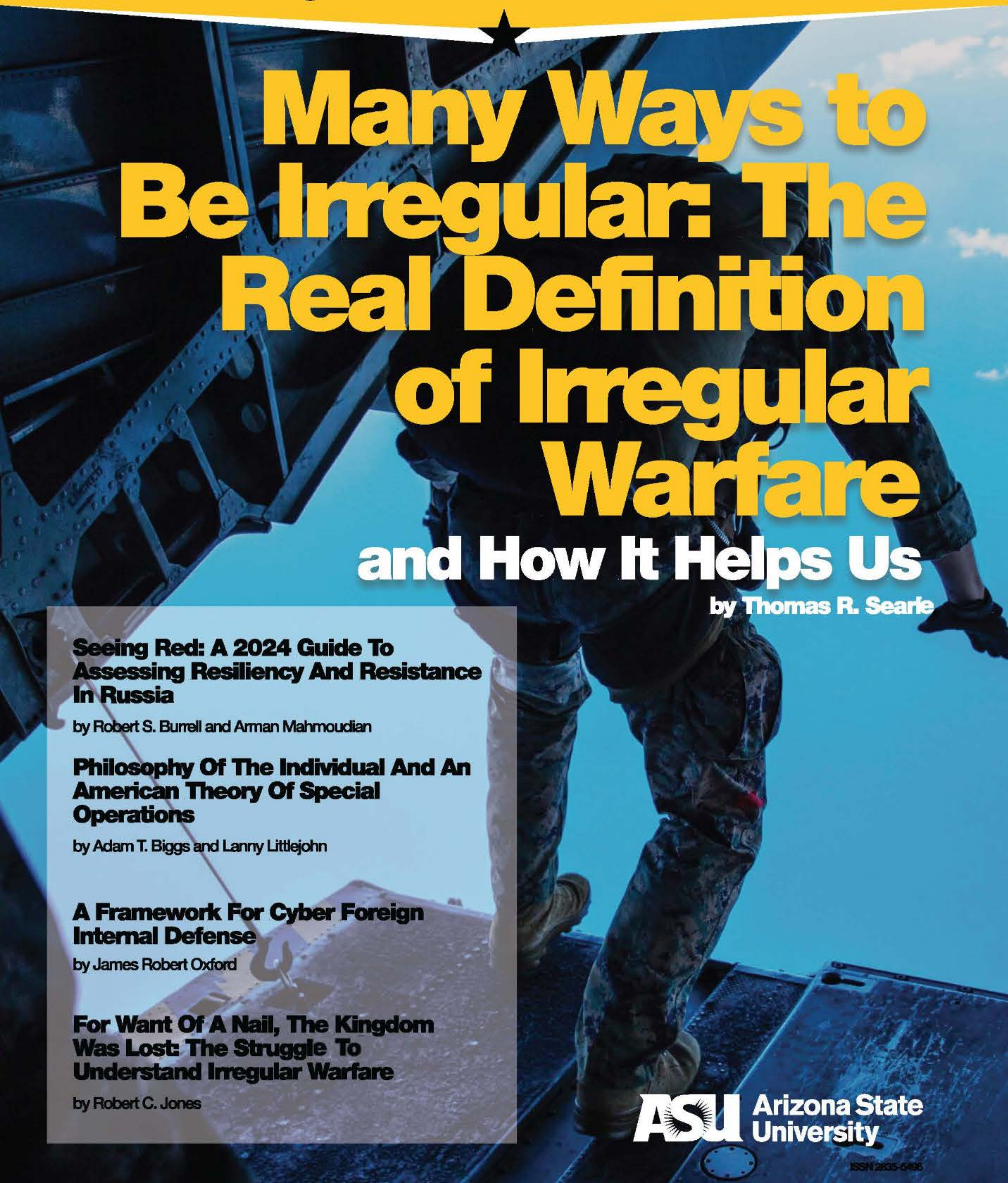


Inter Populum

Journal of Irregular Warfare and Special Operations



Many Ways to Be Irregular: The Real Definition of Irregular Warfare

and How It Helps Us

by Thomas R. Searle

Seeing Red: A 2024 Guide To Assessing Resiliency And Resistance In Russia

by Robert S. Burrell and Arman Mahmoudian

Philosophy Of The Individual And An American Theory Of Special Operations

by Adam T. Biggs and Lanny Littlejohn

A Framework For Cyber Foreign Internal Defense

by James Robert Oxford

For Want Of A Nail, The Kingdom Was Lost: The Struggle To Understand Irregular Warfare

by Robert C. Jones

INTER POPULUM: The Journal of Irregular Warfare and Special Operations

Inter Populum: The Journal of Irregular Warfare and Special Operations, published by Arizona State University, is an academically rigorous, peer-reviewed publication focused on furthering studies, thought, and discussion on special operations and irregular warfare topics. It is published once a year in print (ISSN: 2836-5496) and twice a year online (ISSN: 2836-6034).

To request a printed copy or inquire about publication consideration, contact our team at interpopulum@asu.edu.

EDITORIAL BOARD

Editors:

Christopher Marsh, U.S. National Defense University, christopher.marsh.civ@ndu.edu
James Kiras, U.S. Air Force School of Advanced Air and Space Studies, james.kiras@us.af.mil
Ryan Shaw, Arizona State University, Ryan.Shaw.I@asu.edu

Managing Editor:

Sarah Shoer, Arizona State University, Sarah.Shoer@asu.edu

Book Review Editor:

Mark Grzegorzewski, Embry Riddle Aeronautical University, grzegorm@erau.edu

Editorial Board:

Leo Blanken, Naval Postgraduate School
Patricia Blocksome, Joint Special Operations University
Paul Brister, Joint Special Operations University
Carolyn Davidson, U.S. National Defense University
David Ellis, New College of Florida
Ken Gleiman, Arizona State University
Stephen Grenier, Johns Hopkins University
Nikolas Gvosdev, U.S. Naval War College
Jaroslaw Jablonski, Jagiellonian University
Martijn Kitzen, Netherlands Defence Academy
Nina Kollars, Joint Special Operations University
Jeffrey Kubiak, Arizona State University
David Maxwell, Center for Asia Pacific Strategy
Mark Moyar, Hillsdale College
Aleksandra Nestic, U.S. Department of State
David Oakley, University of South Florida
Ulrica Pettersson, Swedish Defence University
Linda Robinson, RAND Corporation
Richard Schultz, Fletcher School, Tufts University
Kalev Sepp, Naval Postgraduate School
Emily Stranger, Indiana University-Bloomington

Copyright © 2025 Arizona Board of Regents/Arizona State University. All rights reserved. No part of this publication may be reproduced, stored, transmitted, or disseminated in any form, by any means, without prior written permission from Arizona State University

INTER POPULUM:
The Journal of Irregular Warfare and Special Operations

The views expressed in this publication are entirely those of the authors and do not reflect the views, policy, or position of Arizona State University, the United States Government, the U.S. Department of Defense, or any other U.S. government entity.

