org/analysis/israels-missile-defense-engagements-october-7th.  
32   
Ibid.  
33   
U.S. Government Accountability Office, Directed Energy Weapons: DOD Should Focus   
on Transition Planning, GAO-23-105868 (Washington, DC: Government Accountability   
Office, April 2023), https://www.gao.gov/assets/gao-23-105868.pdf.  
34   
James Black, “Directed Energy: The Focus on Laser Weapons Intensifies,” RAND,   
January 25, 2024, https://www.rand.org/pubs/commentary/2024/01/directed-energy-  
the-focus-on-laser-weapons-intensifies.html.  
35   
Ibid.  
36   
Thomas Karako, “Deterrence, Air Defense, and Munitions Production in a New Missile   
Age,” Hoover Institution, December 23, 2022, https://www.hoover.org/research/  
deterrence-air-defense-and-munitions-production-new-missile-age.  
37   
Ibid.  
38   
Seth G. Jones, Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense   
Industrial Base (Washington, DC: CSIS, January 2023), 1, https://www.csis.org/analysis/  
empty-bins-wartime-environment-challenge-us-defense-industrial-base.  
39   
Thomas Karako, “The Missile Defeat Review in Context,” in Missile Defense and Defeat:   
Considerations for the New Policy Review, ed. Thomas Karako (Washington, DC: CSIS,   
March 2017), 10, https://missilethreat.csis.org/missile-defense-and-defeat/.   
40 Kenneth Todorov, “A Vector Check for America’s Missile Defense: Assessing the Course   
for the Trump Administration,” in Missile Defense and Defeat: Considerations for the New   
Policy Review, ed. Thomas Karako (Washington, DC: CSIS, March 2017), 60, https://  
missilethreat.csis.org/missile-defense-and-defeat/.  
41   
Jon Harper, “U.S. Challenged to Defend Against Chinese Missiles,” National Defense,   
March 7, 2022, https://www.nationaldefensemagazine.org/articles/2022/3/7/  
us-challenged-to-defend-against-chinese-missiles.  
42   
Ian Williams and Masao Dahlgren, “As Missile Threats Grow, Don’t Give Up on Boost-  
Phase Defense,” Defense News, July 22, 2022, https://www.defensenews.com/opinion/  
commentary/2022/07/22/as-missile-threats-grow-dont-give-up-on-boost-phase-  
defense/.

**Page 188**

182  
A Report of the CSIS Defense and Security Department  
43   
Clayton Swope and Tom Karako, “Why a Missile Shield in Space Makes Sense,”   
SpaceNews, February 4, 2025, https://spacenews.com/why-a-missile-shield-in-space-  
makes-sense/.  
44   
Troy Meink, keynote address at 2024 Space Symposium, April 9, 2024, transcript,   
https://www.nro.gov/Portals/135/Documents/news/speeches/2024/Space\_Symposium\_  
Remarks\_PREPARED\_FOR\_DELIVERY\_04082024.pdf.  
INTELLIGENCE IN AN TRANSPARENT WORLD  
1   
Joshua Yaffa, “How Bellingcat Unmasked Putin’s Assassins,” New Yorker, March 31,   
2021, https://www.newyorker.com/news/dispatch/how-bellingcat-unmasked-putins-  
assassins.  
2   
U.S. Department of the Treasury, “Treasury Targets Individuals Involved in the   
Poisoning of Aleksey Navalny,” press release, February 8, 2025, https://home.treasury.  
gov/news/press-releases/jy1700.  
3   
Yaffa, “How Bellingcat Unmasked Putin’s Assassins.”  
4   
Fabio Duarte, “Amount of Data Created Daily (2025),” Exploding Topics, last updated   
April 24, 2025, https://explodingtopics.com/blog/data-generated-per-day.  
5   
The concept of “smart cities” likely began in the late 1990s, but many point to Songdo   
in South Korea as the first city intentionally designed to be smart. For more, see   
Jeongwha Huh et al., “Who built Songdo, the ‘world’s first smart city?’ questioning   
technology firms’ ability to lead smart city development,” Eurasian Geography and   
Economics (February 2024): 1–18, https://doi.org/10.1080/15387216.2024.2309879; and   
Alberto De Marco and Giulio Mangano, “Evolutionary Trends in Smart City Initiatives,”   
Sustainable Futures 3, no. 100052 (May 2021): 100052, https://doi.org/10.1016/j.  
sftr.2021.100052.  
6   
“Ubiquitous Technical Surveillance Has Made Spying More Difficult,” The Economist,   
July 1, 2024, https://www.economist.com/technology-quarterly/2024/07/01/ubiquitous-  
technical-surveillance-has-made-spying-more-difficult.  
7   
Ibid.  
8   
Ibid.  
9   
Senior Advisory Group Panel on Commercially Available Information, Report to the   
Director of National Intelligence (Washington, DC: Office of the Director of National   
Intelligence, January 2022), 2–3, https://www.dni.gov/files/ODNI/documents/  
assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.  
10   
Souad Mekhennet and Joby Warrick, “Mossad’s Pager Operation: Inside Israel’s   
Penetration of Hezbollah,” Washington Post, October 5, 2024, https://www.  
washingtonpost.com/world/2024/10/05/israel-mossad-hezbollah-pagers-nasrallah/.  
11   
Jim Hockenhull, “How open-source intelligence has shaped the Russia-Ukraine war,”   
UK Ministry of Defence, December 9, 2022, https://www.gov.uk/government/speeches/  
how-open-source-intelligence-has-shaped-the-russia-ukraine-war.  
12   
“Ukraine, Russia Exploit Dating and Social Media Apps to Extract Military Intel,”   
Defense Mirror, October 19, 2024, https://www.defensemirror.com/news/37954/  
Ukraine\_\_Russia\_Exploit\_Dating\_and\_Social\_Media\_Apps\_to\_Extract\_Military\_Intel.  
13   
Through the Diia app, Ukrainians can “submit location-tagged photos and videos of   
Russian military sightings—as well as tips on ‘suspicious’ people who might be invaders   
or saboteurs. The data . . . are aggregated onto a map visible to Ukrainian intelligence   
officials working on defense and counterstrikes.” Drew Harwell, “Instead of Consumer   
Software, Ukraine’s Tech Workers Build Apps of War,” Washington Post, March 24,   
2022, https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-  
russian-invasion/. For more, see “How Smartphones and Social Media Became a Key   
Tool for War in Ukraine | WSJ Tech News Briefing,” YouTube video, posted by WSJ   
Podcasts, June 15, 2025, 7:34, https://youtu.be/OF-Wt4BeZE4; and Den Prystai, “From

**Page 189**

183  
War and the Modern Battlefield  
Ukrainians to Ukrainians. 5 Digital Tools Created to Help in Wartime,” war.ukraine.  
ua, October 5, 2022, https://war.ukraine.ua/articles/digital-tools-created-to-help-in-  
wartime/.  
14   
“Ukraine, Russia Exploit Dating and Social Media Apps to Extract Military Intel,”   
Defense Mirror, October 19, 2024, https://www.defensemirror.com/news/37954/  
Ukraine\_\_Russia\_Exploit\_Dating\_and\_Social\_Media\_Apps\_to\_Extract\_Military\_Intel; and   
David Kirichenko, Military Lessons for NATO from the Russia-Ukraine War: Preparing   
for the Wars of Tomorrow (London: The Henry Jackson Society and Centre for Russia   
and Eurasia Studies, October 2024), 52, https://henryjacksonsociety.org/publications/  
military-lessons-for-nato-from-the-russia-ukraine-war-preparing-for-the-wars-of-  
tomorrow/.  
15   
Harwell, “Instead of Consumer Software.”  
16   
Michael Peck, “Ukrainian Troops Used ‘Wedding Drones’ and Google Maps to Batter   
Russian Forces during the War’s Chaotic Early Days, Commanders Say,” Business   
Insider, May 16, 2023, https://www.businessinsider.com/ukrainian-artillery-uses-  
drones-google-maps-to-find-russian-targets-2023-5.  
17   
“Ukraine, Russia Exploit Dating and Social Media Apps to Extract Military Intel,”   
Defense Mirror. Also see Simon Newton, “Tinder Trap: Ukraine and Russia using fake   
profiles to trick soldiers into revealing intel,” Forces News, October 18, 2024, https://  
www.forcesnews.com/ukraine/tinder-trap-ukraine-and-russia-using-women-glean-  
intel-enemy-soldiers.  
18   
“Ukraine, Russia Exploit Dating and Social Media Apps to Extract Military Intel,”   
Defense Mirror.  
19   
Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft On the   
Issues (blog), June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/  
defending-ukraine-early-lessons-from-the-cyber-war/.  
20   
Ronen Bergman and Adam Goldman, “Israel Knew Hamas’s Attack Plan More Than a   
Year Ago,” New York Times, November 30, 2023, https://www.nytimes.com/2023/11/30/  
world/middleeast/israel-hamas-attack-intelligence.html.  
21   
“Head of IDF Devil’s Advocate Unit Tried Repeatedly in September to Warn of Possible   
Hamas Attack,” Times of Israel, January 6, 2024, https://www.timesofisrael.com/  
liveblog\_entry/head-of-idf-devils-advocate-unit-tried-repeatedly-in-september-to-warn-  
of-possible-hamas-attack/.  
22   
“Egypt Intelligence Official Says Israel Ignored Repeated Warnings of ‘Something Big’,”   
Times of Israel, October 9, 2023, https://www.timesofisrael.com/egypt-intelligence-  
official-says-israel-ignored-repeated-warnings-of-something-big/.  
23   
Emanuel Fabian, “Hours Before Hamas Attack, IDF Noticed Dozens of Terrorists   
Activating Israeli SIMs,” Times of Israel, February 26, 2024, https://www.timesofisrael.  
com/hours-before-hamas-attack-idf-noticed-hundreds-of-terrorists-activating-israeli-  
sims/.  
24   
Amy B. Zegart, Spies, Lies, and Algorithms: The History and Future of American   
Intelligence (Princeton, NJ: Princeton University Press, 2022), Ch. 5: Why Analysis is so   
Hard: the Seven Deadly Biases.  
25   
Emily Harding, Move Over JARVIS, Meet OSCAR (Washington, DC: CSIS, January 2022),   
https://www.csis.org/analysis/move-over-jarvis-meet-oscar.  
26   
Sam Trendall, “MI6 and CIA chiefs: ‘We are using generative AI to identify key   
information in a sea of data,’” Public Technology, September 10, 2024, https://www.  
publictechnology.net/2024/09/10/defence-and-security/mi6-and-cia-chiefs-we-are-  
using-generative-ai-to-identify-key-information-in-a-sea-of-data/; and Edward Wong et   
al., “Chinese Spy Agency Rising to Challenge the C.I.A.,” New York Times, December 27,   
2023, https://www.nytimes.com/2023/12/27/us/politics/china-cia-spy-mss.html.  
27   
For more, see the CSIS report No Front Lines, which was pending release at time of   
publication.

**Page 190**

184  
A Report of the CSIS Defense and Security Department  
THE SPACE DIMENSION  
1   
Mykhailo Fedorov (@FedorovMykhailo), “@elonmusk, while you try to colonize   
Mars—Russia try to occupy Ukraine!,” X post, Feb 26, 2022, 7:06 a.m., https://x.com/  
FedorovMykhailo/status/1497543633293266944.  
2   
Specifically, the target was Viasat’s KA-SAT satellite communications network. See   
“KA-SAT Network Cyber Attack Overview,” Viasat, March 20, 2022, https://www.  
viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/; UK   
Foreign, Commonwealth and Development Office, “Russia Behind Cyber-Attack with   
Europe-Wide Impact an Hour Before Ukraine Invasion,” press release, May 10, 2022,   
https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-  
impact-an-hour-before-ukraine-invasion; Antony J. Blinken, “Attribution of Russia’s   
Malicious Cyber Activity Against Ukraine,” U.S. Department of State, https://2021-  
2025.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/; U.S.   
Department of Justice, “Russian National Charged for Conspiring with Russian Military   
Intelligence to Destroy Ukrainian Government Computer Systems and Data,” press   
release, June 26, 2024, https://www.justice.gov/archives/opa/pr/russian-national-  
charged-conspiring-russia-military-intelligence-destroy-ukrainian; and Patrick Howell   
O’Neill, “Russia Hacked an American Satellite Company One Hour Before the Ukraine   
Invasion,” MIT Technology Review, May 10, 2022, https://www.technologyreview.  
com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine- .  
3   
Fedorov, “@elonmusk, while you try to colonize Mars.”  
4   
Google translation of Mykhailo Fedorov, “Ще 5 тисяч терміналів Starlink отримали   
від Польщі” [Another 5 thousand Starlink terminals received from Poland],   
Facebook post, April 3, 2025, https://www.facebook.com/mykhailofedorov.com.ua/  
videos/4020061868252926/.  
5   
Sandra Erwin, “As Russia Prepared to Invade, U.S. Opened Commercial Imagery   
Pipeline to Ukraine,” SpaceNews, April 6, 2022, https://spacenews.com/as-russia-  
prepared-to-invade-u-s-government-and-satellite-imagery-suppliers-teamed-up-to-  
help-ukraine/.  
6   
Alex Horton, Serhii Korolchuk, and Eva Dou, “Russia’s Illicit Starlink Terminals Help   
Power Its Advance in Ukraine,” Washington Post, October 12, 2024, https://www.  
washingtonpost.com/world/2024/10/12/starlink-russia-ukraine-elon-musk/.  
7   
Sandra Erwin, “On National Security | Drawing Lessons from the First Commercial   
Space War,” SpaceNews, May 20, 2022, https://spacenews.com/on-national-security-  
drawing-lessons-from-the-first-commercial-space-war/; and Kari A. Bingen, Kaitlyn   
Johnson, and Makena Young, Space Threat Assessment 2023 (Washington, DC: CSIS,   
April 2023), foreword, https://www.csis.org/analysis/space-threat-assessment-2023.  
8   
For example, see global trends in commercial space-based remote sensing in Kari A.   
Bingen, David Gauthier, and Madeleine Chang, Gold Rush: The 2024 Commercial Remote   
Sensing Global Rankings (Washington, DC: CSIS, October 2024), https://www.csis.org/  
analysis/gold-rush-2024-commercial-remote-sensing-global-rankings.   
9   
Vera Bergengruen, “How Tech Giants Turned Ukraine into an AI War Lab,” Time,   
February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.  
10   
Those companies include Maxar, Planet Labs, Blacksky, Airbus Space and Defense,   
Capella, ICEYE, Rheinmetall, and others.  
11   
“Aviation Week Names Maxar a 2022 Laureate Award Winner,” Maxar Technologies,   
July 25, 2022, https://blog.maxar.com/for-a-better-world/2022/aviation-week-names-  
maxar-a-2022-laureate-award-winner; and “The Most Documented Invasion in History,”   
Planet, n.d., https://www.planet.com/ukraine-photo-story/.  
12   
“Просто космос — результати використання ‘народного супутника’ ICEYE” [Just   
Space — Results of Using the ‘People’s Satellite’ ICEYE], Defence Intelligence Agency of   
the Ministry of Defense of Ukraine, June 26, 2024, https://gur.gov.ua/content/prosto-  
kosmos-rezultaty-vykorystannia-narodnoho-suputnyka-iceye.html; and Howard   
Altman, “‘People’s Satellite’ Helped Ukraine Hit Over 1,000 Targets Spy Agency Says,”