Table of Contents

Articles

Many Ways to Be Irregular: The Real Definition of Irregular Warfare and How It Helps Us by Thomas R. Searle	4
Seeing Red: A 2024 Guide to Assessing Resiliency and Resistance in Russia by Robert S. Burrell and Arman Mahmoudian	20
Philosophy of the Individual and an American Theory of Special Operations by Adam T. Biggs and Lanny Littlejohn.....	49
A Framework for Cyber Foreign Internal Defense by James Robert Oxford.....	66
For Want of a Nail, the Kingdom Was Lost: The Struggle to Understand Irregular Warfare by Robert C. Jones.....	86

Book Reviews

<i>Info Ops: From World War I to the Twitter Era</i> Edited by Ofer Fridman, Vitaly Kabernik, and Francesca Granelli Reviewed by James F. Slaughter	106
<i>No Shortcuts: Why States Struggle to Develop a Military Cyber-Force</i> by Max Smeets Reviewed by Mark Grzegorzewski	108
<i>Cognitive Electronic Warfare: An Artificial Intelligence Approach</i> by Karen Haigh and Julia Andrusenko Reviewed by Sean Pascoli	111
<i>Proxy War Ethics: The Norms of Partnering in Great Power Competition</i> by C. Anthony Pfaff Reviewed by LTC Joshua Lehman	114
<i>Risk: A User's Guide</i> by Stanley A. McChrystal and Anne Butrico Reviewed by Ibrahim Kocaman.....	117
<i>The Rise of China Inc.</i> by Shaomin Li Reviewed by Ian Murphy.....	120
<i>The Unit: My Life Fighting Terrorists as One of America's Most Secret Military Operatives</i> by Adam Gamal Reviewed by James Stejskal	123

COMMENTARY

Many Ways to Be Irregular: The Real Definition of Irregular Warfare and How It Helps Us

Thomas R. Searle, Joint Special Operations University, Tampa, Florida, USA

ABSTRACT

The U.S. military has long struggled to define and understand irregular warfare (IW). This essay argues that IW should be defined as “all warfare other than conventional warfare,” shifting the focus from finding a universal characteristic to analyzing the specific irregularities of each conflict. To support this approach, the essay provides a detailed definition of conventional warfare, which has remained stable for a century, and contrasts it with the diverse ways warfare can be irregular. By embracing the complexity and variety of IW rather than seeking a rigid definition, this framework allows for greater flexibility, adaptability, and creativity in both exploiting and countering irregular threats.

KEYWORDS

irregular warfare;
conventional warfare;
unconventional warfare; defining warfare

The Problem: Negative Terms

There is a forever war between U.S. military doctrine and the English language, particularly with negative definitions. Words with positive definitions tell us what something is, while words with negative definitions tell us what something is not. In English, we routinely create words with negative definitions by adding a negative prefix, such as *un-*, *non-*, or *ir-*, to a word with a positive definition. This is how words with positive definitions such as *cool*, *negotiable*, and *responsible* are transformed into *uncool*, *nonnegotiable*, and *irresponsible* which mean, respectively, *not cool*, *not negotiable*, and *not responsible*. Negative prefixes give the English language an enormous number of terms with negative definitions. As an aside, it is worth noting that a negative definition does not mean the term describes a bad thing. For example, the term *nontoxic* has a negative definition, but it is obviously better than the positive term *toxic*.

CONTACT Thomas R. Searle | thomas.searle@jsou.edu

The views expressed in this article are solely those of the author(s) and do not necessarily reflect the views, policy, or position of the U.S. Government, United States Special Operations Command, Joint Special Operations University, or Department of Defense.

© 2025 Arizona Board of Regents/Arizona State University

Negative definitions are not problematic for the English language but do pose a problem for U.S. military doctrine. This is because the military prides itself on its bias for action. Soldiers, Sailors, Airmen, Marines, and Guardians want to know what to do, and we look to military doctrine to tell us what to do and how to do it. By telling us what something is, a positive definition puts us one step closer to knowing what to do. A negative definition, on the other hand, does not tell us what to do. At best, a negative definition might tell us what not to do. For example, conformists know that they should always conform in every way. On the other hand, nonconformists must choose from a vast array of different ways not to conform. The nonconformists might insist on walking backward wherever they go, keeping their eyes shut and living as blind people every Tuesday or laughing uproariously every time anyone says the word “of”. As this example indicates, negative definitions are a blessing if you crave options, and a curse if you want everyone to agree on exactly what to do.

The U.S. military, and particularly the Special Operations community within the U.S. military, has a long and unsatisfactory relationship with two different negative terms: unconventional warfare (UW) and irregular warfare (IW). Historically, the U.S. military has taken a bad approach to both by imposing positive definitions on these negative terms. The appeal of a positive definition is obvious since it helps the U.S. military decide what to do. The reason this is a bad solution is that imposing a positive definition on a negative term immediately creates confusion and conflict between the U.S. military and every other speaker of the English language.

The current U.S. military definition of unconventional warfare is: “Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area.”¹ This definition has remained fairly stable for decades even though, from this positive definition, one would think the term should be: support to resistance and insurgency rather than unconventional warfare. This definition of UW has caused unending difficulties within the U.S. military and the interagency community since, in English, unconventional means “not conventional.” Support to resistance and insurgency is not conventional warfare, but there are many other types of warfare that are equally not conventional and most English speakers are reluctant to limit unconventional warfare to support to resistance and insurgency.

In English, unconventional warfare and irregular warfare are nearly synonymous, and the U.S. military has traditionally imposed positive definitions on both terms. However, while the definition of UW has been remarkably stable, the definition of IW has changed to follow the latest unconventional threat. Thus, during the Cold War, when communist insurgencies were the new and alarming unconventional threat, the definition focused on them; after 9/11, when the focus of concern shifted to jihadi-inspired terrorism and insurgency, the definition shifted to focus on this new irregular threat; and now, as the most dangerous unconventional threats seem to come from nation-states like Iran, Russia, and the People’s Republic of China, the definition is shifting focus once again.² Of course, the continuous redefinition of IW highlights the inability of a positive definition to capture the full variety inherent in a negative term like irregular.

At this point, the reader must be asking why, if the U.S. military craves positive definitions, does it insist on using negative terms like unconventional warfare and IW.³ The answer is that these negative terms accurately capture the unwelcome strangeness of warfare that is not the conventional warfare the U.S. military understands and considers normal. The terms unconventional warfare and IW appear more often in public debate when the warfare of the day does not conform to the public's expectations. The U.S. military is even more invested in a specific, conventional, understanding of warfare than the public is and hence, the U.S. military is even more disconcerted by warfare that is not conventional and violates expectations. Imposing a positive and, in the case of UW, static definition on these negative terms gives the U.S. military the comforting illusion that it has captured all the unwelcome strangeness in a single positive definition and the positive definition offers the hope of a single solution that will lead to success in every non-conventional situation.

The Two-Stage Solution to the IW Problem

First, let's recognize that the U.S. military has invested too much in the UW term for too long to be willing to radically redefine it now. Instead, we should focus on the more realistic goal of fixing the definition of IW.