**Page 191**

185  
War and the Modern Battlefield  
TWZ, June 26, 2024, https://www.twz.com/news-features/peoples-satellite-helped-  
ukraine-hit-over-1000-targets-spy-agency-says.   
13   
“Space and Data Domain Lessons from Russia-Ukraine | Conflict in Focus,” CSIS,   
transcript, April 10, 2025, https://www.csis.org/analysis/space-and-data-domain-  
lessons-russia-ukraine-conflict-focus.   
14   
David Ignatius, “How the Algorithm Tipped the Balance in Ukraine,” Washington Post,   
December 19, 2022, https://www.washingtonpost.com/opinions/2022/12/19/palantir-  
algorithm-data-ukraine-war/; and “GEOINT Lessons Being Learned from the Russian-  
Ukrainian War,” U.S. Geospatial Intelligence Foundation, February 22, 2024, https://  
usgif.org/geoint-lessons-being-learned-from-the-russian-ukrainian-war/.  
15   
Lori Hinnant, Mstyslav Chernov, and Vasilisa Stepanenko, “AP Evidence Points to   
600 Dead in Mariupol Theater Airstrike,” AP News, May 4, 2022, https://apnews.com/  
article/russia-ukraine-war-mariupol-theater-c321a196fbd568899841b506afcac7a1.  
16   
Oksana Markarova, keynote address, Defense and Intelligence Space Conference 2024,   
February 27, 2024, Virginia, https://nssaspace.org/event/disc24/; “Ukraine Conflict   
Observatory,” Yale School of Public Health, accessed July 22, 2025, https://medicine.  
yale.edu/lab/khoshnood/conflict-observatory/ukraine/.  
17   
Florian Vidal, Russia’s Space Policy: The Path of Decline? (French Institute of   
International Relations, January 2021), https://www.ifri.org/sites/default/files/migrated\_  
files/documents/atoms/files/vidal\_russia\_space\_policy\_2021\_3.pdf.   
18   
Office of the Director of National Intelligence (ODNI), Annual Threat Assessment of the   
U.S. Intelligence Community (Washington, DC: ODNI, March 2025), https://www.dni.  
gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.  
19   
U.S. Department of the Treasury, “Treasury Sanctions Russian Proxy Wagner Group as   
a Transnational Criminal Organization,” press release, January 26, 2023, https://home.  
treasury.gov/news/press-releases/jy1220; and “Russia-Related Designations; Issuance of   
Russia-Related General Licenses and Frequently Asked Question; Revocation of Russia-  
Related General License,” U.S. Department of the Treasury, Office of Foreign Assets   
Control, April 12, 2023, https://ofac.treasury.gov/recent-actions/20230412.   
20   
Horton, Kkorolchuk, and Dou, “Russia’s Illicit Starlink Terminals.”  
21   
“KA-SAT Network,” Viasat; “Air and Space Domain Lessons from Russia-Ukraine:   
Part One | Conflict in Focus,” CSIS, transcript, March 20, 2025, https://www.csis.org/  
analysis/air-and-space-domain-lessons-russia-ukraine-part-one-conflict-focus; and   
O’Neill, “Russia Hacked an American Satellite Company.”   
22   
Space-based systems include three segments: the satellites in-orbit; transmission   
uplinks and downlinks between the satellites and ground stations; and ground stations,   
infrastructure, and user equipment used to operate the satellites, receive data, and   
relay commands. All of these segments can be targeted by counterspace weapons that   
degrade satellite performance.   
23   
Shira Rubin and Loveday Morris, “How Hamas Broke Through Israel’s Border Defenses   
During Oct. 7 Attack,” Washington Post, October 27, 2023, https://www.washingtonpost.  
com/world/2023/10/27/hamas-attack-israel-october-7-hostages/.  
24   
“Watch: Netanyahu says Israel targeted Iran’s nuclear and military sites,” BBC, June   
12, 2025, https://www.bbc.com/news/videos/cz70x722zvyo; and Thomas Newdick,   
“Israel Strikes Key Iranian Command And Control Sites In Tehran (Updated),” The War   
Zone, June 23, 2025, https://www.twz.com/news-features/israel-strikes-key-iranian-  
command-and-control-sites-in-tehran.  
25   
U.S. Department of Defense (DOD), Military and Security Developments Involving the   
People’s Republic of China 2024: Annual Report to Congress (Washington, DC: DOD,   
2024), 86, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-  
SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.  
PDF; and DOD, Military and Security Developments Involving the People’s Republic   
of China 2022: Annual Report to Congress (Washington, DC: DOD, 2022), 86, https://

**Page 192**

186  
A Report of the CSIS Defense and Security Department  
media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-  
DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.  
26   
DOD, Military and Security Developments Involving the People’s Republic of China 2023:   
Annual Report to Congress (Washington, DC: DOD, 2023), iv, 95, https://media.defense.  
gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-  
INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.   
27   
The 2025 Space Threat Assessment noted: “Many regions of the world, from the Baltic   
Sea through Eastern Europe, to the Middle East and parts of South Asia, have been   
affected by GPS jamming and spoofing nearly every day since the publication of last   
year’s report.” See Clayton Swope et al., Space Threat Assessment 2025 (Washington,   
DC: CSIS, April 2025), https://www.csis.org/analysis/space-threat-assessment-2025.   
For detailed definitions of jamming and spoofing, refer to past editions of Space Threat   
Assessment.  
28   
Courtney Kube, “Russia has figured out how to jam U.S. drones in Syria, officials say,”   
NBC News, April 10, 2018, https://www.nbcnews.com/news/military/russia-has-figured-  
out-how-jam-u-s-drones-syria-n863931; and Stephen Losey, “SOCOM boss: Adversaries   
are disabling Air Force gunships in Syria,” Air Force Times, April 27, 2018, https://www.  
airforcetimes.com/flashpoints/2018/04/27/socom-boss-adversaries-are-disabling-air-  
force-gunships-in-syria/.  
29   
Mike Eckel, “Ex-US Army Commander Warns of Russian Capabilities in Ukraine,” Radio   
Free Europe/Radio Liberty, January 24, 2018, https://www.rferl.org/a/ukraine-drones-  
artillery-ukrainian-forces/28994516.html.  
30   
Debra Werner, “HawkEye 360 Detects GPS Interference in Ukraine,” SpaceNews, March   
4, 2022, https://spacenews.com/hawkeye-360-gps-ukr/.  
31   
“OSCE SMM Spot Report 8/2021: Forced Emergency Landing of Long-Range Unmanned   
Aerial Vehicle Due to Dual GPS Signal Interference,” Organization for Security and   
Co-operation in Europe, April 9, 2021, https://www.osce.org/special-monitoring-  
mission-to-ukraine/483149; “Spot Report 6/2021: SMM Long-Range UAV Unable to Take   
Off Due to Dual GPS Signal Interference,” Organization for Security and Co-operation   
in Europe, April 7, 2021, https://www.osce.org/special-monitoring-mission-to-  
ukraine/483008; and Dana Goward, “Russia Ramps up GPS Jamming Along with   
Troops at Ukraine Border,” GPS World, April 21, 2021, https://www.gpsworld.com/  
russia-ramps-up-gps-jamming-along-with-troops-at-ukraine-border/.  
32   
Tereza Pultarova, “Ukraine’s Bold Gamble on an Electronic Warfare ‘Wall’,” IEEE   
Spectrum, May 19, 2025, https://spectrum.ieee.org/electronic-warfare-ukraine; Jack   
Watling and Nick Reynolds, Tactical Developments During the Third Year of the Russo-  
Ukrainian War (London: Royal United Services Institute, February 2025), https://  
static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.  
pdf; and “Russia Doubles Production of Key Types of Military Equipment—PM,” TASS,   
September 20, 2023, https://tass.com/defense/1677893.  
33   
Bryan Clark, “The Fall and Rise of Russian Electronic Warfare,” IEEE Spectrum, July   
20, 2022, https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare; and   
Carlotta Gall and Vladyslav Golovin, “Some U.S. Weapons Stymied by Russian Jamming   
in Ukraine,” New York Times, May 25, 2024, https://www.nytimes.com/2024/05/25/  
world/europe/us-weapons-russia-jamming-ukraine.html.  
34   
Alex Marquardt, Natasha Bertrand, and Zachary Cohen, “Russia’s Jamming of U.S.-  
Provided Rocket Systems Complicates Ukraine’s War Effort,” CNN, May 6, 2023,   
https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine;   
Isabelle Khurshudyan and Alex Horton, “Russian Jamming Leaves Some High-Tech   
U.S. Weapons Ineffective in Ukraine,” Washington Post, May 24, 2024, https://www.  
washingtonpost.com/world/2024/05/24/russia-jamming-us-weapons-ukraine/; and   
Gall and Golovin, “Some U.S. Weapons Stymied.”  
35   
Valerii Zaluzhnyi, “Modern Positional Warfare and How to Win in It,” The Economist,   
2023, https://infographics.economist.com/2023/ExternalContent/ZALUZHNYI\_FULL\_  
VERSION.pdf.

**Page 193**

187  
War and the Modern Battlefield  
36   
Thomas Withington, “The Underwhelming Performance of Russian Land Forces   
Electronic Warfare—Watt Happened?,” Defence Horizon Journal, August 18, 2022,   
https://tdhj.org/blog/post/watt-happened/.  
37   
A jamming signal is broadcast at sufficient strength to overpower legitimate GPS   
signals. A spoofing signal is meant to appear like a legitimate GPS signal, but the   
spoofing signal transmits incorrect positional information. See Swope et al., Space   
Threat Assessment 2025.  
38   
Ibid.  
39   
“Space Threat Fact Sheet,” Headquarters Space Force Intelligence, updated May 16,   
2025, https://nssaspace.org/wp-content/uploads/2025/05/20250516-S2-Space-Threat-  
Fact-Sheet-v8-RELEASE.pdf.  
40 Courtney Albon, “New US Space Force Jammers Aim to Disrupt China’s SATCOM   
Signals,” DefenseNews, December 19, 2024, https://www.defensenews.com/  
space/2024/12/19/new-us-space-force-jammers-aim-to-disrupt-chinas-satcom-  
signals/; and Colin Demarest, “US Army Set to Test Combined Cyber, Jamming,   
Signal Intelligence Tool,” Army Times, August 15, 2023, https://www.armytimes.com/  
electronic-warfare/2023/08/15/us-army-set-to-test-combined-cyber-jamming-signal-  
intelligence-tool/.   
41   
Clayton Swope et al., Space Threat Assessment 2024 (Washington, DC: CSIS, April 2024),   
https://www.csis.org/analysis/space-threat-assessment-2024; and Swope et al., Space   
Threat Assessment 2025.  
42   
“UN agencies warn of satellite navigation jamming and spoofing,” International   
Telecommunication Union, March 26, 2025, https://www.itu.int/hub/2025/03/  
un-agencies-warn-of-satellite-navigation-jamming-and-spoofing/.  
43   
Valeria Insinna, “SpaceX Beating Russian Jamming Attack Was ‘Eyewatering’: DoD   
Official,” Breaking Defense, April 20, 2022, https://breakingdefense.com/2022/04/  
spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/.  
44   
For example, many drone manufacturers and operators exhibiting at the Drone   
Summit 2025 in Riga, Latvia, in May 28, 2025, showcased technical and operational   
solutions aimed at mitigating the battlefield effects of GPS interference, https://  
dronesummit.lv/. Watling and Reynolds, Tactical Developments.  
45   
Ibid.; and Pultarova, “Ukraine’s Bold Gamble.”  
46   
Troy Meink, David W. Allvin, and B. Chance Saltzman, “Department of the Air   
Force Posture Statement: Fiscal Year 2026,” Presentation to the Committees and   
Subcommittees of the U.S. Senate and House of Representatives, 119th Cong., 1st sess.,   
https://www.armed-services.senate.gov/imo/media/doc/saltzman\_opening\_statement.  
pdf; U.S. Space Systems Command, “U.S. Space Force Field Commands Announce   
Accelerated GPS III Mission to Enhance Warfighter Capabilities,” press release, April 7,   
2025, https://www.ssc.spaceforce.mil/Newsroom/Article/4147205/us-space-force-field-  
commands-announce-accelerated-gps-iii-mission-to-enhance-w; and Theresa Hitchens,   
“Ensured SATCOM, GPS Alternatives Tops Among Space Force Budget Wishes,”   
Breaking Defense, September 5, 2024, https://breakingdefense.com/2024/09/ensured-  
satcom-gps-alternatives-tops-among-space-force-wishes/.   
47   
The two nascent Chinese LEO broadband satellites constellations referenced are   
the GuoWang constellation, led by China Satellite Network Group Co., Ltd. (“China   
SatNet”), and the Thousand Sails (or “Qianfan”) constellation, led by Shanghai   
Spacecom Satellite Technology (SSST); Blaine V. Curcio, testimony submitted to the   
U.S.-China Economic and Security Review Commission, Hearing on Hearing on China’s   
Ambitions in Space, April 3, 2025, https://www.uscc.gov/sites/default/files/2025-04/  
Blaine\_Curcio\_Testimony.pdf; and ODNI, Annual Threat Assessment, 15.  
48   
B. Chance Saltzman, testimony submitted to the U.S.-China Economic and Security   
Revision Commission, Hearing on China’s Ambitions in Space, April 3, 2025, https://  
www.uscc.gov/sites/default/files/2025-04/Chance\_Saltzman\_Testimony.pdf.

**Page 194**

188  
A Report of the CSIS Defense and Security Department  
49   
Swope et al., Space Threat Assessment 2025. There are several other good references   
on space threats including the Secure World Foundation’s Annual Report, the Defense   
Intelligence Agency’s Challenges to Security in Space, and the U.S. Space Force’s   
quarterly space threat update.  
50   
Bingen, Johnson, and Young, Space Threat Assessment 2023. In recent years, Russian   
officials have showcased the Peresvet ground-based satellite laser and Sokol-Eshelon,   
an airborne laser system that is a revival of a Soviet-era program, which has the stated   
capability to attack satellites in LEO.  
51   
Swope et al., Space Threat Assessment 2024.  
52   
ODNI, Annual Threat Assessment, 15.  
53   
“SDA Layered Network of Military Satellites Now Known as “Proliferated Warfighter   
Space Architecture,” Space Development Agency, January 23, 2023, https://www.sda.  
mil/sda-layered-network-of-military-satellites-now-known-as-proliferated-warfighter-  
space-architecture/.  
54   
Stephen Chen, “Chinese Physicists Simulate Nuclear Blast against Satellites,” South   
China Morning Post, October 20, 2022, https://www.scmp.com/news/china/science/  
article/3196629/chinese-physicists-simulate-nuclear-blast-against-satellites.   
55   
Bingen, Johnson, and Young, Space Threat Assessment 2023.  
56   
Theresa Hitchens, “‘Space fires’ to enable ‘space superiority’ are top SPACECOM   
priorities for FY27,” Breaking Defense, August 6, 2024, https://breakingdefense.  
com/2024/08/space-fires-to-enable-space-superiority-are-top-spacecom-priorities-  
for-fy27/.  
57   
“Space Warfighting: A Framework for Planners,” U.S. Space Force, released April 2025,   
https://www.spaceforce.mil/Portals/2/Documents/SAF\_2025/Space\_Warfighting\_-\_A\_  
Framework\_for\_Planners\_BLK2\_(final\_20250410).pdf.  
58   
Ministère des Armées [Ministry of the Armed Forces], LPM 2024-2030: Les   
grandes orientations [LPM 2024-2030: The Major Directions] (Paris: Government   
of France, 2023), 9–10, https://www.defense.gouv.fr/sites/default/files/ministere-  
armees/Livret%20de%20pr%C3%A9sentation%20de%20la%20Loi%20de%20  
programmation%20militaire%202024-2030%20%286%20avril%202023%29.pdf; and   
“France to launch 'fearsome' surveillance satellites to bolster space defences,” Reuters,   
July 25, 2019, https://www.reuters.com/article/us-france-space-defence/france-to-  
launch-fearsome-surveillance-satellites-to-bolster-space-defenses-idUSKCN1UK1TY/.   
59   
“Jackal for Geosynchronous Orbit and Cislunar Space,” True Anomaly, April 3, 2025,   
https://www.trueanomaly.space/newsroom/jackal-for-geosynchronous-orbit-and-  
cislunar-space.  
60 For example, in May 2025, the Polish Ministry of National Defense signed an agreement   
with Finland’s ICEYE for the company to deliver three SAR satellites to the Polish   
Armed Forces to advance its sovereign reconnaissance systems for ISR activities.   
ICEYE, “ICEYE to provide SAR satellites for the Armed Forces of Poland,” press release,   
May 14, 2025, https://www.iceye.com/newsroom/press-releases/iceye-to-provide-sar-  
satellites-for-the-armed-forces-of-poland.  
61   
U.S. Geospatial Intelligence Foundation, “GEOINT Lessons Being Learned from the   
Russian-Ukrainian War.”  
62   
“Russia warns West: We can target your commercial satellites,” Reuters, October 27,   
2022, https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-  
be-targets-2022-10-27/.  
63   
Swope et al., Space Threat Assessment 2024.  
TECHNOLOGICAL EVOLUTION ON THE BATTLEFIELD  
1   
Marc Santora, “Rise of the Dragons: Fire-Breathing Drones Duel in Ukraine,” New York   
Times, October 12, 2024, https://www.nytimes.com/2024/10/12/world/europe/ukraine-