To fix the IW term, we can look at how another community handles the problem of negative definitions, specifically the term irregular. The medical profession uses the term irregular heartbeat. As every English speaker would expect, there is essentially one way to be regular but many ways to be not regular or irregular. In this case, a normal or regular heartbeat falls within well-defined limits in terms of speed and rhythm. An irregular heartbeat, on the other hand, can take many forms such as being too slow or too fast, jumping between being too slow and too fast or having any rhythm other than the normal rhythm, etc. Different forms of irregularity will have very different implications for treatment. For example, we want to slow down a heart that is beating too fast, but slowing down a heart that is already too slow could be fatal. Thus, using the same treatment for all irregular heartbeats would be disastrous, and trying to find such a treatment is a dubious quest, but it would be the implied task if medicine imposed a positive definition on the term irregular heartbeat.

The term irregular heartbeat does not tell us what treatment to apply, but this does not make it a useless term. On the contrary, it works well for both the patient and the medical professional because the first question they are asking is whether the heart is doing its job. The quickest and easiest way to check is to listen to the heartbeat. A regular heartbeat is a good sign whereas an irregular heartbeat is a bad sign requiring further investigation. The focus then turns to finding exactly how the heartbeat is irregular, such as whether the heartbeat is too fast or too slow, and how to treat the specific irregularity. Thus, medical professionals deal with the negative definition of irregular heartbeat with a two-stage solution. In the first stage, they determine whether the patient has a normal or irregular heartbeat. If the heartbeat is irregular, then they go to the second stage and determine

exactly what is irregular about the heartbeat. This produces a positive definition of the patient's condition and indicates the specific treatment required.

Applying this approach to IW gives us an accurate definition of IW as warfare that is not regular or conventional. (The U.S. military prefers the term conventional warfare over regular warfare, just as the medical community prefers the term normal heartbeat over regular heartbeat.) As with the irregular heartbeat, this definition of IW leaves us with the follow-up or second-stage challenge of defining exactly what is irregular about a particular instance of warfare and how to deal with that irregularity. This two-stage approach to IW also tracks with the ever-expanding list of IW activities, which started with five in 2010 and grew to twelve by 2021⁴, since the activities are positive terms with associated doctrine.

Defining Conventional Warfare, The Many Ways to Be Irregular, and their Implications

At first glance, defining IW as warfare that is not conventional warfare seems unhelpful since it merely forces us to define conventional warfare. Fortunately, conventional warfare has had a very stable definition for a century and provides a great starting point for defining IW. Since World War I, conventional warfare has had the following characteristics:

- It is conducted by the uniformed armed forces of recognized nation-states, during times of recognized hostilities between them, in areas recognized as theaters of armed conflict.
- The armed forces are attempting to destroy one another using self-propelled metal warships on the surface of the sea, submarines below the surface of the sea, aircraft attacking targets on land and sea and in the air, and armies attacking each other with direct and indirect fire from cannons, rockets, missiles, machineguns, grenades, etc.
- The ground troops increase their mobility using cargo aircraft as well as wheeled and tracked vehicles, often protected by some sort of armor.
- Outside their vehicles, soldiers seek cover and concealment using camouflage, trenches, and foxholes.
- Military forces are commanded by designated military authorities, assisted by extensive staff, and the entire system is connected by wired and wireless electronic communications.

It is worth contrasting the remarkable stability of conventional warfare over the past hundred years with the extraordinary changes in conventional warfare between 1820 and 1920. In 1820, there were no aircraft or submarines, warships were made of wood and powered by sails, there were neither wired nor wireless electronic communications, there were no indirect fire or motor vehicles, armies wore brightly colored uniforms and marched toward the enemy shoulder to shoulder across open fields, military staffs were little more than a collection of the commander's chums and a few errand boys, and the feudal

kingdoms and empires that conducted conventional warfare were hopelessly disorganized compared to the industrial-era states of 1920.

There have been periods during the last hundred years when conventional wars were relatively rare compared to other forms of armed conflict, but the common understanding of conventional warfare has been surprisingly stable for a long time.

Two additional points require emphasis before moving to the concept of IW. First, IW, like diplomacy, can take place with or without conventional warfare. Since the start of conventional warfare does not mean the end of IW, the two are often intertwined and mutually supporting. Second, different nations have different relationships with any given conflict. For example, the Second World War was the largest in human history, involving unprecedented levels of conventional warfare and IW, but for neutral nations like Sweden or Turkey, the Second World War involved no warfare of any kind. By the same token, at the time of this writing Ukraine and Russia are engaged in a large conventional war, but many nations, such as Poland and Belarus, that are not direct participants in the conventional warfare, are supporting one side or the other and are therefore conducting IW activities against the side they oppose. Thus, the same event can be conventional warfare for some parties, IW for other parties, and not warfare at all for neutrals who take no part in the contest.

Defining the key aspects of conventional warfare allows us to identify some of the ways warfare can be irregular. The specific irregularity, like a specific type of irregular heartbeat, gives us clues as to how to handle that specific case. To structure our discussion, we will define conventional warfare in terms of the 5W's—*who, when, where, what/how, and why*—and then define IW in these same terms and consider the implications for the conduct of IW. The findings are summarized in Table 1 below, followed by a more extensive discussion of each of the 5W's.

5Ws	Conventional Warfare	Irregular Warfare (IW)	Implications for IW
Who	<ul style="list-style-type: none"> Uniformed armed forces of nation-states on both sides. 	<ul style="list-style-type: none"> Uniformed forces on one side, irregular forces on the other (e.g., insurgents, terrorists, criminals) States using proxies, surrogates, intelligence services 	<ul style="list-style-type: none"> Diverse actors create complex coordination challenges. Requires adaptability in strategy and operations.
When	<ul style="list-style-type: none"> Fixed periods of interstate conflict. 	<ul style="list-style-type: none"> No time constraints; often prolonged. 	<ul style="list-style-type: none"> IW campaigns have fluid start and end points. Rules of Engagement (ROE) and authorities evolve continuously.
Where	<ul style="list-style-type: none"> Defined state territories and international waters. 	<ul style="list-style-type: none"> No territorial limitations. 	<ul style="list-style-type: none"> Geographic flexibility affects ROE and authorities.
What/How	<ul style="list-style-type: none"> Direct/indirect combat to defeat enemy forces. 	<ul style="list-style-type: none"> Sabotage, subversion, guerrilla warfare. Support to one party in a conventional war without direct involvement. Information, economic, and financial warfare. 	<ul style="list-style-type: none"> Conventional forces have a smaller role, while SOF and non-DoD actors have a larger role. Security Force Assistance (SFA) and Security Cooperation are key.

<p>Why Conduct One Over the Other</p>	<ul style="list-style-type: none"> • States maintain control. • Clear, legitimate, and state-enhancing outcomes. 	<ul style="list-style-type: none"> • Lower cost and risk than conventional warfare. • Opponents struggle to identify who, where, when, and how they are being engaged 	<ul style="list-style-type: none"> • Conventional warfare is rare; IW is continuous. • IW is harder to control and produces more ambiguous outcomes.
--	--	---	--

Table 1: Comparative analysis of conventional and irregular warfare, highlighting key distinctions and their strategic implications.

Who

Who participates in conventional warfare: Conventional warfare is conducted by the uniformed armed forces of nation-states operating against the uniformed armed forces of the opposing nation-states.