**Page 195**

189  
War and the Modern Battlefield  
russia-dragon-drones.html.  
2   
“How Britain Invented The Tank In The First World War,” Imperial War Museums, n.d.,   
https://www.iwm.org.uk/history/how-britain-invented-the-tank-in-the-first-world-war;   
and Stephen Dowling, “The WWI tank that helped change warfare forever,” BBC, May   
31, 2018, https://www.bbc.com/future/article/20180531-the-wwi-tank-that-helped-  
change-warfare-forever.  
3   
The Battle of Medina Ridge was fought in February 1991 between U.S.-led coalition   
forces and Iraq’s Republican Guard. It involved more than 3,000 tanks and is   
considered one of the largest tank battles of the twentieth century. See “The Untold   
Story of the World’s Fiercest Tank Battle,” National Geographic, last modified February   
22, 2021, https://www.nationalgeographic.com/history/article/untold-story-worlds-  
fiercest-tank-battle-gulf-war.  
4   
Yaroslav Trofimov, “Drones Everywhere: How the Technological Revolution on Ukraine   
Battlefields Is Reshaping Modern Warfare,” Wall Street Journal, September 28, 2023,   
https://www.wsj.com/world/drones-everywhere-how-the-technological-revolution-on-  
ukraine-battlefields-is-reshaping-modern-warfare-bf5d531b.  
5   
Ibid.  
6   
David Axe, “Bullseye! A Grenade-Tossing Ukrainian Drone Knocked Out One Russian   
Tank—And Then Terrorized A Second Tank That Came To The Rescue,” Forbes,   
November 12, 2023, https://www.forbes.com/sites/davidaxe/2023/11/12/bullseye-a-  
grenade-tossing-ukrainian-drone-knocked-out-one-russian-tank-and-then-terrorized-  
a-second-tank-that-came-to-the-rescue/; and Jaspreet Gill, “As US Army transforms,   
it’s gleaning lessons about high- and low-tech fighting from Ukraine, Israel,” Breaking   
Defense, November 29, 2023, https://breakingdefense.com/2023/11/as-us-army-  
transforms-its-gleaning-lessons-about-high-and-low-tech-fighting-from-ukraine-israel/  
7   
Marc Santora, “Rise of the Dragons: Fire-Breathing Drones Duel in Ukraine,” New York   
Times, October 12, 2024, https://www.nytimes.com/2024/10/12/world/europe/ukraine-  
russia-dragon-drones.html.  
8   
Trofimov, “Drones Everywhere.”  
9   
Ibid.  
10   
Andrew E. Kramer, “In a Tough Year on Land, Drones Give Ukraine Some Success at   
Sea,” New York Times, December 20, 2023, https://www.nytimes.com/2023/12/20/  
world/europe/ukraine-drones-sea.html.  
11   
Brian Glyn Williams, “How the Ukrainians – With No Navy – Defeated Russia’s Black Sea   
Fleet,” MarineLink, July 23, 2024, https://www.marinelink.com/news/ukrainians-navy-  
defeated-russias-black-515405; H. I. Sutton, “Uncrewed Platforms Have Been Critical to   
Ukraine’s Success in the Black Sea,” Royal United Services Institute, August 20, 2024,   
https://www.rusi.org/explore-our-research/publications/commentary/uncrewed-  
platforms-have-been-critical-ukraines-success-black-sea; Michael Ashcroft, “Meet a   
Real-Life ‘Q’: Mastermind Behind Ukraine’s Sea Drone Warfare Success,” Kyiv Post,   
December 1, 2024, https://www.kyivpost.com/post/42949; and Kramer, “In a Tough   
Year on Land.”  
12   
Kateryna Zakharchenko, “Ukraine Naval Drone Shoots Down Two Russian Warplanes   
in 24 Hours: First-Ever USV Fighter Jet Kills (Updated),” Kyiv Post, May 4, 2024, https://  
www.kyivpost.com/post/51994; and Howard Altman, “Two Russian Su-30 Flankers   
Downed By AIM-9s Fired From Drone Boats: Ukrainian Intel Boss,” The War Zone, May   
3, 2025, https://www.twz.com/news-features/two-russian-su-30-flankers-downed-by-  
aim-9s-fired-from-drone-boats-ukrainian-intel-boss.  
13   
Vitalii Hnidyi, “Ukrainian Brigade Pioneers Remote-Controlled Ground Assaults,”   
Reuters, January 16, 2025, https://www.reuters.com/world/europe/ukrainian-brigade-  
pioneers-remote-controlled-ground-assaults-2025-01-16/; and Warren Murray, “Ukraine   
war briefing: Gravehawk revealed as new air defence system pledged by Starmer,” The   
Guardian, January 16, 2025, https://www.theguardian.com/world/2025/jan/17/ukraine-  
war-briefing-gravehawk-revealed-as-new-air-defence-system-pledged-by-starmer.

**Page 196**

190  
A Report of the CSIS Defense and Security Department  
14   
“Basic qualification levels for drone operators approved,” Odessa Journal, January   
14, 2025, https://odessa-journal.com/basic-qualification-levels-for-drone-operators-  
approved; Kateryna Bondar, “Why Ukraine is Establishing Unmanned Forces Across   
Its Defense Sector and What the United States Can Learn from It,” CSIS, Commentary,   
November 19, 2024, https://www.csis.org/analysis/why-ukraine-establishing-  
unmanned-forces.  
15   
“Basic qualification levels,” Odessa Journal.  
16   
Olivia Savage, “Ukraine conflict: Ukraine establishes world’s first unmanned force,”   
Janes, June 14, 2024, https://www.janes.com/osint-insights/defence-news/air/ukraine-  
conflict-ukraine-establishes-worlds-first-unmanned-force.  
17   
Sarah Young, “UK firm supports Ukrainian armed forces in drone tech race,” Reuters,   
March 28, 2024, https://www.reuters.com/business/aerospace-defense/uk-firm-  
supports-ukrainian-armed-forces-drone-tech-race-2024-03-27/.  
18   
David Axe, “Ukraine Is Jamming Russian Glide Bombs All Along The Front Line, Erasing   
One Of Russia’s Main Battlefield Advantages,” Forbes, February 26, 2025, https://www.  
forbes.com/sites/davidaxe/2025/02/26/ukraine-is-jamming-russian-glide-bombs-  
all-along-the-front-line-erasing-one-of-russias-main-battlefield-advantages/; Boyko   
Nikolov, “Russian glide bombs fell off a cliff, a VKS insider reports,” BulgarianMilitary.  
com, February 27, 2025, https://bulgarianmilitary.com/2025/02/27/russian-glide-  
bombs-fell-off-a-cliff-a-vks-insider-reports/; Axe, “Ukraine Is Jamming”; and Nikolov,   
“Russian glide bombs.”  
19   
Nataliia Kushnerska, “Missiles, AI, and drone swarms: Ukraine’s 2025 defense tech   
priorities,” Atlantic Council, January 2, 2025, https://www.atlanticcouncil.org/blogs/  
ukrainealert/missiles-ai-and-drone-swarms-ukraines-2025-defense-tech-priorities/.  
20   
Guy Faulconbridge, “Russia uses new laser weapons in Ukraine, Zelenskiy mocks   
‘wonder weapon’,” Reuters, May 18, 2022, https://www.reuters.com/world/  
europe/russia-touts-new-generation-blinding-laser-weapons-2022-05-18/; and   
Dominika Kunertova and Stephen Herzog, “Emerging and Disruptive Technologies   
Transform, but Do Not Lift, the Fog of War – Evidence from Russia’s War on   
Ukraine,” ETH Zurich, February 14, 2024, https://www.research-collection.ethz.ch/  
bitstream/handle/20.500.11850/696795/2024-09-29Kunertova-HerzogFNDUEDTs.  
pdf?sequence=7&isAllowed=y.  
21   
Kris Osborn, “Ukraine’s Decentralized Command Puts Russia on the Defensive,”   
National Interest, September 11, 2022, https://nationalinterest.org/blog/buzz/ukraines-  
decentralized-command-puts-russia-defensive-204714.  
22   
Alistair MacDonald and Ievgeniia Sivorka, “Russia Trots Out Its Newest Weapons in   
Ukraine: Horses,” Wall Street Journal, March 9, 2025, accessed March 10, 2025, https://  
www.wsj.com/world/russia-ukraine-war-horses-8079ebb6.  
23   
Ibid.  
24   
Bobby Allyn, “Deepfake video of Zelenskyy could be ‘tip of the iceberg’ in info war,   
experts warn,” NPR, March 16, 2022, https://www.npr.org/2022/03/16/1087062648/  
deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia; and Kunertova   
and Herzog, “Emerging and Disruptive.”  
25   
Bryan Sicard, “Can Facial Recognition Technology Save Ukraine’s Children? One   
Company’s Strides Tracking the Perpetrators and Victims of War Crimes,” Journal of   
High Technology Law, Suffolk University Law School, April 17, 2024, https://sites.suffolk.  
edu/jhtl/2024/04/17/can-facial-recognition-technology-save-ukraines-children-one-  
companys-strides-tracking-the-perpetrators-and-victims-of-war-crimes/.  
26   
Ibid.  
27   
Sicard, “Can Facial Recognition”; and Потерь.НЕТ, https://poteru.net/. Потерь.НЕТ   
[Losses.net] is the online database created by Ukraine to document deceased Russian   
soldiers.  
28   
Vera Bergengruen, “How Tech Giants Turned Ukraine Into an AI War Lab,” Time,

**Page 197**

191  
War and the Modern Battlefield  
February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.  
29   
Ellen Nakashima and Alex Horton, “Russian government hackers have likely   
penetrated critical Ukrainian computer systems, U.S. says,” Washington Post, February   
15, 2022, https://www.washingtonpost.com/national-security/2022/02/15/russia-  
ukraine-cyber-attacks/.  
30   
Jon Bateman, “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts,   
Influences, and Implications,” Carnegie Endowment for International Peace, December   
16, 2022, https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-  
operations-in-ukraine-military-impacts-influences-and-implications?lang=en/.  
31   
Khrystyna Kvartsiana, “Ukraine’s Cyber Defense: Lessons in Resilience,” German   
Marshall Fund of the United States, December 2023, https://www.gmfus.org/sites/  
default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf; and   
Aiden Render-Katolik, “The IT Army of Ukraine,” CSIS (blog), August 15, 2023, https://  
www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine.  
32   
Ulrike Franke and Jenny Söderström, “Star tech enterprise: Emerging technologies in   
Russia’s war on Ukraine,” European Council on Foreign Relations, September 5, 2023,   
https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-  
war-on-ukraine/#lesson-1-private-technology-companies-are-playing-an-ever-more-  
important-role-in-warfare.   
33   
Bergengruen, “How Tech Giants.”  
34   
Kateryna Bondar, “How Ukraine Rebuilt Its Military Acquisition System Around   
Commercial Technology,” CSIS, January 13, 2025, https://www.csis.org/analysis/how-  
ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology.  
35   
Ibid.  
36   
Marta Bo and Jessica Dorsey, “Symposium on Military AI and the Law of Armed   
Conflict: The ‘Need’ for Speed – The Cost of Unregulated AI Decision-Support   
Systems to Civilians,” OpinioJuris, April 4, 2024, https://opiniojuris.org/2024/04/04/  
symposium-on-military-ai-and-the-law-of-armed-conflict-the-need-for-speed-the-cost-  
of-unregulated-ai-decision-support-systems-to-civilians/. Companion systems Fire   
Factory, Depth of Wisdom, Alchemist, and Lavender have also played a role on the   
battlefield.  
37   
Harry Davies, Bethan McKernan, and Dan Sabbagh, “‘The Gospel’: how Israel uses   
AI to select bombing targets in Gaza,” The Guardian, December 1, 2023, https://www.  
theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-  
targets; Bo and Dorsey, “Symposium on Military”; and Geoff Brumfiel, “Israel is using   
an AI system to find targets in Gaza. Experts say it’s just the start,” NPR, December 14,   
2023, https://www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-  
targets-in-gaza-experts-say-its-just-the-st.   
38   
Bo and Dorsey, “Symposium on Military”; and Brumfiel, “Israel is using.”  
39   
Brumfiel, “Israel is using”; and Bethan McKernan and Harry Davies, “‘The machine did   
it coldly’: Israel used AI to identify 37,000 Hamas targets,” The Guardian, April 3, 2024,   
https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-  
airstrikes. Separately, the Lavender system was used to rapidly identify potential   
“junior” Hamas and Palestinian Islamic Jihad operatives, with the AI system identifying   
37,000 Palestinian men for targeting.  
40 Nick Robins-Early, “How Israel uses facial-recognition systems in Gaza and beyond,”   
The Guardian, April 19, 2024, https://www.theguardian.com/technology/2024/apr/19/  
idf-facial-recognition-surveillance-palestinians.   
41   
Sheera Frenkel, “Israel Deploys Expansive Facial Recognition Program in Gaza,” New   
York Times, March 27, 2024, https://www.nytimes.com/2024/03/27/technology/israel-  
facial-recognition-gaza.html; Sophia Yan, “Israel ‘using facial recognition technology   
to identify Hamas terrorists’,” The Telegraph, March 28, 2024, https://www.telegraph.  
co.uk/world-news/2024/03/28/israel-using-facial-recognition-pinpoint-hamas-gaza/;

**Page 198**

192  
A Report of the CSIS Defense and Security Department  
Meghan McCarty Carino, Jesús Alvarado, and Daniel Shin, “Facial recognition part of   
Israel’s arsenal in Gaza war,” Marketplace, April 8, 2024, https://www.marketplace.org/  
shows/marketplace-tech/israel-gaza-hamas-facial-recognition/; and Robins-Early, “How   
Israel uses.”  
42   
Emily Rose, “Israeli Startups Make Global Plans After Key Role in War,” Reuters,   
January 31, 2025, https://www.reuters.com/world/middle-east/israeli-startups-make-  
global-plans-after-key-role-war-2025-01-31/; and “Israel: Proposed ‘Green Track’ for   
R&D Centers,” KPMG, November 7, 2024, https://kpmg.com/us/en/taxnewsflash/  
news/2024/11/tnf-israel-proposed-green-track-r-and-d-centers.html.  
43   
Rose, “Israeli Startups Make.”  
44   
Ibid.  
45   
Ibid.  
46   
Sam Mednick, Garance Burke, and Michael Biesecker, “How US tech giants supplied   
Israel with AI models, raising questions about tech’s role in warfare,” AP News,   
February 18, 2025, https://apnews.com/article/israel-palestinians-ai-weapons-430f6f15a  
ab420806163558732726ad9.  
47   
Ibid.  
48   
Ibid.  
49   
Harry Davies and Yuval Abraham, “Revealed: Microsoft Deepened Ties with Israeli   
Military to Provide Tech Support During Gaza War,” The Guardian, January 23, 2025,   
https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft;   
and Oren Ziv, “Microsoft, OpenAI Provide Cloud Services to Israeli Army,” +972   
Magazine, April 16, 2024, https://www.972mag.com/microsoft-azure-openai-israeli-  
army-cloud/.  
50   
McKernan and Davies, “‘The machine did it coldly’.”  
51   
Ibid.  
52   
Ibid.  
53   
Frenkel, “Israel Deploys Expansive”; Robins-Early, “How Israel uses”; and Jerusalem   
Post Staff, “IDF enhances wartime surveillance, deploys facial recognition in   
Gaza,” Jerusalem Post, March 28, 2024, https://www.jpost.com/israel-hamas-war/  
article-794128.  
54   
Frenkel, “Israel Deploys Expansive.”  
55   
These guerrilla-style tactics are likely to take place under the canopy of a separate   
high-tech exchange of fire. Precision strikes have marked the conflicts in Ukraine and   
around Israel and are likely to be decisive in a Pacific contingency. For more on this   
form of war, see Chapter 6: The Enduring Role of Fires).  
56   
Emily Harding and Harshana Ghoorhoo, Seven Critical Technologies for Winning the Next   
War (Washington, DC: CSIS, April 2023), https://www.csis.org/analysis/seven-critical-  
technologies-winning-next-war; and Emily Harding and Aosheng Pusztaszeri, Averting   
Strategic Surprise in Nontraditional Intelligence Domains (Washington, DC: CSIS,   
October 2024) [private report].  
57   
Harding and Ghoorhoo, Seven Critical Technologies.  
58   
Ibid.  
59   
John Mike, “EOD Group One Trains on Next-Generation Communications Technology,”   
U.S. Navy, June 12, 2023, https://www.navy.mil/Press-Office/News-Stories/display-  
news/Article/3426428/eod-group-one-trains-on-next-generation-communications-  
technology/.  
60 Sicard, “Can Facial Recognition”; and David E. Sanger, Julian E. Barnes, and Kate   
Conger, “As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the   
War,” New York Times, February 28, 2022, https://www.nytimes.com/2022/02/28/us/

**Page 199**

193  
War and the Modern Battlefield  
politics/ukraine-russia-microsoft.html.  
61   
Brumfiel, “Israel is using.”  
62   
Rob Hastings, “Israel’s spies relied too much on tech over human informants   
before Hamas attack, ex-intelligence officer says,” The i Paper, October 11, 2023,   
https://inews.co.uk/news/world/israel-spies-tech-human-informants-hamas-attack-  
intelligence-officer-2680503?srsltid=AfmBOoqb4cbNmxA\_V6hNoY6f2ZtBmfNB\_cz\_  
GANyBTv4YY1pFWY5YXqC; Tia Goldenberg, “What went wrong? Questions emerge   
over Israel’s intelligence prowess after Hamas attack,” AP News, October 9, 2023,   
https://apnews.com/article/israel-hamas-gaza-attack-intel-a5287a18773232f26ca1712  
33be01721; and Ronen Bergman, Mark Mazzetti, and Maria Abi-Habib, “How Years of   
Israeli Failures on Hamas Led to a Devastating Attack,” New York Times, October 29,   
2023, https://www.nytimes.com/2023/10/29/world/middleeast/israel-intelligence-  
hamas-attack.html.  
63   
Geoff Brumfiel, “U.S. Navy Brings Back Navigation By The Stars For Officers,” NPR,   
February 22, 2016, https://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-  
navigation-by-the-stars-for-officers.  
THE EVOLUTION OF AIRPOWER  
1   
Giulio Douhet, Command of the Air, trans. Dino Ferrari (New York: Coward-McCann   
Inc., 1942), https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B\_0160\_  
DOUHET\_THE\_COMMAND\_OF\_THE\_AIR.PDF.  
2   
E.J. Kingston-McCloughry, War in Three Dimensions: The Impact of Air-Power Upon the   
Classical Principles of War (London: Jonathan Cape, 1949).  
3   
Fred C. Kelly, The Wright Brothers (San Diego, CA: Harcourt, Brace and Company, 1943),   
https://www.gutenberg.org/files/67672/67672-h/67672-h.htm.  
4   
U.S. Air Force, Air Force Doctrine Document 3-01: Counterair Operations (Washington,   
DC: U.S. Air Force, June 2023), https://www.doctrine.af.mil/Portals/61/documents/  
AFDP\_3-01/3-01-AFDP-COUNTERAIR.pdf.  
5   
Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms   
(Washington, DC: Joint Chiefs of Staff, November 2010), https://edocs.nps.edu/2014/  
December/jp1\_02.pdf.  
6   
U.S. Air Force, Counterair Operations.  
7   
David A. Deptula and Christopher J. Bowie, The Significance of Air Superiority: The   
Ukraine-Russia War (Arlington, VA: Mitchell Institute, July 2024), https://www.  
mitchellaerospacepower.org/the-significance-of-air-superiority-the-ukraine-russia-  
war/; and Douglass Barrie and Giorgio Di Mizio, “Moscow’s Aerospace Forces: No Air of   
Superiority,” IISS Military Balance (blog), February 2024, https://www.iiss.org/online-  
analysis/military-balance/2024/02/moscows-aerospace-forces-no-air-of-superiority/.  
8   
Yasir Atalan and Benjamin Jensen, “Breaking Down Russian Missile Salvos: What Drives   
Neutralization?,” CSIS, Commentary, February 24, 2025, https://www.csis.org/analysis/  
breaking-down-russian-missile-salvos-what-drives-neutralization.  
9   
Ibid.  
10   
Guy Faulconbridge and Anton Kolodyazhnyy, “Three killed in biggest Ukrainian drone   
attack on Moscow region,” Reuters, March 11, 2025, https://www.reuters.com/world/  
europe/ukraine-launches-drone-attacks-targeting-moscow-russia-says-2025-03-11/.  
11   
Kari Bingen and Clayton Swope, “Why the United States Acted Now Against Iran,” CSIS,   
Commentary, June 25, 2025, https://www.csis.org/analysis/why-united-states-acted-  
now-against-iran.  
12   
Paul Iddon, “Israel’s Air Force Blazes a Path to Iran’s Border,” Business Insider,   
January 2025, https://www.businessinsider.com/israeli-air-force-superiority-path-iran-  
border-2025-1; and Emanuel Fabian, “Israeli Air Force says it has achieved total air   
superiority above Syria,” Times of Israel, December 12, 2024, https://www.timesofisrael.

**Page 200**

194  
A Report of the CSIS Defense and Security Department  
com/liveblog\_entry/israeli-air-force-says-it-has-achieved-total-air-superiority-above-  
syria/.  
13   
Gerry Doyle, Mariano Zafra, Adolfo Arranz, and Jitesh Chowdhury, “Israel’s Iron   
Dome,” Reuters, April 18, 2024, https://www.reuters.com/graphics/ISRAEL-  
PALESTINIANS/IRAN-DEFENCE/mypmkljzopr/.  
14   
David Horovitz, “Israel warded off a huge Iranian attack, but that success is not the   
same as a victory,” Times of Israel, April 14, 2025, https://www.timesofisrael.com/israel-  
warded-off-a-huge-iranian-attack-but-that-success-is-not-the-same-as-a-victory/.  
15   
Atalan and Jensen, “Breaking Down Russian Missile Salvos.”  
16   
Kateryna Bondar, “How Ukraine’s Operation ‘Spider’s Web’ Redefines Asymmetric   
Warfare,” CSIS, Critical Questions, June 2, 2025, https://www.csis.org/analysis/why-  
united-states-acted-now-against-iran.  
17   
Steve Balestrieri, “F-35I Adir: The Isreali Fighter That Destroyed Iran’s Air Defenses,”   
19fortyfive, March 25, 2025, https://www.19fortyfive.com/2025/03/f-35i-adir-the-isreali-  
fighter-that-destroyed-irans-air-defenses/; and Isaac Stanley-Becker and Shane Harris,   
“How Israel Executed Its Surprise Assault on Iran,” The Atlantic, June 13, 2025, https://  
www.theatlantic.com/politics/archive/2025/06/how-israel-surprised-iran/683184/.  
18   
“IDF Reveals Full Story of How Houthi Drone Struck Tel Aviv,” Viewpoint Israel, July 25,   
2024, https://viewpointisrael.com/idf-reveals-full-story-of-how-houthi-drone-struck-tel-  
aviv/.  
19   
“How will mines dropped by drones change warfare?,” The Economist, January 31,   
2025, https://www.economist.com/the-economist-explains/2025/01/31/how-will-mines-  
dropped-by-drones-change-warfare.  
20   
Vikram Mittal, “Russia And Ukraine Are Using One-Time Use Drones. Future Wars   
May Not.,” Forbes, May 8, 2025, https://www.csis.org/programs/futures-lab/projects/  
russian-firepower-strike-tracker-analyzing-missile-attacks-ukraine.  
21   
Ibid.; Atalan and Jensen, “Breaking Down Russian Missile Salvos.”   
22   
 Peter Dickinson, “Ukrainian drones reportedly knock out 10 percent of Russian efining   
capacity,” Atlantic Council, February 13, 2025, https://www.atlanticcouncil.org/blogs/  
ukrainealert/ukrainian-drones-reportedly-knock-out-10-percent-of-russian-refining-  
capacity/; and Chaouki Chenai, “Countering the Growing Threat of Drone Attacks on   
Energy Infrastructure,” New Lines Institute, May 14, 2024, https://newlinesinstitute.  
org/environmental-challenges/countering-the-growing-threat-of-drone-attacks-on-  
energy-infrastructure/.  
23   
Brendan Cole, “Russia Loses $4 Million Worth of Tanks, IFVs in Ukraine Strike,”   
Newsweek, May 12, 2025, https://www.newsweek.com/russia-ukraine-tanks-ifvs-  
strike-2070894; and Francis Farrell, “‘He’s mine’ – How Ukraine’s ace drone unit   
hunts Russian soldiers near Kupiansk,” Kyiv Independent, January 9, 2025, https://  
kyivindependent.com/lacking-manpower-to-hold-back-russia-ukraine-turns-to-its-  
crack-drone-units/.  
24   
Fabian Hinz, “Made in Yemen? Assessing the Houthis’ arms-production capacity,” IISS   
Missile Dialogue Initiative, April 10, 2025, https://www.iiss.org/online-analysis/missile-  
dialogue-initiative/2025/04/made-in-yemen-assessing-the-houthis-arms-production-  
capacity/.  
25   
Kerry Chávez and Ori Swed, “How Hamas innovated with drones to operate like   
an army,” Bulletin of the Atomic Scientists, November 1, 2023, https://thebulletin.  
org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army.  
26   
Seth J. Frantzman, “Israel’s Aeronautics introduces loitering munition, surveillance   
drone combination,” Breaking Defense, June 14, 2024, https://breakingdefense.  
com/2024/06/israels-aeronautics-introduces-loitering-munition-surveillance-drone-  
combination/.  
27   
Harper Ellis, “How Effective are Loitering Munitions in Real Combat Scenarios?,”

**Page 201**

195  
War and the Modern Battlefield  
Defense Feeds, May 7, 2025, https://defensefeeds.com/analysis/weapons/loitering-  
munitions/.  
28   
Yonah Jeremy Bob, “Israeli drone power: How UAVs have taken the IDF to a new level,”   
Jerusalem Post, June 2, 2023, https://www.jpost.com/israel-news/article-744845; “Qods   
Mohajer UAV,” War Wings Daily, https://warwingsdaily.com/drones-uavs-ucavs/qods-  
mohajer-uav/; and Emanuel Fabian, “IDF shoots down Hezbollah surveillance drone,   
in first such incident since ceasefire Terror group appears to violate US-brokered truce   
days after IDF struck,” Times of Israel, January 30, 2025, https://www.timesofisrael.  
com/idf-shoots-down-hezbollah-surveillance-drone-in-first-such-incident-since-  
ceasefire/.  
29   
Stefan Korshak, “Ukraine Drone Production Tops 2.5 Million a Year, Aircraft Numbers   
on Track to Grow,” Kyiv Post, February 10, 2025, https://www.kyivpost.com/post/46892.  
30   
Sofiia Syngaivska, “Ukraine Deploys World’s First Drone-Based Air Defense: the   
Nemesis Regiment Downs 60 Shahed and Geran Drones in Two Months,” Defense   
Express, May 1, 2025, https://en.defence-ua.com/analysis/ukraine\_deploys\_worlds\_first\_  
drone\_based\_air\_defense\_the\_nemesis\_regiment\_downs\_60\_shahed\_and\_geran\_drones\_  
in\_two\_months-14369.html.  
31   
“Use It, Don’t Lose It: The Case for Recoverable and Reusable Loitering Munitions,”   
Teledyne FLIR, April 28, 2025, https://www.flir.com/discover/government-defense/use-  
it-dont-lose-it-the-case-for-recoverable-and-reusable-loitering-munitions/.  
32   
“Ships, trucks, and suitcases: How Israel reportedly got its attack drones into Iran,”   
Times of Israel, June 15, 2025, https://www.timesofisrael.com/ships-trucks-and-  
suitcases-how-israel-reportedly-got-its-attack-drones-into-iran/; and Tom Balmforth   
and Max Hunder, “To attack Russian air bases, Ukrainian spies hid drones in wooden   
sheds,” Reuters, June 1, 2025, https://www.reuters.com/business/aerospace-  
defense/ukraine-stages-major-attack-russian-aircraft-with-drones-security-official-  
says-2025-06-01/.  
33   
Paul Mozur and Adam Satariano, “Russia, in New Push, Increasingly Disrupts   
Ukraine’s Starlink Service,” New York Times, May 25, 2024, https://www.nytimes.  
com/2024/05/24/technology/ukraine-russia-starlink.html; and Thomas Gibbons-  
Neff and Yurii Shyvala, “‘Jamming’: How Electronic Warfare Is Reshaping Ukraine’s   
Battlefields,” New York Times, March 12, 2024, https://www.nytimes.com/2024/03/12/  
world/europe/ukraine-drone-russia-jamming.html.  
34   
David Hambling, “Jam-Resistant American Radio Keeps Ukraine’s Long-  
Range Drones Flying,” Forbes, April 17, 2024, https://www.forbes.com/sites/  
davidhambling/2024/04/17/jam-resistant-american-radio-keeps-ukraines-long-range-  
drones-flying/; and David Hambling, “Inside The ‘Magic Radio’ Protecting Russian   
Drones From Jamming,” Forbes, December 20, 2023, https://www.forbes.com/sites/  
davidhambling/2023/12/20/inside-the-magic-radio-protecting-russian-drones-from-  
jamming/.  
35   
“Phalanx Weapon System,” RTX, https://www.rtx.com/raytheon/what-we-do/sea/  
phalanx-close-in-weapon-system; and “Harpy NG,” IAI, https://www.iai.co.il/sites/  
default/files/2023-06/HARPY%20Brochure.pdf.  
36   
Tess Horlings, Roy Lindelauf, and Sebastiaan Rietjens, “Battling information overload   
in military intelligence & security organisations,” in Towards a Data-Driven Military: A   
Multidisciplinary Perspective, eds. Peter B.M.J. Pijpers, Mark Voskuijl, and Robert J.M.   
Beeres (Leiden, Netherlands: Leiden University Press, 2023), https://www.jstor.org/  
stable/jj.14250136.16?seq=1.  
37   
Serhiy Horbatenko, “Fiber-Optic Ukrainian Ground Drones Keep Critical Supplies   
Moving to the Front,” Radio Free Europe Radio Liberty, May 15, 2025, https://www.  
rferl.org/a/ukraine-war-fiber-optic-ground-drones-supplies/33415190.html; “Strategic   
Blindness: the Effect of Ukraine’s Attack on Voronezh-M Over-the-Horizon Radar in   
Orsk Explained,” Defense Express, May 27, 2024, https://en.defence-ua.com/news/  
strategic\_blindness\_the\_effect\_of\_ukraines\_attack\_on\_voronezh\_m\_over\_the\_horizon\_  
radar\_in\_orsk\_explained-10643.html; and “Israeli researchers develop AI-based radar

**Page 202**

196  
A Report of the CSIS Defense and Security Department  
system to detect hostile drones in bad weather,” All Israel News, July 24, 2024, https://  
allisrael.com/israeli-researchers-develop-ai-based-radar-system-to-detect-hostile-  
drones-in-bad-weather.  
38   
“Bullfrog M2,” Allen Control Systems, https://www.allencontrolsystems.com/products/  
bullfrog-m2.  
39   
Avi Goldfarb and Jon R. Lindsay, “Prediction and Judgment: Why Artificial Intelligence   
Increases the Importance of Humans in War,” International Security 46, no. 3 (2022),   
https://doi.org/10.1162/isec\_a\_00425.  
40 Bill Hutchinson, “High-tech radar used in Ukraine-Russia war to be deployed to crack   
Northeast drone mystery,” ABC News, December 17, 2024, https://abcnews.go.com/US/  
high-tech-radar-ukraine-russia-war-deployed-crack/story?id=116822053.  
41   
Editorial Team, “Understanding Integrated Air Defense Systems for Modern Warfare,”   
Total Military Insight, June 25, 2024, https://totalmilitaryinsight.com/integrated-air-  
defense-systems/.  
42   
Martin Blass, Stefan Grebien, and Franz Graf, “Experimental Evaluation of Acoustic   
Drone Tracking using Mobile Microphone Arrays,” presented at Quietdrones 2024,   
University of Salford, Manchester, UK, September 2024, https://www.researchgate.net/  
publication/383877168\_Experimental\_Evaluation\_of\_Acoustic\_Drone\_Tracking\_using\_  
Mobile\_Microphone\_Arrays; and Peter Karanja, “How to Detect a Drone in the Sky,”   
Drone Blog, March 16, 2022, https://www.droneblog.com/detect-a-drone/.  
43   
Tate Nurkin, et al., China’s Remote Sensing (Washington, DC: U.S. China-Economic and   
Security Review Commission, December 2024), https://www.uscc.gov/sites/default/  
files/2024-12/Chinas\_Remote\_Sensing.pdf.  
44   
Clayton Swope, “No Place to Hide: A Look into China’s Geosynchronous Surveillance   
Capabilities,” CSIS, Critical Questions, January 19, 2024, https://www.csis.org/analysis/  
no-place-hide-look-chinas-geosynchronous-surveillance-capabilities.  
45   
Theresa Hitchens and Michael Marrow, “Space Force testing space-based sensors to   
track airborne targets,” Breaking Defense, May 15, 2025, https://breakingdefense.  
com/2025/05/space-force-testing-space-based-sensors-to-track-airborne-targets/.  
46   
“ADAPTIV - Cloak of Invisibility,” BAE Systems, https://www.baesystems.com/en/  
feature/adativ-cloak-of-invisibility.  
47   
William Mitchell, Winged Defense: The Development and Possibilities of Modern Air   
Power—Economic and Military (Mineola, NY: Dover Publications, 2006), 20.   
THE FUTURE OF SEAPOWER  
1   
For a description of these successes, see Mark F. Cancian, “Ukraine’s Victory at Sea:   
How Kyiv Subdued the Russian Fleet—and What It Will Need to Build on Naval Success,”   
Foreign Affairs, February 8, 2024, https://www.foreignaffairs.com/ukraine/ukraines-  
victory-sea.  
2   
Jakub Janovsky et al., “Attack on Europe: Documenting Russian Equipment Losses   
During the Russian Invasion Of Ukraine,” Oryx, February 24, 2022, https://www.  
oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.  
3   
Mark F. Cancian, Matt Cancian, and Eric Heginbotham, The First Battle of the Next   
War: Wargaming a Chinese Invasion of Taiwan (Washington, DC: Center for Strategic   
and International Studies, January 2023), https://www.csis.org/analysis/first-battle-  
next-war-wargaming-chinese-invasion-taiwan; Bryan Clark and Timothy A. Walton,   
Taking Back the Seas: Transforming the U.S. Surface Fleet for Decision-Centric Warfare   
(Washington, DC: Center for Strategic and Budgetary Assessments, December 2024),   
https://csbaonline.org/research/publications/taking-back-the-seas-transforming-  
the-u.s-surface-fleet-for-decision-centric-warfare; Bryan Clark and Michael G.   
Roberts, Shoring Up the Foundation: Affordable Approaches to Improve U.S. and Allied   
Shipbuilding and Ship Repair (Washington, DC: Hudson Institute, December 2024),   
https://www.hudson.org/supply-chains/shoring-foundation-affordable-approaches-