Who participates in IW: IW is conducted by, or against non-state actors such as terrorist organizations, revolutionaries, insurgents, and criminal organizations. IW is also conducted by nation-states through combat or other warlike activities by forces other than their uniformed armed services. Such forces include proxies, surrogates, intelligence services, and irregular armed civilians as well as military personnel out of uniform like the “Little Green Men” Russia employed in Crimea in 2014.

Implications of irregular participants: Irregular participants have specific implications and definitions under U.S. legislation and military doctrine (JP 3-05). Employing U.S. forces against terrorist organizations is Counterterrorism (CT). The employment of U.S. forces against revolutionaries and insurgents is Counter Insurgency (COIN). Employing U.S. forces to assist a partner nation in combating subversion, terrorism, insurgents, revolutionaries, and criminal organizations is Foreign Internal Defense (FID). Employing U.S. forces to assist foreign insurgents or foreign forces resisting occupation is Unconventional Warfare (UW). Employing U.S. forces to assist a foreign nation in reforming, improving, and expanding its armed forces, including during wartime, falls under Security Force Assistance (SFA) which in turn falls under Defense Security Cooperation (DSC). Covert action, typically by U.S. intelligence agencies, falls under Title 50 U.S. Code § 3093.⁵ U.S. support to foreign forces that are assisting U.S. Special

Operations Forces combatting terrorism falls under Title 10 U.S. Code § 127e.⁶ When the U.S. military recruits, trains, equips, and pays salaries to foreign militaries, paramilitaries, and individuals supporting U.S. IW operations, it falls under section 1202 of the 2018 National Defense Authorization Act.⁷

Thus, IW involves an extraordinarily diverse set of actors, each with their own strengths and weaknesses, capabilities, and limitations, and this creates a much wider variety of friendly and enemy options and friendly and enemy vulnerabilities than in conventional warfare. Taking full advantage of all the unusual tools available in IW, and defending against all of the adversaries' irregular options, requires even more imagination and mental agility than conventional warfare.

When

When does conventional warfare take place: Conventional warfare takes place when a recognized nation-state announces that it is in hostilities with another recognized nation-state. So much has been made of the lack of official declarations of war⁸ that commentators seem to have lost sight of how clearly and consistently nation-states announce the commencement of conventional warfare. When Russian President Vladimir Putin launched a full-scale conventional invasion of Ukraine in 2022, he announced it to the world on television.⁹ When former U.S. President George W. Bush invaded Iraq in 2003, he announced it to the world on television,¹⁰ just as his father had announced the start of conventional warfare against Iraq in 1991.¹¹ Conventional warfare also ends with a major public announcement such as the much-maligned announcement of the end of major combat operations in Iraq by President George W. Bush aboard the USS Abraham Lincoln on 1 May 2003.¹²

When does IW take place: By contrast, Putin made no similar announcement when his "Little Green Men," i.e., Russian soldiers pretending not to be Russian soldiers, entered Crimea in 2014. In fact, Russian spokesmen denied these IW operations were being conducted by Russian forces,¹³ or later, claimed that the Russian troops fighting in Ukraine were on vacation and not acting on orders from the Russian government.¹⁴ Similarly, when the U.S. military conducts counterterrorism strikes in places like Somalia,¹⁵ the operations are not acknowledged or are followed with minimal public announcement and certainly nothing like the dramatic public announcements that accompany the beginning and ending of conventional warfare. The beginning and end of IW operations and activities may require the approval of the highest levels of government but will rarely involve major public announcements.

Implications for IW: IW activities lack the clear beginning and ending characteristics of conventional warfare. Instead, IW typically starts long before conventional warfare and continues long after conventional warfare is over, and frequently IW campaigns begin and end without any conventional warfare taking place. This means IW requires a flexible mindset capable of frequently and carefully updating tactics, techniques, procedures, and

rules of engagement to accomplish missions while staying within evolving peacetime and wartime legal authorities and permissions.

Public announcement of IW events: The emphasis on publicly announced beginning and endings for conventional warfare does not mean Presidents and other heads of state never announce IW operations. For example, U.S. President Ronald Reagan made a major public announcement after U.S. planes bombed Libyan government facilities in 1986,¹⁶ and U.S. President Barack Obama announced the 2010 killing of Osama bin Laden immediately after that event as well.¹⁷ However, these announcements were made to announce the end of these operations. Reagan said that he had struck Libya in retaliation for a recent terrorist attack on U.S. servicemen in West Germany by Libyan agents, but also that he considered the matter closed and would not continue similar raids unless Libya conducted another terrorist attack. Likewise, Obama was announcing a major counterterrorism success but was also announcing to Pakistan that it was a single event that was now over and not the beginning of a campaign of unilateral U.S. attacks inside sovereign Pakistani territory. By contrast, the long campaign of U.S. counterterrorism drone strikes inside Pakistan was conducted with minimal publicity and without dramatic announcements signaling either the beginning or end of the campaign.¹⁸

Where

Where does conventional warfare take place: The geographic boundaries of conventional warfare are the territories of the contesting states and wherever their forces meet in international waters, but it excludes the territory of neutral states. For example, in 2024, if Ukrainian and Russian forces meet in Ukraine, or Russia, they are duty-bound to try to kill one another, and if captured, they are entitled to prisoner-of-war status. However, if Ukrainian and Russian military personnel are in uniform in Buenos Aires, Argentina, and attempt to kill each other, they are subject to prosecution for attempted murder by the Argentine legal system.

Where IW takes place: Any warfare in neutral territory by the parties to a traditional war is inherently IW. These activities, such as World War II operations by the Axis and Allies in neutral Portugal and Turkey, are typically conducted by intelligence services making them irregular in both location and participants. IW can also take place inside the same territory as conventional warfare, if the participants or methods are irregular, for example, attacks on German forces in occupied France were IW when conducted by the French Resistance while attacks on those same forces were conventional warfare when conducted by uniformed Allied forces.

Implications of IW geography: Even when conventional warfare is underway, IW is not bound by the geographic limits of conventional warfare. Instead, IW has a different geography specific to the type of IW campaign underway. However, IW campaigns are not therefore geographically unbounded and may face very specific geographic restrictions and completely different rules of engagement, authorities, and permissions depending on where they are conducted. For example, assassinating Nazi officials in occupied Europe was a

common IW tactic during World War II,¹⁹ but similar assassinations were generally not conducted in neutral territory.

What/How

What sorts of operations are conventional/How is conventional warfare conducted: Conventional warfare operations directly attack the armed forces of the opposing power. Conventional operations can also indirectly attack the enemy's armed forces through things like sieges, blockades, attacks on transportation networks, attacks on industrial production, and other targets that weaken enemy forces by denying them logistical support. Of course, uniformed military forces have often been used against civilians, as in the famous Nanjing Massacre of 1937-38, but these are usually considered war crimes and hence not part of conventional warfare.

The tools of conventional warfare have been remarkably consistent and well-understood for generations. Overhead, military aircraft monitor and attack the enemy. Under the sea, submarines hunt surface ships and each other. On the surface of the sea, internally powered metal warships hunt submarines and each other while protecting themselves from air attack. On land, uniformed soldiers take and hold terrain, move across the land in wheeled and tracked vehicles that are often armored, and attack the enemy with direct and indirect fires from guns, rockets, and missiles while protecting themselves from air attacks. All these forces are commanded and controlled by national civilian and military leaders, supported by large staffs, relying on wired and wireless communications.

There have been some innovations. For example, in the past half-century, some of the overhead monitoring has been done from space and some of the wireless communication has been facilitated by satellites. Furthermore, in the past thirty years, some of the wired and wireless communication has involved cyber. Additionally, in the past two decades, a growing number of aircraft have been unmanned. In the future, some of the staff functions may be done by Artificial Intelligence. However, these technical innovations have enhanced rather than replaced conventional activities.

What sorts of operations are IW/How is IW conducted: President John F. Kennedy provided a famous description of IW methods during a speech in 1962 when he said:

This is another type of warfare, new in its intensity, ancient in its origins, war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat: by infiltration instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him.²⁰

President Kennedy was a veteran of conventional warfare in World War II, speaking to the American public that had witnessed World War II, or grown up on stories of the war, and had internalized conventional warfare as the normal form of warfare. Kennedy was not providing a catalog of every possible IW technique but rather providing an emotional and impressionistic understanding of IW to help his audience recognize the challenges ahead.

As Kennedy suggests, an enormous variety of operations fall under IW and since no list of such operations could be exhaustive, we will not attempt such a list here.

However, one sort of IW deserves special attention and that is when a nation assists one party in conventional warfare rather than participating directly in the conventional fight. Two major examples, a half-century apart, are Soviet support to North Vietnamese forces that were conducting conventional warfare against U.S. forces in Vietnam, and U.S. support to Ukraine in the conventional warfare Ukraine has been conducting against Russia since February 2022. In Vietnam, the U.S. and North Vietnam were conducting conventional warfare and IW against each other, whereas the Soviets were conducting IW against the U.S. but not conducting conventional warfare. Similarly, after Russia launched a full-scale invasion of Ukraine, Ukraine and Russia are conducting both conventional warfare and IW against each other but the U.S. is only conducting IW against Russia and is not conducting conventional warfare.

The difficult question: What methods are, and are not, warfare? This analysis has benefited from the impressively consistent understanding of conventional warfare methods over the last hundred years. However, there is no such consensus about what is—and is not—warfare. Some feel that warfare must involve violence or at least the threat of violence. Others embrace more expansive visions of warfare. What are we to make of terms like economic warfare, financial warfare, information warfare, or even George Kennan's term from the early days of the Cold War, political warfare? Are these metaphorical uses of the term warfare like the use of war in the War on Poverty or even the Cold War? Or are these genuine forms of warfare outside the conventional method of direct attack but within the IW realm? It is a judgment call and one we will not attempt to resolve here, but to the extent that these liminal cases are in fact warfare, they are IW and not conventional warfare.

The use of the word warfare within the IW term also creates problems within the U.S. government and with partners and allies. In many forms of IW, the U.S. military is working closely with, or even in support of, civilian agencies, departments, and international partners. These agencies, departments, and foreign partners are anxious to advance U.S. and partner interests and counter threats to those interests, but they are often uncomfortable having their activities described as warfare. From their perspective, warfare takes place only during wartime. Until there is a traditional war with large-scale conventional combat operations, they consider themselves to be at peace and hence not involved in warfare. Furthermore, there is concern that the term warfare implies the military should be the lead agency and non-military agencies are anxious to avoid subordinating themselves to the military in peacetime.

For all these reasons, interagency and international partners may be more comfortable with terms like strategic competition than IW for describing unfriendly activities below the level of conventional warfare.

Why

All warfare is conducted to protect and advance the political goals of the participants, so the purpose is identical for both conventional warfare and IW. There are, however, reasons for choosing one or the other.

Why conduct conventional warfare: Conventional warfare has several advantages over IW. First, conventional warfare, particularly when conducted within the laws of war, lends greater legitimacy to the outcome and the participants. Conventional warfare reinforces state authority since it is conducted by states through the overt actions of uniformed employees of the state in pursuit of the publicly announced goals of the state. Successful conventional wars, such as the North Vietnamese conquest of South Vietnam in 1975 and the U.S. liberation of Panama in 1989 and Kuwait in 1991, enhance the reputation of the victors while achieving their goals. Clandestine and covert actions, on the other hand, always have a nefarious and dishonest feel to them. Even when they succeed, it is hard to take credit for them and the outcome is less legitimate since the victor seems to have cheated. Governments also have a high degree of control over their uniformed armed forces, but much less control over irregular surrogates, making many IW operations more difficult to control than conventional military operations.

Why conduct IW: For non-state actors, there is no other choice. Either they conduct IW, or they conduct no warfare at all and find more cooperative ways to interact with their enemies.

For states, conventional warfare has some unattractive features. First, conventional warfare is spectacularly expensive. In fact, it is usually the most expensive activity states engage in, and the expense is not merely financial. Conventional warfare requires—and risks destroying—the most expensive land, sea, and air vehicles available at the time. They also involve enormous property damage while killing and maiming thousands, or even millions of government employees and citizens. Conventional warfare also involves enormous opportunity costs since it is difficult for a nation to do anything else while conducting conventional warfare. For example, President Lyndon Johnson blamed the Vietnam War for the limited impact of his Great Society programs: his administration simply could not do both at once.²¹

In addition to the cost, conventional warfare is enormously risky. Since conventional warfare is highly visible and closely associated with the national leadership conducting it, defeat is frequently fatal. Manuel Noriega and Slobodan Milosevic failed in conventional warfare and died in prison. Saddam Hussein failed in conventional warfare and was executed by his own people. Even winning in conventional warfare does not guarantee the leader's political future. For example, Winston Churchill was voted out of office immediately after winning World War II and George W. Bush lost the 1992 presidential election shortly after winning the 1991 Gulf War.

IW, on the other hand, usually comes with much lower costs and risks. IW activities typically involve much smaller and less expensive forces and frequently much of the personal risk is being borne by foreigners. The clandestine nature of many IW activities

makes it easier to deny when they fail. Even a spectacular and undeniable IW failure, like the Kennedy administration's famous fiasco at the Bay of Pigs, had a minimal impact on the President's political future and the financial and human costs were trivial compared to conventional warfare. For example, if Kennedy had landed the U.S. Marine Corps at the Bay of Pigs and it had turned out the same way, the results would have been infinitely worse for his administration.

For anyone assessing the relative merits of conventional warfare and IW as methods of accomplishing national goals, Vladimir Putin's experience in Ukraine is highly instructive. Let's quickly review that history. In 2014, a pro-Russia President was forced out of Ukraine by street protests (the Maiden Revolution). Putin responded with a highly successful IW campaign that captured Crimea at nearly no cost, and less successful IW campaigns in several other Ukrainian oblasts that gained him control of about half of Donetsk and Luhansk at an acceptable cost. However, after 2014, Ukraine and its supporters were on the lookout for "Little Green Men" and Putin's other IW tricks. By 2022, it appeared that Putin had gained all he could in Ukraine via IW. Putin should have watched and waited and advanced his interests when and where he could with IW methods. Instead, he lost patience, doubled down on his maximalist goals, and escalated to conventional warfare.