**Page 203**

197  
War and the Modern Battlefield  
improve-us-allied-shipbuilding-ship-repair-bryan-clark-michael-roberts; and Johannes   
R. Fischbach, Closing the Gap: China Homes in on US Navy VLS Advantage (London:   
International Institute for Strategic Studies, December 2024), https://www.iiss.org/  
online-analysis/military-balance/2024/12/closing-the-gap-china-homes-in-on-us-navy-  
vls-advantage/.   
4   
Note for the cognoscenti: Doenitz appears to be holding a model of a Type XXIII   
U-boat.   
5   
“Ship Battle Forces,” Naval Vessel Registry, U.S. Navy, accessed July 27, 2025, https://  
www.nvr.navy.mil/nvr/getpage.htm?pagetype=shipbattleforce.  
6   
Ronald O’Rourke, Navy Force Structure and Shipbuilding Plans: Background and Issues   
for Congress, CRS Report No. RL32665 (Washington, DC: Congressional Research   
Service, April 2025), https://sgp.fas.org/crs/weapons/RL32665.pdf.   
7   
Office of the Chief of Naval Operations, Report to Congress on the Annual Long-Range   
Plan for Construction of Naval Vessels for Fiscal Year 2025 (Washington, DC: Office of the   
Chief of Naval Operations, March 2024), 20 (Table A1-5), https://s3.amazonaws.com/  
static.militarytimes.com/assets/pdfs/1710968056.pdf.  
8   
Sam LaGrone and Mallory Shelbourne, “New Navy Long-Range Shipbuilding Plan   
Details 19 Ship Decommissionings in FY 2025,” U.S. Naval Institute News, March 19,   
2024, https://news.usni.org/2024/03/19/new-navy-long-range-shipbuilding-plan-details-  
19-ship-decommissionings-in-fy-2025.   
9   
Thirty-five years may be optimistic. For a detailed discussion of ship service lives, see   
Steven Wills, “Running Ahead of the Rust: The Dangers of Extending Warship Service   
Lives,” Center for Maritime Strategy, June 6, 2023, https://centerformaritimestrategy.  
org/publications/running-ahead-of-the-rust-the-dangers-of-extending-warship-service-  
lives/.  
10   
The reconciliation bill was negotiated between Congress, principally the Armed   
Services Committees, and the White House but drew most of its inspiration from   
congressional documents, for example, Sen. Wicker’s “21st Century Peace Through   
Strength: A Generational Investment in the U.S. Military,” https://www.wicker.senate.  
gov/services/files/BC957888-0A93-432F-A49E-6202768A9CE0.  
11   
International Institute for Strategic Studies, “Chapter Five: Asia,” The Military Balance   
125, no.1 (2025), 243, https://doi.org/10.1080/04597222.2025.2445477.  
12   
Ibid.  
13   
U.S. Department of Defense, Military and Security Developments Involving the People’s   
Republic of China 2024 (Washington, DC: U.S. Department of Defense, December 2024),   
https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-  
DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.  
14   
Mark F. Cancian, “Who’s Responsible for the Navy’s Carrier Shortage?,” War on the   
Rocks, August 12, 2016, https://warontherocks.com/2016/08/whos-responsible-for-the-  
navys-carrier-shortage/.   
15   
 Mark F. Cancian, U.S. Military Forces in FY 2022: Peering into the Abyss (Washington,   
C: Center for Strategic and International Studies, March 2022), https://www.csis.org/  
analysis/us-military-forces-fy-2022-peering-abyss.  
16   
Thomas Newdick, “HMS Queen Elizabeth Is First British Carrier To Send Jets Into   
Combat In Over Two Decades,” The War Zone, November 17, 2021, https://www.twz.  
com/41213/hms-queen-elizabeth-is-first-british-carrier-to-send-jets-into-combat-in-over-  
two-decades; and Fred Pleitgen, “On board the French nuclear carrier battling ISIS,”   
CNN, October 17, 2016, https://www.cnn.com/2016/10/17/middleeast/france-nuclear-  
carrier-mosul-iraq-isis/index.html.  
17   
Jonathan Beale, “On board the pride of the French navy,” BBC, May 27, 2011, https://  
www.bbc.com/news/world-europe-13573848; and Norman Friedman, “British   
Aircraft Carriers Returns,” Proceedings 147, no. 8 (August 2017), https://www.usni.org/  
magazines/proceedings/2017/august/british-aircraft-carriers-return.

**Page 204**

198  
A Report of the CSIS Defense and Security Department  
18   
For data on carrier fleets in 1975, see John Moore ed., Jane’s Fighting Ships 1974-  
1975(London: Macdonald and Janes, 1975), 642.  
19   
Mark F. Cancian, “Penny Wise and Pound Foolish: The Navy’s Carrier Construction   
Strategy,” Proceedings 145, no. 3 (March 2019), https://www.usni.org/magazines/  
proceedings/2019/march/penny-wise-and-pound-foolish-navys-carrier-construction-  
strategy.  
20   
Mark F. Cancian, Inflicting Surprise: Gaining Competitive Advantage in Great Power   
Conflicts (Washington, DC: Center for Strategic and International Studies, January   
2021), https://www.csis.org/analysis/inflicting-surprise-gaining-competitive-advantage-  
great-power-conflicts.   
21   
Geoff Ziezulewicz, “What the Navy’s Massive Orca Submarine Drone Is Actually   
Capable Of,” The War Zone, January 14, 2025, https://www.twz.com/news-features/  
what-the-navys-massive-orca-submarine-drone-is-actually-capable-of.  
22   
U.S. Government Accountability Office, Extra Large Unmanned Undersea Vehicle: Navy   
Needs to Employ Better Management Practices to Ensure Swift Delivery to the Fleet, GAO-  
22-105974 (Washington, DC: Government Accountability Office, September 2022),   
https://www.gao.gov/products/gao-22-105974.  
23   
The U.S. Navy’s last 30-year shipbuilding program envisioned 134 “unmanned   
vehicles” in the fleet, but all recent Navy and DOD naval force structures have included   
large numbers of USVs and UUVs. See Chief of Naval Operations, Report to Congress,   
4. The Navy has asked industry what technologies might be available, but the effort is   
a long way from a fielded capability. See Sam LaGrone and Aaron-Matthew Lariosa,   
“Pentagon Puts Out Call for Swarming Attack Drones That Could Blunt a Taiwan   
Invasion,” U.S. Naval Institute, January 30, 2024, https://news.usni.org/2024/01/30/  
pentagon-puts-out-call-for-swarming-attack-drones-that-could-blunt-a-taiwan-invasion.  
24   
Xavier Vavasseur, “UK’s CETUS XLUUV launched by MSubs in Plymouth,” Naval News,   
May 3, 2025, https://www.navalnews.com/naval-news/2025/03/uks-cetus-xluuv-  
launched-by-msubs-in-plymouth/.  
25   
Kiran Suman-Chauhan, Nicolas Jouan, and James Black, “Navies Look to Uncrewed   
Systems to Counter Threats Beneath the Waves,” RAND Corporation, May 21, 2024,   
https://www.rand.org/pubs/commentary/2024/05/navies-look-to-uncrewed-systems-  
to-counter-threats.html.  
26   
“Cole (DDG-67),” Naval History and Heritage Command, U.S. Navy, https://www.  
history.navy.mil/browse-by-topic/ships/modern-ships/uss-cole.html.   
27   
“Japanese Midget Submarines,” Naval History and Heritage Command, U.S. Navy,   
https://www.history.navy.mil/our-collections/photography/wars-and-events/world-  
war-ii/pearl-harbor-raid/japanese-forces-in-the-pearl-harbor-attack/japanese-midget-  
submarines-used-in-the-attack-on-pearl-harbor.html.   
28   
I.e., a significant nonevent. See the famous incident in the Sherlock Holmes story   
“The Adventure of Silver Blaze,” in which a dog should have barked at an intruder, but   
didn’t.  
29   
Geoff Ziezulewicz, “Navy Just Revealed Tally Of Surface-To-Air Missiles Fired In Ongoing   
Red Sea Fight,” The War Zone, January 14, 2025, https://www.twz.com/news-features/  
navy-just-disclosed-how-many-of-each-of-its-surface-to-air-missiles-it-fired-during-red-  
sea-fight.   
30   
Department of Defense, Department of the Navy Fiscal Year (FY) 2025 Budget Estimates   
Justification Book, Weapons Procurement (Washington, DC: Department of Defense,   
2024), xiii, https://www.secnav.navy.mil/fmc/fmb/Documents/25pres/WPN\_Book.pdf.   
31   
Cancian, Cancian and Heginbotham, The First Battle, 88.  
32   
Seth Jones, Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense   
Industrial Base (Washington, DC: Center for Strategic and International Studies,   
January 2023), https://www.csis.org/analysis/empty-bins-wartime-environment-  
challenge-us-defense-industrial-base.

**Page 205**

199  
War and the Modern Battlefield  
33   
For example, Michael Brown, “The Empty Arsenal of Democracy,” Foreign Affairs, April   
22, 2025, https://www.foreignaffairs.com/united-states/empty-arsenal-democracy-  
michael-brown; Tyler Hacker, “Money Isn’t Enough: Getting Serious About Precision   
Munitions,” War on the Rocks, April 24, 2023, https://warontherocks.com/2023/04/  
money-isnt-enough-getting-serious-about-precision-munitions/; and Stacie Pettyjohn   
and Hannah Dennis, “The Pentagon Isn’t Buying Enough Ammo,” Foreign Policy,   
May 21, 2024, https://foreignpolicy.com/2024/05/21/united-states-defense-pentagon-  
military-industrial-base-ammunition/.   
34   
Sebastian Roblin, “How the Falklands War (Thanks to a Stealthy Submarine)   
Could Have Gone Very Differently,” National Interest, November 28, 2016, https://  
nationalinterest.org/blog/buzz/how-the-falklands-war-thanks-stealthy-submarine-  
could-have-18495.  
35   
DOD, FY 2025 Budget Estimates Justification Book, 233.  
36   
Nathan Gain, “NATO countries sign MoU on Maritime Battle Decisive Munitions   
initiative,” Naval News, June 27, 2019, https://www.navalnews.com/naval-  
news/2019/06/nato-countries-sign-mou-on-maritime-battle-decisive-munitions-  
initiative/; and Sabine Siebold, “Germany, eight other Baltic Sea nations seek to jointly   
buy naval mines,” Reuters, July 9, 2024, https://www.reuters.com/world/europe/  
germany-eight-other-baltic-sea-nations-seek-jointly-buy-naval-mines-2024-07-09/.  
37   
Costs from DOD, FY 2025 Budget Estimates Justification Book, 123, 233; service life from   
AMRDEC Public Affairs, “Army researchers extend missile system shelf life,” U.S. Army,   
October 19, 2015, https://www.army.mil/article/156942/army\_researchers\_extend\_  
missile\_system\_shelf\_life.  
THE EVOLUTION OF IRREGULAR WARFARE  
1   
As used here, “irregular warfare” refers to activities short of conventional and nuclear   
warfare that are designed to expand a country’s influence and legitimacy. These   
activities include information and cyber operations, support to nonstate actors like   
partisans and terrorists, covert action, and economic coercion. Irregular warfare can   
occur as a prelude to, in conjunction with, or independently from a conventional   
attack.  
2   
Oleksandr V. Danylyuk, “Against the Odds: Lessons from the Ukrainian Resistance   
Movement,” Royal United Services Institute, July 4, 2023, https://www.rusi.org/explore-  
our-research/publications/commentary/against-odds-lessons-ukrainian-resistance-  
movement; and Jade McGlynn, Crossing Thresholds: Ukrainian Resistance to Russian   
Occupation (Washington, DC: CSIS, June 2024), https://www.csis.org/analysis/crossing-  
thresholds-ukrainian-resistance-russian-occupation.  
3   
Doug Livermore, “Ukraine’s Railway Wars: How to Sabotage Russian Military Logistics,”   
Irregular Warfare, January 10, 2025, https://irregularwarfare.org/articles/ukraines-  
railway-wars-how-to-sabotage-russian-military-logistics/; and Isabel van Brugen,   
“Russian Railway Networks Facing ‘Imminent Collapse’: Report,” Newsweek, August   
6, 2024, https://www.newsweek.com/russian-railway-collapse-sanctions-ukraine-  
war-1935049.  
4   
OHCHR, “Number of civilian casualties in Ukraine during Russia’s invasion verified   
by OHCHR from February 2022 to August 2024, by month,” Statista, October 1, 2024,   
https://www.statista.com/statistics/1318455/ukraine-war-casualties-monthly/.  
5   
Jessica Parker, “Ukraine Says It Blew up Railway in Eastern Russia,” BBC News,   
December 1, 2023, https://www.bbc.com/news/world-europe-67593041.  
6   
“Swords of Iron: IDF Casualties,” Israeli Ministry of Foreign Affairs, March 11, 2023,   
https://www.gov.il/en/pages/swords-of-iron-idf-casualties.  
7   
Jennifer Hassan and Adam Taylor, “Israel’s Massive Mobilization of 360,000 Reservists   
Upends Lives,” Washington Post, October 10, 2023, https://www.washingtonpost.com/  
world/2023/10/10/israel-military-draft-reservists/.