Two years after switching to conventional warfare, Putin had roughly doubled the part of Ukraine he controlled, but at a catastrophic cost to his military (hundreds of thousands of casualties and so much equipment destroyed that he is pulling 60-year-old tanks out of storage); his economy (he is facing economic sanctions unlike anything imposed on a major country since World War II); and his nation (in addition to hundreds of thousands of casualties, hundreds of thousands of healthy and educated young men have fled Russia to avoid participation in the war). The cost increases daily, with no end in sight, while there is little reason to hope he will ever expand his territorial gains enough to justify the cost. Putin's switch from IW to conventional warfare makes a strong case for IW and highlights the risks of escalating to conventional warfare.

Conclusion

This essay has provided an explanation of why the U.S. military has had difficulty defining IW and proposed a two-step solution to the problem modeled on the way medical professionals treat an irregular heartbeat. The first step is to embrace the definition of IW as "all warfare other than conventional warfare" and assess whether a specific challenge falls into the IW category. The second step is identifying what is irregular about a specific instance of IW and how best to exploit or counter that form of irregularity.

The essay then provided a detailed description of conventional warfare that has remained stable for a century and did so in terms of the 5Ws: who, when, where, what/how, and why. It then used the description of conventional warfare to provide a detailed description of the many ways warfare can be irregular and investigated their implications.

By following the model medicine uses with irregular heartbeats, this essay has avoided the trap of seeking some magical element common to every instance of IW. Instead, this

essay embraces the vast diversity within IW and the enormous number of options it provides to IW practitioners. By emphasizing the myriad options available, it is hoped that the two-step approach suggested here will unleash the creativity and imagination of IW practitioners.

Endnotes

¹ U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, January 2021, <https://irp.fas.org/doddir/dod/dictionary.pdf>.

² Jared M. Tracy, "From 'Irregular Warfare' to Irregular Warfare: History of a Term," *Veritas* 19, no. 1 (2023).

³ It is interesting to note that the Russians get by without the term irregular warfare and only use the term to describe how it is used in U.S. doctrine, even though the Russians have extensive doctrine for many different forms of irregular warfare. See Christopher Marsh, "Russia's 'Special' Way of War," forthcoming in *New Faces of Irregular Warfare*, edited by the Irregular Warfare Center (Washington, D.C.: Irregular Warfare Center, 2024). Perhaps centuries of Imperial Russian and Soviet experience with many forms of irregular warfare has made today's Russians more comfortable than their Western counterparts with warfare that is not conventional.

⁴ Office of Irregular Warfare and Competition, Directorate for Joint Force Development (J-7), *Curriculum Development Guide for Irregular Warfare*, June 3, 2022, 8.

⁵ U.S. Code, 50 U.S.C. § 3093, <https://www.law.cornell.edu/uscode/text/50/3093>.

⁶ U.S. Code, 10 U.S.C. § 127e, <https://www.law.cornell.edu/uscode/text/10/127e>.

⁷ *Public Law 115-91*, U.S. Congress, December 12, 2017, <https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf>.

⁸ Valery Gerasimov, "The Value of Science Is in the Foresight," *Military Review*, January-February 2016.

⁹ Vladimir Putin, "Address by the President of the Russian Federation," *Kremlin*, Moscow, February 24, 2022, <http://en.kremlin.ru/events/president/news/67843>.

¹⁰ George W. Bush, "President Bush Announces Start of Iraq War," CNN, March 19, 2003, https://www.youtube.com/watch?v=5BwxI_l84dc.

¹¹ George H. W. Bush, "Address to the Nation Announcing Operation Desert Storm," *The Gilder Lehrman Institute of American History*, January 16, 1991, accessed May 26, 2023, <https://www.gilderlehrman.org/history-resources/spotlight-primary-source/address-nation-announcing-operation-desert-storm-1991>.

¹² Office of the Press Secretary, "President Bush Announces Major Combat Operations in Iraq Have Ended," *The White House*, May 1, 2003, <https://georgewbush-whitehouse.archives.gov/news/releases/2003/05/20030501-15.html>.

¹³ Bill Chappell and Mark Memmott, "Putin Says Those Aren't Russian Forces in Crimea," *NPR*, March 4, 2014, <https://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea>.

¹⁴ Terrence McCoy, "Russian Troops Fighting in Ukraine? Naw. They're Just on 'Vacation,'" *Washington Post*, August 28, 2014, <https://www.washingtonpost.com/news/morning-mix/wp/2014/08/28/russians-troops-fighting-in-ukraine-naw-just-on-vacation/>.

¹⁵ "The War in Somalia," *New America*, accessed March 5, 2025, <https://www.newamerica.org/future-security/reports/americas-counterterrorism-wars/the-war-in-somalia/>.

¹⁶ Ronald Reagan, "President Reagan's Address to the Nation on the Bombing of Libya, April 14, 1986," *Reagan Library*, April 14, 1986, <https://www.youtube.com/watch?v=pjYMVSA6xM8>.

¹⁷ Barack Obama, "President Obama on Death of Osama bin Laden," *The Obama White House*, May 1, 2011, <https://www.youtube.com/watch?v=ZNYmK19-d0U>.

¹⁸ Aqdas Khudadad, “Secret War: U.S. Drone Strikes in Pakistan,” *Immigration and Human Rights Law Review*, November 29, 2022, <https://lawblogs.uc.edu/ihr/r/2022/11/29/secret-war-u-s-drone-strikes-in-pakistan/>.

¹⁹ Callum MacDonald, *The Assassination of Reinhard Heydrich* (Edinburgh, UK: Birlinn, 2007).

²⁰ John F. Kennedy, “United States Military Academy Commencement Address,” *American Rhetoric: Online Speech Bank*, delivered June 6, 1962, West Point, New York, <https://www.americanrhetoric.com/speeches/jfkwestpointcommencementspeech.htm>.

²¹ Francis M. Bator, “No Good Choices: LBJ and the Vietnam/Great Society Connection,” *American Academy of Arts & Sciences*, January 2007, <https://www.amacad.org/publication/lbj-vietnam-great-society-connection>.

‘Seeing Red: A 2024 Guide to Assessing Resiliency and Resistance in Russia’¹

Robert S. Burrell, University of South Florida, Tampa, Florida, USA

Arman Mahmoudian, University of South Florida, Tampa, Florida, USA

ABSTRACT

This essay employs a data-driven, human-centric methodology to examine resiliency and resistance in President Vladimir Putin’s Russia. Using a four-phase approach, it analyzes state resiliency, assesses resistance to governance, identifies resistance movements, and explores options for external actors to influence Russia’s stability or support opposition to Putin. The methodologies used are drawn from previous publications in *Small Wars & Insurgencies and Expeditions* with Marine Corps University Press. Findings indicate that while Putin’s Russia exhibits fragility in resiliency, external actors—particularly China—have opportunities to bolster the regime. Though Russia harbors significant resistance potential, external support for such movements remains challenging. Based on available data, the Communist Party of the Russian Federation emerges as one of the most effective resistance groups, with the potential to inspire broader opposition.