**Page 206**

200  
A Report of the CSIS Defense and Security Department  
8   
Anatoly Kurmanaev and Constant Méheut, “Ukraine Is Losing Fewer Soldiers than   
Russia - but It’s Still Losing the War,” New York Times, January 23, 2025, https://www.  
nytimes.com/2025/01/23/world/europe/ukraine-russia-soldiers-loss.html.  
9   
Gwyn Topham, “Thousands of Flights to and from Europe Affected by Suspected   
Russian Jamming,” The Guardian, April 22, 2024, https://www.theguardian.com/  
business/2024/apr/22/thousands-of-flights-to-and-from-europe-affected-by-suspected-  
russian-jamming; Andy Greenberg, “Hackers Linked to Russia’s Military Claim Credit   
for Sabotaging US Water Utilities,” Wired, April 17, 2024, https://www.wired.com/story/  
cyber-army-of-russia-reborn-sandworm-us-cyberattacks/; and Laura Kayali et al.,   
“Europe Is under Attack from Russia. Why Isn’t It Fighting Back?,” Politico, November   
25, 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-  
germany-cyberattacks-election-interference/.  
10   
Sébastian Seibt, “Suspected Russian Sabotage: The Great Return of Kremlin Agents to   
Europe?,” France 24, May 10, 2024, https://www.france24.com/en/europe/20240510-  
suspected-russian-sabotage-campaigns-great-return-russian-agents-europe; and   
Matthew M. Burke, “Trio Charged in Germany for Pro-Russia Plot Targeting US Bases   
in Bavaria,” Stars and Stripes, December 31, 2024, https://www.stripes.com/branches/  
army/2024-12-31/dual-nationals-charged-spying-russia-16331452.html.  
11   
Ukrainian Ministry of Reintegration and the National Information Bureau, Діти   
війни [Children of War], https://childrenofwar.gov.ua/en; and Kristina Hook, The   
Russian Federation’s Escalating Commission of Genocide in Ukraine: A Legal Analysis   
(Washington, DC: New Lines Institute, July 26, 2023), https://newlinesinstitute.org/  
wp-content/uploads/20230726-Genocide-Ukraine-Report-NISLAP\_.pdf.  
12   
RFE/RL’s Ukrainian Service and RFE/RL’s Russian Service, “‘Liquidated’: Two ‘Traitors   
Of Ukraine’ Killed In Separate Incidents,” RadioFreeEurope/RadioLiberty, December   
7, 2023, https://www.rferl.org/a/ukraine-russia-kyva-popov-sbu-investigative-  
committee/32718964.html.  
13   
Kate Connolly, “US Reportedly Foiled Russian Plot to Kill Boss of German Arms Firm   
Supplying Ukraine,” The Guardian, July 11, 2024, https://www.theguardian.com/world/  
article/2024/jul/11/us-reportedly-foiled-russian-plot-to-kill-boss-of-german-arms-firm-  
supplying-ukraine; and “Russian agents killed after assassinating Ukraine colonel, Kyiv   
Says,” CBS News, July 13, 2025, https://www.cbsnews.com/news/russian-agents-killed-  
assassination-ukraine-colonel-kyiv-says/.  
14   
Edward Wong, Julian E. Barnes, and Eric Schmitt, “Israel Has Destroyed Half of   
Hezbollah’s Arsenal, U.S. and Israeli Officials Say,” New York Times, October 1, 2024,   
https://www.nytimes.com/2024/10/01/us/politics/israel-lebanon-hezbollah-airstrikes.  
html; and Seth G. Jones et al., The Coming Conflict with Hezbollah (Washington, DC:   
CSIS, March 21, 2024), https://www.csis.org/analysis/coming-conflict-hezbollah.  
15   
Becky Sullivan and Kat Lonsdorf, “3 Hostages Killed by Israeli Soldier in Gaza Were   
Waving a White Flag, Israel Says,” NPR, December 16, 2023, https://www.npr.  
org/2023/12/15/1219695220/israel-soldiers-mistakenly-kill-hostages-gaza.  
16   
Timour Azhari, “Kataib Hezbollah: Why Iran Ally in Iraq Stood down after US Attacks,”   
Reuters, February 1, 2024, https://www.reuters.com/world/middle-east/how-an-  
iranian-ally-iraq-was-made-stand-down-2024-01-31/.  
17   
Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds, The Threat from Russia’s   
Unconventional Warfare Beyond Ukraine, 2022–2024 (London: Royal United Services   
Institute, February 2024), https://static.rusi.org/SR-Russian-Unconventional-Weapons-  
final-web.pdf.  
18   
U.S. Army, Army Multi-Domain Transformation: Ready to Win in Competition and Conflict   
(Washington, DC: Headquarters, Department of the Army, March 16, 2021), 5, https://  
api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-  
version.pdf.  
19   
Eric Schmitt and Farnaz Fassihi, “Iran Likely Will Strike Israel, Not U.S. Forces,   
U.S. and Iranian Officials Say,” New York Times, April 12, 2024, https://www.  
nytimes.com/2024/04/12/world/middleeast/american-intelligenc.html; and

**Page 207**

201  
War and the Modern Battlefield  
I.R.IRAN Mission to UN, NY (@Iran\_UN), “Conducted on the strength of Article   
51 of the UN Charter pertaining to legitimate defense, Iran’s military action was   
in response to the Zionist regime’s aggression against our diplomatic premises   
in Damascus. The matter can be deemed concluded. However, should the Israeli   
regime make another mistake, Iran’s response will be considerably more severe.   
It is a conflict between Iran and the rogue Israeli regime, from which the U.S.   
MUST STAY AWAY!,” X post, April 13, 2024, 6:06 pm, https://x.com/iran\_un/  
status/1779269993043022053?s=58&t=qm1hvFA9ri9r73laNoAV1w&mx=2.  
DEFENSE BUDGETS IN AN UNCERTAIN SECURITY ENVIRONMENT  
1   
“Defense Funding in the 2025 Reconciliation Law (H.R. 1; P.L. 119-21, Title II),”   
Congressional Research Service, IN12580, Updated July 24, 2025, https://www.  
congress.gov/crs\_external\_products/IN/PDF/IN12580/IN12580.4.pdf.   
2   
“Defence expenditures and NATO’s 5% commitment,” NATO, August 27, 2025, https://  
www.nato.int/cps/en/natohq/topics\_49198.htm.  
3   
Analysis based on data published by NATO in “Defence Expenditure of NATO Countries   
(2014-2025),” NATO, August 28, 2025, https://www.nato.int/cps/en/natohq/news\_237171.  
htm  
4   
Iceland is not represented on any figures in this report as it has no armed forces.  
5   
Bastian Giegerich and Ben Schreer, “Zeitenwende one year on,” International Institute   
for Strategic Studies, February 27, 2023, https://www.iiss.org/ar-BH/online-analysis/  
online-analysis/2023/02/zeitenwende-one-year-on/   
6   
Ibid.; Sebastian Shukla, Claudia Otto, and Nadine Schmidt, “Germany is unlocking   
billions to supercharge its military at a seismic moment for Europe,” CNN, March 23,   
2025, https://www.cnn.com/2025/03/23/europe/germany-military-investment-intl.   
7   
Ibid.; Frank Gardner and Toby Luckhurst, “Germany votes for historic boost to defence   
spending,” BBC, March 18, 2025, https://www.bbc.com/news/articles/c62z6gljv2yo;   
Saim Dušan Inayatullah, “Germany aims to have ‘strongest’ military in Europe — Merz,”   
DW, May 5, 2025, https://www.dw.com/en/germany-aims-to-have-strongest-military-in-  
europe-merz/a-72546478.   
8   
Michał Oleksiejuk, “Sharing the burden: How Poland and Germany are shifting the dial   
on European defence expenditure,” NATO Review, April 18, 2025, https://www.nato.int/  
docu/review/articles/2025/04/14/sharing-the-burden-how-poland-and-germany-are-  
shifting-the-dial-on-european-defence-expenditure/index.html.   
9   
Ibid.; Kateryna Kvasha, ““Security, Europe!”: Poland’s Rise as NATO’s Defense   
Spending Leader,” Wilson Center, March 6, 2025, https://www.wilsoncenter.org/article/  
security-europe-polands-rise-natos-defense-spending-leader.   
10   
Prime Minister's Office, "Prime Minister sets out biggest sustained increase in defence   
spending since the Cold War, protecting British people in new era for national   
security," press release, February 25, 2025, https://www.gov.uk/government/news/  
prime-minister-sets-out-biggest-sustained-increase-in-defence-spending-since-the-cold-  
war-protecting-british-people-in-new-era-for-national-security; and Keir Starmer, "PM   
statement on defence spending: 25 February 2025," Prime Minister's Office, February   
25, 2025, https://www.gov.uk/government/speeches/pm-statement-on-defence-  
spending-25-february-2025.  
11   
“Press statement by President von der Leyen on the defence package,” European   
Commission, March 3, 2025, https://ec.europa.eu/commission/presscorner/detail/et/  
statement\_25\_673.  
12   
“ReArm Europe Plan / Readiness 2030,” European Commission, 2025, https://  
defence-industry-space.ec.europa.eu/document/download/13ec18d2-8366-4fc8-a4ff-  
2bdfdf8e1f5f\_en?filename=REARM%20Europe%20factsheet%20v17\_1.pdf; “Press   
statement by President von der Leyen on the defence package,” March 3, 2025; Sophie   
Kiderlin and Silvia Amaro, “European leaders push for even more defense spending —

**Page 208**

202  
A Report of the CSIS Defense and Security Department  
despite plans for $867 billion ‘ReArm’ package,” CNBC, March 20, 2025, https://www.  
cnbc.com/2025/03/20/european-leaders-push-for-even-more-defense-spending.html.  
13   
Ibid.  
14   
Holly Ellyatt, "Can Trump force the hand of NATO allies to spend up to 5% of GDP on   
defense?," CNBC, January 23, 2025, https://www.cnbc.com/2025/01/23/can-trump-get-  
nato-allies-to-spend-more-on-defense.html.  
15   
Laura Kayali and Antoaneta Roussi, “NATO allies agree to boost weapon inventories   
ahead of Trump-pleasing Summit,” POLITICO, June 5, 2025, https://www.politico.eu/  
article/nato-allies-weapon-inventories-defense-spending-donald-trump/.   
16   
 The Hague Summit Declaration, NATO, June 25, 2025, https://www.nato.int/cps/en/  
atohq/official\_texts\_236705.htm; Mark Rutte, NATO Press Conference, June 5, 2025,   
https://www.nato.int/cps/en/natohq/opinions\_235894.htm.   
17   
“Defence Expenditure of NATO Countries (2014-2025),” NATO, August 28, 2025, https://  
www.nato.int/cps/en/natohq/news\_226465.htm.   
18   
Seamus P. Daniels and Todd Harrison, “What Does the Bipartisan Budget Act of 2019   
Mean for Defense?” Center for Strategic and International Studies, August 5, 2019,   
https://www.csis.org/analysis/what-does-bipartisan-budget-act-2019-mean-defense.   
19   
Seamus P. Daniels, “What the Fiscal Responsibility Act of 2023 Means for Defense   
Spending,” Center for Strategic and International Studies, June 15, 2023, https://www.  
csis.org/analysis/what-fiscal-responsibility-act-2023-means-defense-spending.   
20   
Letter, CBO to Senator Jeff Merkley, “Effects on Deficits and the Debt of Public Law   
119-21 and of Making Certain Tax Policies in the Act Permanent,” Congressional Budget   
Office, August 4, 2025, https://www.cbo.gov/system/files/2025-08/61466-DebtService.  
pdf.   
21   
Roger Wicker, “Chairman Wicker Releases Statement on the FY26 Budget Proposal,”   
May 2, 2025, https://www.wicker.senate.gov/2025/5/chairman-wicker-releases-  
statement-on-the-fy26-budget-proposal.  
22   
“SIPRI Military Expenditure Database, 1949-2024,” Stockholm International Peace   
Research Institute, https://www.sipri.org/databases/milex.  
23   
See Julian Cooper, Preparing for a Fourth Year of War: Military Spending in Russia’s   
Budget for 2025, SIPRI Insights on Peace and Security, No. 2025/04, Stockholm   
International Peace Research Institute, April 2025, https://www.sipri.org/sites/default/  
files/2025-04/preparing\_for\_a\_fourth\_year\_of\_war-military\_spending\_in\_russias\_budget\_  
for\_2025\_1.pdf.   
24   
Ibid.  
25   
Xiao Liang, et. al., Trends in World Military Expenditure, 2024, SIPRI Fact Sheet,   
Stockholm International Peace Research Institute, April 2025, https://www.sipri.org/  
sites/default/files/2025-04/2504\_fs\_milex\_2024.pdf.   
26   
Ibid., 5.  
27   
Alexandra Prokopenko, “Putin’s insatiable appetite for war,” Financial Times, June 5,   
2025, https://www.ft.com/content/2278e8c6-d8c9-4860-89e0-fc6c7d69b2e1.   
28   
Christopher Bodeen, “China will increase its defense Budget 7.2% this year,” AP, March   
5, 2025, https://apnews.com/article/china-defense-budget-taiwan-4ac7cbdc7d5b8897  
32cd55916ff7eb36; M. Taylor Fravel, George J. Gilboy, Eric Heginbotham, “Estimating   
China’s Defense Spending: How to Get It Wrong (and Right),” Texas National Security   
Review, Vol. 7, Issue 3, Summer 2024, 40-54, https://tnsr.org/2024/06/estimating-  
chinas-defense-spending-how-to-get-it-wrong-and-right/.   
29   
“What Does China Really Spend on its Military?,” CSIS, ChinaPower, updated March 5,   
2025, https://chinapower.csis.org/ military-spending/.  
30   
Cooper, Preparing for a Fourth Year of War.

**Page 209**

203  
War and the Modern Battlefield  
31   
Mary Ilyushina, “Putin says he won’t allow Russia to fall into recession amid warnings,”   
Washington Post, June 20, 2025, https://www.washingtonpost.com/world/2025/06/20/  
putin-says-he-wont-allow-russia-fall-into-recession-amid-gloomy-economy/; “Russia’s   
Year of Truth: The Runaway Military Budget,” Center for European Policy Analysis,   
January 22, 2025, https://cepa.org/article/russias-year-of-truth-the-runaway-military-  
budget/.   
32   
Prokopenko, “Putin’s insatiable appetite for war.”  
33   
Fenella McGerty, “European defence funding: fiscal manoeuvres,” International   
Institute for Strategic Studies, March 13, 2025, https://www.iiss.org/online-analysis/  
military-balance/2025/03/european-defence-funding-fiscal-manoeuvres/.  
34   
Todd Harrison and Seamus P. Daniels, Analysis of the FY 2021 Defense Budget, Center   
for Strategic and International Studies, August 2020, https://defense360.csis.org/  
wp-content/uploads/2020/08/Analysis-of-the-FY-2021-Defense-Budget.pdf.  
INDUSTRIAL ROADBLOCKS: PRODUCING AT A SCALE AND   
ADOPTING NEW TECHNOLOGIES  
1   
Seth G. Jones, Empty Bins in a Wartime Environment (Washington, DC: CSIS, January   
23, 2023), https://www.csis.org/analysis/empty-bins-wartime-environment-challenge-  
us-defense-industrial-base; and Cynthia R. Cook, et al., Transatlantic Defense during   
Wartime (Washington, DC: CSIS, September 2023), https://www.csis.org/analysis/  
transatlantic-defense-during-wartime.  
2   
Numerous think tank assessments have shed light on the challenge, including: Becca   
Wasser and Philip Sheers, From Production Lines to Front Lines: Revitalizing the U.S.   
Defense Industrial Base for Future Great Power Conflict (Washington, DC: Center for a   
New American Security, April 3, 2025), https://www.cnas.org/publications/reports/  
from-production-lines-to-front-lines; William C. Greenwalt, The Decline of the United   
States Defense Industrial Base and the Need to Restore Industrial Deterrence (Washington,   
DC: American Enterprise Institute, December 5, 2024), https://aei.org/wp-content/  
uploads/2024/12/The-Decline-of-the-United-States-Defense-Industrial-Base-and-the-  
Need-to-Restore-Industrial-Deterrence.pdf?x85095; and Robert Greenway, A Strategy   
to Revitalize the Defense Industrial Base for the 21st Century (Washington, DC: Heritage   
Foundation, 2019), https://www.heritage.org/defense/report/strategy-revitalize-the-  
defense-industrial-base-the-21st-century.  
3   
John Tirpak, “LaPlante on Why Weapon Production Constitutes Deterrence,” Air &   
Space Forces Magazine, October 27, 2022, https://www.airandspaceforces.com/laplante-  
on-why-weapon-production-constitutes-deterrence/.  
4   
Paul Iddon, “Expansive Military Operations Are Depleting Israel’s Munition Stocks,”   
Forbes, January 8, 2025, https://www.forbes.com/sites/pauliddon/2025/01/08/  
expansive-military-operations-are-depleting-israels-munition-stocks/; and Shelby   
Holliday, Anat Peled and Drew Fitzgerald, “Israel’s 12-Day War Revealed Alarming Gap   
in America’s Missile Stockpile,” Wall Street Journal, July 24, 2025, https://www.wsj.com/  
world/israel-iran-us-missile-stockpile-08a65396.  
5   
Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, The First Battle of the Next   
War: Wargaming a Chinese Invasion of Taiwan (Washington, DC: CSIS, January 2023),   
https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.  
6   
Mark F. Cancian, “Rebuilding U.S. Inventories: Six Critical Systems,” CSIS, Commentary,   
January 9, 2023, https://www.csis.org/analysis/rebuilding-us-inventories-six-critical-  
systems.  
7   
Laura Alviz, “Europe Is Short of Gunpowder and TNT When It Needs Them Most,”   
Japan Times, March 22, 2025, https://www.japantimes.co.jp/business/2025/03/22/  
eu-ukraine-low-munitions-stockpile/.  
8   
Julian Cooper, “Military Production in Russia Before and After the Start of the War With   
Ukraine: To What Extent has it Increased and how has This Been Achieved?,” The RUSI   
Journal 169, no. 4 (2024), 10–29, https://doi.org/10.1080/03071847.2024.2392990.

**Page 210**

204  
A Report of the CSIS Defense and Security Department  
9   
Cynthia R. Cook, Reviving the Arsenal of Democracy: Steps for Surging Defense Industrial   
Capacity (Washington, DC: CSIS, March 2023), https://www.csis.org/analysis/reviving-  
arsenal-democracy-steps-surging-defense-industrial-capacity.  
10   
Government Accountability Office, Defense Industrial Base: Actions Needed to Address   
Risks Posed by Dependence on Foreign Suppliers, GAO-25-107283 (Washington, DC:   
Government Accountability Office, July 2025), https://www.gao.gov/products/gao-25-  
107283.   
11   
Cortney Weinbaum et al., Assessing Systemic Strengths and Vulnerabilities of China’s   
Defense Industrial Base (Santa Monica, CA: RAND Corporation, February 2022), https://  
www.rand.org/pubs/research\_briefs/RBA930-1.html.  
12   
Seth G. Jones and Alexander Palmer, Rebuilding the Arsenal of Democracy: The U.S. and   
Chinese Defense Industrial Bases in an Era of Great Power Competition (Washington,   
DC: CSIS, March 2024), https://www.csis.org/analysis/china-outpacing-us-defense-  
industrial-base.   
13   
Ted Harshberger et al., A Proactive, Network-Based Approach to Defense Supply Chain   
Capacity (Santa Monica, CA: RAND Corporation, January 2025), https://www.rand.org/  
pubs/perspectives/PEA2899-1.html.  
14   
John T. Correll, “Lifeline in Danger,” Air & Space Forces Magazine, November 1988,   
https://www.airandspaceforces.com/PDF/MagazineArchive/Documents/1988/  
November%201988/1188danger.pdf.  
15   
U.S. Department of Defense, Quadrennial Defense Review Report (Washington, DC:   
U.S. Department of Defense, February 2010), https://history.defense.gov/Portals/70/  
Documents/quadrennial/QDR2010.pdf.  
16   
“Presidential Executive Order on Assessing and Strengthening the Manufacturing   
and Defense Industrial Base and Supply Chain Resiliency of the United States,” White   
House Archives, 2017, https://trumpwhitehouse.archives.gov/presidential-actions/  
presidential-executive-order-assessing-strengthening-manufacturing-defense-  
industrial-base-supply-chain-resiliency-united-states/; and Office of the Under   
Secretary of Defense for Acquisition and Sustainment, Assessing and Strengthening the   
Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United   
States (Washington, DC: U.S. Department of Defense, September 2018), https://media.  
defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-  
THE-MANUFACTURING-AND-DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-  
RESILIENCY.PDF.  
17   
Office of the Under Secretary of Defense for Acquisition and Sustainment, Securing   
Defense-Critical Supply Chains (Washington, DC: U.S. Department of Defense, February   
2022), https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-  
REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.  
18   
Department of Defense, National Defense Industrial Strategy (Washington, DC: U.S.   
Department of Defense, updated March 2025), https://www.businessdefense.gov/docs/  
ndis/2023-NDIS.pdf. The strategy was originally released November 16, 2023, and then   
updated to comply with March 2025 executive orders.  
19   
Hannah Aries, Bastian Giegerich, and Tim Lawrenson, “The Guns of Europe: Defence-  
Industrial Challenges in a Time of War,” Survival 65, no. 3 (June–July 2023), https://  
www.iiss.org/online-analysis/survival-online/2023/06/the-guns-of-europe-defence-  
industrial-challenges-in-a-time-of-war/.  
20   
Clara Falkenek, “Who’s at 2 percent? Look how NATO allies have increased their   
defense spending since Russia’s invasion of Ukraine,” Atlantic Council, July 8, 2020,   
https://www.atlanticcouncil.org/blogs/econographics/whos-at-2-percent-look-how-  
nato-allies-have-increased-their-defense-spending-since-russias-invasion-of-ukraine/.  
21   
Sebastian Clapp, “European Defence Industrial Strategy,” European Parliamentary   
Research Service, September 2024, https://www.europarl.europa.eu/RegData/etudes/  
BRIE/2024/762402/EPRS\_BRI(2024)762402\_EN.pdf.

**Page 211**

205  
War and the Modern Battlefield  
22   
Cynthia R. Cook et al., Enhancing Defense Industrial Cooperation between Australia and   
the United States (Washington, DC: CSIS, March 2025), https://www.csis.org/analysis/  
enhancing-defense-industrial-cooperation-between-australia-and-united-states;   
and Cynthia R. Cook and Kester Abbott, “Partnering for forward deterrence in the   
Indo-Pacific: Overcoming barriers to US-Australia cooperation on Australia’s GWEO   
Enterprise,” University of Sydney United States Study Center, July 2025, https://www.  
ussc.edu.au/partnering-for-forward-deterrence-in-the-indo-pacific-overcoming-  
barriers-to-us-australia-cooperation-on-australia-s-gweo-enterprise.  
23   
Australian Department of Defence, Defence Industry Development Strategy (Canberra:   
Asutralian Department of Defence, February 2024), https://www.defence.gov.au/  
about/strategic-planning/defence-industry-development-strategy.  
24   
Gregg Rubinstein, “Japan’s New Defense Buildup Plan and Its Defense Industrial   
Base,” CSIS, Commentary, January 26, 2023, https://www.csis.org/analysis/japans-new-  
defense-buildup-plan-and-its-defense-industrial-base.  
25   
Gordon Arthur, “How South Korea’s Defense Industry Transformed Itself into a Global   
Player,” Breaking Defense, November 6, 2023, https://breakingdefense.com/2023/11/  
how-south-koreas-defense-industry-transformed-itself-into-a-global-player/.  
26   
“Poland signs $6.5 billion deal to purchase a second batch of K2 tanks,” Korea JoongAng   
Daily, August 2, 2025, https://koreajoongangdaily.joins.com/news/2025-08-02/  
national/defense/Poland-signs-65-billion-deal-to-purchase-second-batch-of-K2-  
tanks/2367180.  
27   
Matthew P. Funaiole, Brian Hart, and Aidan Powers-Riggs, Ship Wars: Confronting   
China’s Dual-Use Shipbuilding Empire (Washington, DC: CSIS, March 2025), https://  
www.csis.org/analysis/ship-wars-confronting-chinas-dual-use-shipbuilding-empire.  
28   
Seth G. Jones, “China Is Ready for War,” Foreign Affairs, October 2, 2024, https://www.  
foreignaffairs.com/china/china-ready-war-america-is-not-seth-jones.  
29   
Theodore Bunzel and Elina Ribakova, “The Russian Economy Remains Putin’s Greatest   
Weakness,” Foreign Affairs, December 9, 2024, https://www.foreignaffairs.com/  
russia/russian-economy-remains-putins-greatest-weakness#author-info; and Richard   
Connolly, “Russia’s Wartime Economy Isn’t as Weak as It Looks,” Royal United Services   
Institute, January 22, 2025, https://www.rusi.org/explore-our-research/publications/  
commentary/russias-wartime-economy-isnt-weak-it-looks.  
30   
Cynthia R. Cook, “Friends over Factories,” Foreign Affairs, March 27, 2023, https://  
www.foreignaffairs.com/united-states/friends-over-factories; and “Defense Industrial   
Base Lessons from Russia-Ukraine,” CSIS, Conflict in Focus, March 13, 2025, https://  
www.csis.org/analysis/defense-industrial-base-lessons-russia-ukraine-conflict-focus.  
31   
Maksym Samoiliuk, “Ukraine War Economy Tracker,” Centre for Economic Strategy,   
https://ces.org.ua/en/tracker-economy-during-the-war/.  
32   
“Fact Sheet on U.S. Security Assistance to Ukraine,” U.S. Department of Defense,   
January 8, 2025, https://media.defense.gov/2025/Jan/09/2003626080/-1/-1/1/UKRAINE-  
FACT-SHEET-JAN-9-2025.PDF; U.S. Department of State, “U.S. Security Cooperation   
with Ukraine: Fact Sheet,” press release, March 12, 2025, https://www.state.gov/  
bureau-of-political-military-affairs/releases/2025/01/u-s-security-cooperation-with-  
ukraine; and Marc Santora and Eric Schmitt, “As F-16s Arrive, Ukraine Still Faces   
Steep Challenges in the Skies,” New York Times, July 28, 224, https://www.nytimes.  
com/2024/07/28/world/europe/ukraine-russia-f-16s.html.   
33   
Lolita Baldor, “China, North Korea and Russia Military Cooperation Raises Threats in   
the Pacific, US Official Warns,” AP News, April 10, 2025, https://apnews.com/article/  
pacific-russia-china-north-korea-weapons-ukraine-8ad7156898f1391557d5e53d5d09a  
02c.  
34   
Omar Al-Ghusbi and Conrad Rousseau, “Airborne Axis: Inside the Deal That Brought   
Iranian Drone Production to Russia,” C4ADS, May 29, 2025, https://c4ads.org/reports/  
airborne-axis/.

**Page 212**

206  
A Report of the CSIS Defense and Security Department  
35   
C. Todd Lopez, “Iran Gives Russia Short-Range Missiles, While U.S., Partners Expect   
to Keep Bolstering Ukrainian Air Defense,” U.S. Department of Defense, September 10,   
2024, https://www.defense.gov/News/News-Stories/Article/Article/3901774/iran-gives-  
russia-short-range-missiles-while-us-partners-expect-to-keep-bolster/.   
36   
“Unlawful Military Cooperation including Arms Transfers between North Korea and   
Russia,” Multilateral Sanctions Monitoring Team, May 29, 2025, https://msmt.info/  
Publications/detail/MSMT%20Report/4195.   
37   
Max Bergmann et al., Collaboration for a Price: Russian Military-Technical Cooperation   
with China, Iran, and North Korea (Washington, DC: CSIS, May 2024), https://www.csis.  
org/analysis/collaboration-price-russian-military-technical-cooperation-china-iran-and-  
north-korea.  
38   
Ibid.  
39   
Isabelle Khurshudyan, Mary Ilyushina, and Kostiantyn Khudov, “Russia and Ukraine   
are fighting the first full-scale drone war,” Washington Post, December 2, 2022, https://  
www.washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/.   
40 Lauren Kahn, “How Ukraine Is Remaking War,” Foreign Affairs, August 29, 2022, https://  
www.foreignaffairs.com/ukraine/how-ukraine-remaking-war.  
41   
Kateryna Bondar, “How Ukraine Rebuilt Its Military Acquisition System Around   
Commercial Technology,” CSIS, January 13, 2025, https://www.csis.org/analysis/how-  
ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology.  
42   
Vitaliy Goncharuk, “Ukraine Isn’t the Model for Winning the Innovation War,” War   
on the Rocks, August 12, 2025, https://warontherocks.com/2025/08/ukraine-isnt-the-  
model-for-winning-the-innovation-war/.  
43   
Jorge Rivero, “Innovating under Fire: Lessons from Ukraine’s Frontline Drone   
Workshops,” Modern War Institute, March 25, 2025, https://mwi.westpoint.edu/  
innovating-under-fire-lessons-from-ukraines-frontline-drone-workshops/; and Jack   
Watling and Nick Reynolds, Tactical Developments During the Third Year of the Russo–  
Ukrainian War (London, UK: Royal United Services Institute, February 2025), tactical-  
developments-third-year-russo-ukrainian-war-february-2205.pdf  
44   
William Shelton, Cynthia R. Cook, and Charlie Barton, A Clean Sheet Approach to Space   
Acquisition in Light of the New Space Force (Santa Monica, CA: RAND Corporation,   
August 2021), https://www.rand.org/pubs/research\_reports/RRA541-1.html.  
45   
Ibid.  
46   
Ibid.  
47   
Philip E. Ross, “Budget Drones in Ukraine Are Redefining Warfare,” IEEE Spectrum,   
May 17, 2023, https://spectrum.ieee.org/drone-warfare-ukraine.  
48   
Tayfun Ozberk, “Analysis: Chain of Negligence Caused the Loss of the Moskva Cruiser,”   
Naval News, April 17, 2022, https://www.navalnews.com/naval-news/2022/04/analysis-  
chain-of-negligence-caused-the-loss-of-the-moskva-cruiser/.  
49   
Cancian, Cancian, and Heginbotham, The First Battle of the Next War.  
50   
Shelton, Cook, and Barton, A Clean Sheet Approach to Space Acquisition.  
51   
Gregory Sanders and Audrey Aldisert, “Burden Sharing via Modular Open Systems   
Approaches: A Collaborative Path to Affordable Mass,” CSIS, Commentary, December   
10, 2024, https://www.csis.org/analysis/burden-sharing-modular-open-systems-  
approaches-collaborative-path-affordable-mass.  
POWER PROJECTION AND THE LOGISTICS OF MODERN WAR  
1   
Ronald Ti and Christopher Kinsey, “Lessons from the Russo-Ukrainian conflict: the   
primacy of logistics over strategy,” Defence Studies 23, no. 3 (2023), https://doi.org/10.10  
80/14702436.2023.2238613.

**Page 213**

207  
War and the Modern Battlefield  
2   
Department of Defense, Joint Concept for Logistics (Washington, DC: Department of   
Defense, August 2010), 8, https://www.jcs.mil/portals/36/Documents/102710173839\_  
Joint\_Concept\_for\_Logistics\_v1\_FINAL\_with\_CJCS\_Sig.pdf.  
3   
Ibid.   
4   
Ibid.   
5   
There are a number of useful review articles focused on the Russian experience. See   
Paul Schwartz et al., Russian Military Logistics in the Ukraine War: Recent Reforms   
and Wartime Operations (Arlington, VA: CNA, September 2023), https://www.cna.org/  
reports/2023/10/Russian-Military-Logistics-in-the-Ukraine-War.pdf; and Marta Kepe,   
Logistics and Sustainment in the Russian Armed Forces (Santa Monica, CA: RAND,   
November 2023), https://www.rand.org/pubs/research\_reports/RRA2523-1.html.   
6   
Bonnie Berkowitz and Artur Galocha, “Why the Russian military is bogged down by   
logistics in Ukraine,” Washington Post, March 30, 2022, https://www.washingtonpost.  
com/world/2022/03/30/russia-military-logistics-supply-chain/.  
7   
Ibid.  
8   
Marta Kepe, Logistics and Sustainment in the Russian Armed Forces (Santa Monica, CA:   
RAND Corporation, November 15, 2023), https://www.rand.org/pubs/research\_reports/  
RRA2523-1.html.  
9   
Angelica Evans et al., “Russian Offensive Campaign Assessment,” Institute for the Study   
of War, June 24, 2025, https://www.understandingwar.org/backgrounder/russian-  
offensive-campaign-assessment-june-24-2025.  
10   
Simone McCarthy, “NATO allies call China a ‘decisive enabler’ of Russia in Ukraine   
war as bloc eyes Asia security threats,” CNN, July 11, 2024, https://www.cnn.  
com/2024/07/11/china/nato-china-russia-ukraine-intl-hnk/index.html.  
11   
Kateryna Stepanenko et al., “Russian Force Generation and Technological Adaptations   
Update,” Institute for the Study of War, July 25, 2025, https://understandingwar.  
org/backgrounder/russian-force-generation-and-technological-adaptations-update-  
july-25-2025.  
12   
Anna Harvey et al., Russian Offensive Campaign Assessment,” Institute for the Study   
of War, August 19, 2025, https://www.understandingwar.org/backgrounder/russian-  
offensive-campaign-assessment-august-19-2025.  
13   
Rachel S. Cohen, “What the Wars in Gaza and Ukraine Are Teaching the US   
About Logistics,” Air & Space Forces Magazine, September 21, 2024, https://www.  
airandspaceforces.com/wars-gaza-ukraine-us-lessons-logistics/.  
14   
Peeter Helme, “Ukraine’s drones make Russia’s rear go up in flames,” Euromaidan   
Press, August 19, 2025, https://euromaidanpress.com/2025/08/19/ukraine-hits-russian-  
supply-depots-deep-in-occupied-luhansk/.  
15   
Elizabeth Hoffman et al., “How Supporting Ukraine Is Revitalizing the U.S. Defense   
Industrial Base,” CSIS, Commentary, April 18, 2024, https://www.csis.org/analysis/how-  
supporting-ukraine-revitalizing-us-defense-industrial-base.  
16   
Department of Defense Office of the Inspector General, Audit of DoD Maintenance   
of Military Equipment Provided in Support of Ukraine, Report No. DODIG-2025-002   
(Washington, DC: Department of Defense, October 2024), https://www.dodig.mil/  
reports.html/Article/3932056/audit-of-dod-maintenance-of-military-equipment-  
provided-in-support-of-ukraine-r/.  
17   
Manuela Tudosia, “Lessons Learned from Ukraine: Logistics,” European Security &   
Defence, June 23, 2023, https://euro-sd.com/2023/06/articles/31845/lessons-learned-  
from-ukraine-logistics/.  
18   
Charles Hamilton, “The Logistics of Victory: Ukraine’s Sustainment Challenge,”   
RealClearDefense, March 17, 2025, https://www.realcleardefense.com/  
articles/2025/03/17/the\_logistics\_of\_victory\_ukraines\_sustainment\_challenge\_1097974.  
html.