KEYWORDS

resistance, resilience, communism, Russia, Vladimir Putin

Introduction

Since Vladimir Putin assumed power in 1999, Russia has witnessed significant civil unrest, demonstrating widespread dissatisfaction with the government and its policies. Putin’s harsh crackdowns have failed to quell the Russian population’s desire for increased transparency, government accountability, and economic equality. In this context, it is crucial to assess the potential for further civil unrest in Russia. This paper utilizes a data-centric methodology to examine Vladimir Putin’s governance and the opposition to it in terms of resilience and resistance. It leverages analytical data from top universities, financial institutions, governmental agencies, and non-governmental organizations to inform a four-phase process.

CONTACT Robert S. Burrell | robertburrell@usf.edu

The views expressed in this article are solely those of the author(s) and do not necessarily reflect the views, policy, or position of the U.S. Government, the University of South Florida, or the Department of Defense.

© 2025 Arizona Board of Regents/Arizona State University

Phase one measures the Putin regime's resiliency, as well as Russia's resistance potential, and then assesses the likely success of external support for resilience or resistance. Phase two identifies prevalent resistance organizations within Russia, categorizes these organizations along a continuum, and classifies their general nature. Phase three assesses one resistance organization (Communist Party of the Russian Federation) by examining its leadership, motivation, operating environment, organization, and activities. Phase four rationally evaluates the gathered information to make recommendations concerning potential external support for Russia's intrastate conflict.

Phase 1: Measuring Russia's Resilience and Resistance

Phase one frames Russia in terms of resilience and resistance (resiliency refers to the Putin regime's ability to overcome internal or external subversion, coercion, or aggression, while resistance refers to Russian society's, the population's, or a subgroup's opposition to malign indigenous power structures). Russia's resiliency and resistance metrics remain essential within the context of the current war in Ukraine, as well as Russia's broader confrontation with Western nations, in addition to possible external support by allies or partners like India, Iran, or China. The study of resilience and resistance in Russia reveals potential for (a) possible uses of external support to increase the Putin regime's resiliency, and (b) possibilities to subvert and destabilize Putin's regime.

Measuring Russia's Resilience

Russia is the largest nation on earth in terms of geography and nearly two times the size of the United States. Russia's population is 140 million, slightly more than Mexico's. The largest ethnic group is Russian at 78%, followed by smaller and varied ethnicities, the largest of which are the Tatars at 3.7%. The Russian diaspora includes 30 million living abroad, of whom 9 million live in Ukraine. In terms of language, the country is more unified with 86% speaking Russian as their primary tongue. The Central Intelligence Agency claims 15-20% of Russians practice the Orthodox faith and 10-15% are Muslim, with the majority nonpracticing believers or nonbelievers. In terms of governance, Russia officially abides by a semi-presidential administration but ostensibly acts as a dictatorship under President Vladimir Putin.²

Historical Factors

Alongside geography and demography, history plays an equally crucial role in Russian resilience. Unlike most European nations, which have deep cultural and civilizational ties with similar nations—for example, the Anglo-Saxon connections between the British, Canadians, Americans, and Australians, or the Germanic links among Germany, Switzerland, Austria, and the Netherlands—Russian kinship consists of Slavic or Russian-speaking peoples. Thus, Russia lacks a broader sense of historical ties with Western nations. This dynamic results in Russia being not alone but a lonely civilization. This perceived isolation influences Russia's resilience. The sense of uniqueness or separation prevents Russians from being inspired by Western forms of governance.

Russia's national identity, shaped by its historical context, plays a vital role in its resilience. Since the formation of the Russian state following the Mongol invasion in the thirteenth century, Russia's identity has been significantly influenced by its conflicts with Western civilization. Historically, Russia has viewed European powers such as Poland, Sweden, France, the United Kingdom, and Germany as adversaries. Western civilization, including its espousal of democracy, capitalism, and liberalism, is perceived by many Russians as a menace. This historical enmity undermines resistance against authoritarianism in Russia.

Russia's historical narrative emphasizes resilience and survival in the face of external threats. This narrative fosters a sense of unity, and a collective identity centered around the idea of a besieged fortress, reinforcing the nation's resolve to withstand external pressures. Throughout history, Russian governments have tried to solidify their grip on power by portraying Western influence as a destabilizing force, as many Russians equate stability with the preservation of their unique identity and sovereignty.

Political Factors

Russia's political spectrum is profoundly shaped by a combination of geography, demography, history, and identity. Putin's emphasis on traditional values and national pride serves as a counterbalance to Western liberal ideals. By promoting a distinct Russian identity rooted in historical experiences and cultural heritage, the state strengthens its position and minimizes the appeal of foreign ideologies. This deliberate cultivation of a unique Russian identity not only bolsters internal cohesion but also legitimizes Putin's authority and makes it harder for external influences to inspire change.

The nation's perceived isolation, historical antagonism towards the West, and emphasis on a unique national identity contribute to its resilience against external influences and internal resistance to authoritarianism. Understanding these factors is essential for comprehending the complexities of Russia's political landscape and its enduring sense of uniqueness in the global arena. Additionally, it also remains important to consider the historical memory of civic movements in Russia. Russians have not had favorable experiences with attempts to democratize the country, which has left a significant imprint on their collective consciousness. There have been two major efforts in Russian history to establish a democratic system, both of which ended in disappointment and turmoil (the Bolshevik Revolution of 1917 and the collapse of the Soviet Union in 1991).

The other political factor contributing to the Russian regime's resilience is Putin's carefully cultivated persona of strength in the face of adversity. Since his entrance on the political scene, Putin has consistently portrayed himself as a strongman by (a) decisively putting oligarchs in their place, (b) forcefully quelling the Chechen insurgency, and (c) standing firm against international sanctions. By curbing the power of the oligarchs, he reasserted state control over key economic sectors, signaling that no individual or entity could challenge his authority. His brutal military campaign in Chechnya demonstrated his willingness to use overwhelming force to maintain territorial integrity and suppress separatism. Additionally, Putin's defiant stance against Western sanctions, imposed in

response to actions such as the annexation of Crimea and interference in Ukraine, has further solidified his image as a resilient leader who can navigate and withstand external pressures. This combination of domestic control and international defiance has bolstered the Russian government's stability and resilience, reinforcing the perception of Putin as an indispensable and invincible leader.

Vladimir Putin's political persona, characterized by his strongman image and Napoleonic charisma, has significantly contributed to the resilience of the Russian government.³ This cultivated image of invincibility and decisive leadership has allowed Putin to centralize power and maintain tight control over the Russian state. His approach, marked by the suppression of dissent, extensive propaganda, and an appeal to nationalism, fosters a collective identity that prioritizes state survival over individual freedoms. This consolidation of power, akin to historical fascist regimes, has enabled the Russian government to navigate internal crises and external pressures with a semblance of unity and stability. Despite economic sanctions and international condemnation, Putin's ability to project strength and resolve has fortified the regime's endurance, effectively manipulating public perception and stifling opposition.

Economic Factors

The ability to generate significant revenue is a crucial component of Putin's power, as it enables his regime to finance its operations and maintain public services, even in times of crisis. In 2022, the World Bank estimated Russian gross domestic product as the eighth largest in the world at \$2.2 trillion, comparable to Canada's.⁴ Having a relatively large GDP and robust revenue generation capability provide a foundation for the government's power and stability, enabling it to withstand various internal and external pressures. It also allows Putin to maintain a high level of government spending on military, security, and social programs, which in turn bolsters his regime's resilience. The Federation's primary export remains mining and extractive industries (coal, oil, gas), but supplemented by a large defense industry and other types of industrial applications with sales worldwide.⁵ Russia's reliance on fossil fuel exports strengthens Putin's resiliency by providing a steady stream of income for governance functions that are relatively independent of direct taxation on its citizens. This fiscal buffer helps the government maintain social stability and mitigate the potential for civil unrest.