**Page 214**

208  
A Report of the CSIS Defense and Security Department  
19   
Ibid.  
20   
Aaron Epstein et al., “Putting Medical Boots on the Ground: Lessons from the War in   
Ukraine and Applications for Future Conflict with Near-Peer Adversaries,” Journal of   
the American College of Surgeons 237, no. 2 (April 2023), https://pmc.ncbi.nlm.nih.gov/  
articles/PMC10344429/.   
21   
Siobhán O’Grady and Serhii Korolchuk, “Borscht from the sky: Ukraine uses drones   
to resupply trench-bound troops,” Washington Post, September 1, 2025, https://www.  
washingtonpost.com/world/2025/09/01/ukraine-drones-resupply-trench/.  
22   
Larry Hanauer and Michael P. Connell, Political Priorities, Poor Intelligence Tradecraft,   
and the Suppression of Dissenting Views: Why Israel Failed to Warn of Hamas’s October 7   
Attack (Alexandria VA: Institute for Defense Analyses, September 2024), https://www.  
ida.org/-/media/8e5040cc7ee5457dba26c8127b47c8e0.ashx.  
23   
Adam Samson and Neri Zilber, “Turkey moves to restrict key exports to Israel,”   
Financial Times, April 9, 2024, https://www.ft.com/content/73edc1c9-a6a9-4337-b719-  
78506e9d1456.  
24   
Cohen, “What the Wars in Gaza and Ukraine Are Teaching the US.”   
25   
Ibid.  
26   
Mark F. Cancian, “Can the United States Equip Israel While Simultaneously Equipping   
Ukraine and Taiwan?,” CSIS, Critical Questions, October 12, 2023, https://www.csis.org/  
analysis/can-united-states-equip-israel-while-simultaneously-equipping-ukraine-and-  
taiwan.  
27   
David Averre, “Israel’s Iron Dome system is running out of ammunition and a joint   
Hezbollah/Iran missile strike could overwhelm defences - as US warns it can’t keep   
supplying IDF AND Ukraine,” Daily Mail, October 15, 2024, https://www.dailymail.  
co.uk/news/article-13961393/israel-iron-dome-hezbollah-iran-missile-strike-tehran-air-  
defence.html.  
28   
Ibid.; and Harrison Morgan, “A Year Since October 7: Three Key Lessons from the War   
in Gaza,” Modern War Institute, October 7, 2024, https://mwi.westpoint.edu/a-year-  
since-october-7-three-key-lessons-from-the-war-in-gaza.  
29   
Larry Jackson, Geraldo Ferrer, and Harrison Schramm, “The Dawn of Offensive   
Supply Chains,” RealClearDefense, October 14, 2024, https://www.realcleardefense.  
com/articles/2024/10/14/the\_dawn\_of\_offensive\_supply\_chains\_1064896.html; and Ari   
Hawkins and Joseph Gedeon, “Middle East pager attacks ignite fear of supply chain   
warfare,” Politico, September 19, 2024, https://www.politico.com/news/2024/09/19/  
pager-attacks-supply-chain-warfare-00180136.   
30   
“Why is Xi Jinping building secret commodity stockpiles?,” The Economist, July 23,   
2024, https://www.economist.com/finance-and-economics/2024/07/23/why-is-xi-  
jinping-building-secret-commodity-stockpiles.  
31   
 Matthew P. Funaiole, Brian Hart, Jaehyun Han, and Jennifer Jun, “China Accelerates   
Construction of ‘Ro-Ro’ Vessels, with Potential Military Implications,” CSIS, China   
Power, October 11, 2023, https://chinapower.csis.org/analysis/china-construct-ro-ro-  
vessels-military-implications/.  
32   
Matthew P. Funaiole, Brian Hart, and Aidan Powers-Riggs, “China Dominates the   
Shipbuilding Industry,” CSIS, CSIS Charts, March 25, 2025, https://www.csis.org/  
analysis/china-dominates-shipbuilding-industry; and Chad Peltier, Tate Nurkin, and   
Sean O’Connor, China’s Logistics Capabilities for Expeditionary Operations (Washington,   
DC: U.S.-China Economic and Security Review Commission, March 2020), https://www.  
uscc.gov/research/chinas-logistics-capabilities-expeditionary-operations.  
33   
“2024 Regional Sustainment Framework,” U.S. Department of Defense, https://www.  
acq.osd.mil/asds/docs/RSF-9MAY24.pdf; “Fact Sheet: Partnership for Indo-Pacific   
Industrial Resilience,” U.S. Department of Defense, June 1, 2025, https://media.defense.  
gov/2025/Jun/02/2003730341/-1/-1/1/FACT-SHEET-PARTNERSHIP-FOR-INDO-PACIFIC-  
INDUSTRIAL-RESILIENCE.PDF; and U.S. Department of Defense, “Under Secretary of

**Page 215**

209  
War and the Modern Battlefield  
Defense for Acquisition and Sustainment Travel to Japan,” Press release, June 5, 2024,   
https://www.defense.gov/News/Releases/Release/Article/3797650/under-secretary-of-  
defense-for-acquisition-and-sustainment-travel-to-japan/.  
34   
Alexandra G. Neenan and Luke A. Nicastro, The Defense Production Act of 1950: History,   
Authorities, and Considerations for Congress, CRS Report No. R43767 (Washington,   
DC: Congressional Research Service, October 2023), https://www.congress.gov/crs-  
product/R43767.   
THE NEXT OFFSET: WINNING THE FIGHT BEFORE IT STARTS  
1   
Carl von Clausewitz, On War (New York: Penguin, 1968), 101.  
2   
Michael C. Horowitz, “Battles of Precise Mass: Technology is Remaking War—and   
America Must Adapt,” Foreign Affairs, October 22, 2024, https://www.foreignaffairs.  
com/world/battles-precise-mass-technology-war-horowitz.  
3   
On offset strategies, see, for example, Robert Martinage, Toward a New Offset Strategy:   
Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability   
(Washington, DC: Center for Strategic and Budgetary Assessment, 2014), https://  
csbaonline.org/uploads/documents/Offset-Strategy-Web.pdf.  
4   
Quoted in Dima Adamsky, The Culture of Military Innovation: The Impact of Cultural   
Factors on the Revolution in Military Affairs in Russia, the US, and Israel (Stanford, CA:   
Stanford University Press, 2010), 2.  
5   
James S. Lay, A Report to the National Security Council (Washington, DC: National   
Security Council, NSC 162/2, October 1953), 2, https://irp.fas.org/offdocs/nsc-hst/nsc-  
162-2.pdf.  
6   
Ibid., 5.  
7   
John Foster Dulles, “Policy for Security and Peace,” Foreign Affairs, April 1, 1954, https://  
www.foreignaffairs.com/articles/united-states/1954-04-01/policy-security-and-peace.  
8   
Quoted in Richard M. Leighton, Strategy, Money, and the New Look, 1953-1956, History   
of the Office of the Secretary of Defense, Vol. III (Washington, DC: Historical Office,   
Office of the Secretary of Defense, 2001), 373, https://history.defense.gov/Portals/70/  
Documents/secretaryofdefense/OSDSeries\_Vol3.pdf.  
9   
See, for example, ibid., 432–434.  
10   
Robert J. Watson, Into the Missile Age, 1956-1960, History of the Office of the Secretary of   
Defense, Vol. IV (Washington, DC: Historical Office, Office of the Secretary of Defense,   
1997), 35, https://history.defense.gov/Portals/70/Documents/secretaryofdefense/  
OSDSeries\_Vol4.pdf.  
11   
See, for example, Donn M. Starry, “Extending the Battlefield,” in Jack D. Kem, Deep   
Operations: Theoretical Approaches to Fighting Deep (Fort Leavenworth, KS: Army   
University Press, 2021), 107-128, https://www.armyupress.army.mil/Portals/7/combat-  
studies-institute/images/LSCO%20DeepOps%20book%20interactive%20with%20  
cover%20spread%2012Nov21.pdf; and Douglas W. Skinner, Airland Battle Doctrine   
(Alexandria, VA: Center for Naval Analyses, September 1988), https://apps.dtic.mil/sti/  
tr/pdf/ADA202888.pdf.  
12   
Department of the Army, Field Manual 100-5 Operations (Washington, DC:   
Headquarters, Department of the Army, 1986), https://cgsc.contentdm.oclc.org/digital/  
collection/p4013coll9/id/893/.  
13   
Richard H. Van Atta, Seymour J. Deitchman, and Sidney G. Reed, DARPA Technical   
Accomplishments, Vol. III (Arlington, VA: Defense Advanced Research Projects Agency,   
July 1991), https://apps.dtic.mil/sti/tr/pdf/ADA241680.pdf; and Benjamin M. Jensen,   
Forging the Sword: Doctrinal Change in the U.S. Army (Stanford, CA: Stanford University   
Press, 2016).  
14   
For an overview of the second offset, see Edward C. Keefer, Harold Brown: Offsetting   
the Soviet Military Challenge, 1977–1981 (Washington, DC: Historical Office, Office of

**Page 216**

210  
A Report of the CSIS Defense and Security Department  
the Secretary of Defense, 2017), 575–600, https://history.defense.gov/Portals/70/  
Documents/secretaryofdefense/OSDSeries\_Vol9.pdf.  
15   
Quoted in ibid., 588.  
16   
William Perry, My Journey at the Nuclear Brink (Stanford, CA: Stanford University Press,   
2015), 38–39.  
17   
Edward C. Keefer, Caspar Weinberger and the U.S. Military Build-up 1981–1985   
(Washington, DC: Historical Office, Office of the Secretary of Defense, 2023), 623–624,   
https://history.defense.gov/Portals/70/Documents/secretaryofdefense/OSDSeries\_  
Vol10.pdf?ver=NHuRp2OYKrNpaUsCQBMq0A%3D%3D.  
18   
Quoted in Gordon S. Barrass, The Great Cold War: A Journey Through the Hall of Mirrors   
(Stanford, CA: Stanford University Press, 2009), 274.  
19   
Robert Work, “Remarks by Deputy Secretary Work on Third Offset Strategy,” (speech,   
Brussels, Belgium, April 28, 2016), https://www.defense.gov/News/Speeches/Speech/  
Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/.  
20   
Data from “SIPRI Military Expenditure Database,” Stockholm International Peace   
Research Institute, https://www.sipri.org/databases/milex.  
21   
“强化政治自觉, 下决心根治‘和平病’” [Strengthen Political Awareness and Resolve to   
Eradicate ‘Peace Disease’], 中国军网 [China Military Network], July 2, 2018; 倪文鑫 [Ni   
Wenxin], “实战化训练必须聚焦明天的 战场—军区空军实战化训练对联合训练的启示”   
[Training Made Realistic to Actual War Must Focus on Tomorrow’s Battlefield: What   
Military Region Air Force’s Training Made Realistic to Actual War Can Tell Us About   
Joint Training], 人民前线 [People’s Front], October 25, 2013; 陈永义 [Chen Yongyi] and   
刘媛媛 [Liu Yuanyuan], “和平病’亦须心药医” [Peace Disease Also Requires Careful   
Medicine], 解放军报 [People’s Liberation Army Daily], July 16, 2019.  
22   
The U.S. Department of Defense has developed some multidomain efforts and related   
concepts, such as Assault Breaker II, which is designed to provide rapid, multidomain   
offensive capabilities to destroy advancing enemy forces before they can consolidate   
their gains; the Joint Warfighting Concept 3.0, the U.S. military’s doctrine for joint   
warfighting, with a focus on information advantage, command and control, joint   
fires, contested logistics, expanded maneuver, and a proactive stance in a competitive   
environment; Hellscape, U.S. Indo-Pacific Command’s integration of unmanned ships,   
aircraft, and submarines working in tandem to engage thousands of targets across the   
Pacific; and the China operational plan (OPLAN). In addition, former U.S. Secretary of   
the Air Force Frank Kendall had several operational imperatives: resilient and effective   
space architectures; Advanced Battle Management System (ABMS) / Air Force Joint All-  
Domain Command and Control; next generation air dominance (NGAD); moving target   
engagement at scale; optimized resilience basing, sustainment, and communication   
in a contested environment; B-21 long rang strike family of systems; and readiness to   
transition to a wartime posture.  
23   
Chieh Chung, “PLA Logistics and Mobilization Capacity in a Taiwan Invasion,” in Joel   
Wuthnow et al., eds., Crossing the Strait: China’s Military Prepares for War with Taiwan   
(Washington, DC: National Defense University Press, 2022), 261, https://ndupress.  
ndu.edu/Portals/68/Documents/Books/crossing-the-strait/crossing-the-strait.pdf;   
Chung Chieh and Andrew N.D. Yang, “Crossing the Strait: Recent Trends in PLA   
‘Strategic Delivery’ Capabilities,” in Joel Wuthnow et al., eds. The PLA Beyond Borders:   
Chinese Military Operations in Regional and Global Context (Washington, DC: National   
Defense University Press, 2021), 54, https://digitalcommons.ndu.edu/books-and-book-  
chapters/1/.  
24   
See, for example, Ivan Kanapathy, “Countering China’s Use of Force,” in Matt Pottinger,   
ed., The Boiling Moat: Urgent Steps to Defend Taiwan (Stanford, CA: Hoover Institution   
Press, 2024), 93.  
25   
Joshua Arostegui, “PLA Army and Marine Corps Amphibious Brigades in a Post-Reform   
Military,” in Wuthnow, et al., eds., Crossing the Strait, 173.  
26   
Phillip C. Saunders and Joel Wuthnow, “Crossing the Strait: PLA Modernization and

**Page 217**

211  
War and the Modern Battlefield  
Taiwan,” in Wuthnow, Crossing the Strait, 8.  
27   
Chung, “PLA Logistics and Mobilization Capacity in a Taiwan Invasion,” 270.  
28   
David A. Ochmanek, Determining the Military Capabilities Most Needed to Counter China   
and Russia: A Strategy-Driven Approach (Santa Monica, CA: RAND, June 2022), https://  
www.rand.org/content/dam/rand/pubs/perspectives/PEA1900/PEA1984-1/RAND\_  
PEA1984-1.pdf.  
29   
Ochmanek, Determining the Military Capabilities Most Needed to Counter China and   
Russia.  
30   
Josh Rogin, “The U.S. Military Plans a ‘Hellscape’ to Deter China from Attacking   
Taiwan,” Washington Post, June 10, 2024, https://www.washingtonpost.com/  
opinions/2024/06/10/taiwan-china-hellscape-military-plan/.  
31   
Admiral Samuel Paparo, “Posture of United States Indo-Pacific Command,” Testimony   
before the Committee on Armed Services, U.S. Senate, April 10, 2025, https://www.  
armed-services.senate.gov/imo/media/doc/4102025fulltranscript.pdf.  
32   
Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, The First Battle of the Next   
War: Wargaming a Chinese Invasion of Taiwan (Washington, DC: CSIS, January 2023),   
https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.  
33   
Ibid.  
34   
Ronald O’Rourke, Navy Virginia-Class Submarine Program and AUKUS Submarine (Pillar   
1) Project: Background and Issues for Congress, CRS Report No. RL32418 (Washington,   
DC: Congressional Research Service, March 2025), https://www.congress.gov/crs-  
product/RL32418.   
35   
See, for example, John A. Tirpak, “Navy Shoots Four LRASMs in ‘Graduation Exercise,’   
as Air Force Ramps Up Multiyear Buy,” Air and Space Forces Magazine, April 3, 2024,   
https://www.airandspaceforces.com/navy-shoots-four-lrasm-air-force-multiyear-buy/.  
36   
John A. Tirpak, “Lockheed Get $122 Million for Gear to Accelerate JASSM and   
LRASM Production,” Air and Space Forces Magazine, March 17, 2025, https://www.  
airandspaceforces.com/lockheed-gear-jassm-and-lrasm-production/.  
37   
Mark A. Milley and Eric Schmidt, “America Isn’t Ready for the Wars of the Future,”   
Foreign Affairs, August 5, 2024, https://www.foreignaffairs.com/united-states/  
ai-america-ready-wars-future-ukraine-israel-mark-milley-eric-schmidt.  
38   
Elon Musk, @elonmusk, X post November 25, 2024, 7:32 AM, https://x.com/elonmusk/  
status/1861070432377737269?lang=en.  
39   
Sharon Weinberger and Heather Somerville, “Tech Bros Are Betting They Can Help   
Win a War with China,” Wall Street Journal, August 9, 2024, https://www.wsj.com/tech/  
anduril-drones-palmer-luckey-china-ukraine-china-951494ec.  
40 Michael C. Horowitz, The Diffusion of Military Power: Causes and Consequences for   
International Politics (Princeton, NJ: Princeton University Press, 2010), 2.  
41   
Stephen Peter Rosen, Winning the Next War: Innovation and the Modern Military (Ithaca,   
NY: Cornell University Press, 1991), 109–129.

**Page 218**

COVER PHOTO DMYTRO SHEREMETA/GETTY IMAGES  
1616 Rhode Island Avenue NW   
Washington, DC 20036   
202 887 0200 | www.csis.org  
New York • London • Oxford • New Delhi • Sydney  
1385 Broadway, Fifth Floor  
New York, NY 10018  
212 419 5300 | www.bloomsbury.com  
ISBN 979-8-7651-9851-3  
ËxH98765y198513z