Despite the historical, political, and economic factors supporting the Putin regime, the analytics demonstrate that the Russian Federation has both low and below-average indicators of resiliency. The following percentiles rank Russia relative to other countries worldwide with 0% as the lowest and 100% as the highest. According to the World Bank, and in comparison, with other nations, Russia ranks at 14.49% in government accountability; 16.04% in political stability; 25.94% in government effectiveness; 13.21% in regulation efficiency; 12.26% in rule of law; and 19.34% in control of corruption.⁶ The *Fund for Peace's* state fragility index, ranks Russian fragility as above average in comparison with others at 53 of 179 (or 29.31%), between that of Turkey and Cambodia.⁷ Additionally, the *Swiss Re Institute's* macroeconomic resilience index showcases Russia's

resiliency as low (22 of 31 developed countries analyzed) at 29.03%. In order to measure Russia’s national will in support of Putin’s regime, we have chosen to rely on a framework developed by Delbert C. Miller.⁸

The following table utilizes Miller’s analysis methods (as closely as possible in line with available polling) and five categories to determine the national morale of the Russian Federation. (1) We consider Russians as the ingroup, in which, when polled, 65% were proud of their nationality.⁹ (2) In the same study, about 36% were optimistic or excited about the prospects of Russia’s political system over the next 10 years.¹⁰ (3) In the third category concerning the competency of national leaders, Vladimir Putin’s approval rating is soaring at 85%.¹¹ (4) In terms of Russian confidence in current resources to defend the interests of the state, about 77% of those polled support the war in Ukraine.¹² Lastly, (5) 52% of those polled believe “Russians are a great people of particular significance to the world,” which likely aligns with the Putin regime’s national goal.¹³ All five factors are outlined in Table 2 to assess national morale, which we assess collectively as 63%.

Factor	Ranking Assessment	Percentage Score
1. Belief in the Superiority of the Social Structure in the Ingroup	Above Average	65%
2. Degree and Manner by Which Personal Goals Are Identified with National Goals	Low	36%
3. Judgments of the Competence of National Leaders	High	85%
4. Belief that Resources Are Available to Hurl Back Any Threats to the Ingroup	High	77%
5. Confidence in the Permanence of the National Goal	Average	52%
TOTAL	Average	63%

Table 1: Basic factors of national morale in the Russian Federation

Tallying the six factors of governance from the World Bank, national morale, and state fragility equally (eight metrics in total), the resiliency of the Russian Federation is estimated at 23.89%, with obviously weak and below-average governance factors but coupled with above-average national morale.¹⁴ This dichotomy between weak governance combined with above-average patriotism indicates a ripe possibility for increasing resiliency in the Russian Federation but lesser opportunities, possibly, for resistance to opposition to the existing governance in the current environment.

Measuring the Potential for External Support to Putin's Resiliency

A variety of external actors have an interest in the stability of the Russian Federation. This is due to several factors including abundant natural resources, Russia's geostrategic position, its massive nuclear arsenal, and a desire to maintain Russia's role as an antagonist to the current international order. Consequently, external support for the Putin regime could include China, Iran, and North Korea but also possibly European states and even the United States. In other words, external support for the Putin regime's resiliency has real incentives that align with the national security interests of an eclectic group of diverse nations. We have determined the potential success of external support for the Russian Federation's resiliency on three factors: (1) the strength of Putin's diplomatic relations, (2) the self-reliance of Russia in terms of meeting its human security obligations in the absence of nonviolent assistance, and (3) the self-reliance of Russia in meeting its national security requirements in the absence of violent aid.

While the United States and much of Europe have imposed sanctions on Russia and provide lethal aid to the defense of Ukraine, in the long term, these same countries could attempt to reinforce the resiliency of governance in Russia in the future (or at least should maintain contingency plans to do so).¹⁵ Meanwhile, North Korea, China, and Iran all have interests in a stable Russian Federation as well, and each of these has provided diplomatic support to Russia following its invasion of Ukraine and is likely to continue to do so.¹⁶ Subjectively, the possibility of an external support strategy for Russian stability is high, estimated at 75%.¹⁷

Today, Russia appears self-sufficient in terms of meeting its human security obligations without the need for nonviolent aid. At its peak in 2007, the United States provided \$1.6B in aid, almost all of it delivered to the energy and military sectors to ensure the safety of Russian nuclear programs. Since 2019, U.S. nonviolent aid to Russia has dropped precipitously, with only \$110,000 in 2023 for wildlife conservation programs.¹⁸ As opposed to needing assistance, Russia has a recent history of contributing external support to the stability of other nations. In 2017, Russia contributed to large-scale developmental assistance programs with "the World Bank Group, the United Nations, major global initiatives, and special-purpose funds" totaling \$1.18B.¹⁹ Based on the Putin regime's self-reliance in meeting the human security requirements of the Russian population, the Russian Federation appears a good candidate for additive stability efforts made by external supporters, with success estimated at 75%.²⁰

Like its strong economic factors, Russia has demonstrated self-reliance in terms of national defense. Instead of importing lethal means, Russia has developed into one of the world's largest exporters. In 2011, Russia provided military sales to 35 countries and nearly matched the arms export material of the United States. Starting in 2019, however, Russian defense industry sales have fallen sharply, particularly after the invasion of Ukraine, which isolated Moscow from some of its former customers. While Russia's most important importers of lethal means remain China and India, it has also expanded its relationship with others like Turkey and Indonesia.²¹ In the short term, the Ukraine War has forced Russia to import war materials from North Korea and Iran, but the Federation will likely continue to

produce most of its security needs. With a self-reliant and world-class capacity, external support to Russian military security remains a sound wager with an estimated 75% chance of successfully increasing resiliency.²²

Averaging all three metrics (Russia's bilateral relations with potential sponsors, its innate ability to secure human security requirements, and its ability to arm, train, and equip its military) to an external actor choosing to bolster the Russian Federation's resiliency equates to 75%, which makes this foreign policy decision decisive if the stability of the regime remains the desired end state. China, in particular, has the resources and proximity to effect positive strength to Putin's Russia if needed, as a counterbalance to the aspirations of the West.

Measuring the Potential for Resistance in the Russian Federation

Over the past two decades, nonviolent and violent resistance in Russia has proven endemic. Between 2019 and 2024, 6,063 acts of violence occurred inside Russia with 1,452 fatalities. In the same period, eleven significant nonviolent protests were mobilized in Moscow, four of which garnered a violent response from the regime.²³ Five of the eleven protests lasted longer than a month and one had more than 100,000 participants. Terrorist acts in Russia have proven historically horrendous. Between 2015 and 2020, the *Global Terrorism Database* records 157 acts of terrorism, perhaps the most predominant during this period conducted by the Caucasus Province of the Islamic State (IS-CP).²⁴ While IS-CP activities have diminished since 2017, Islamic extremism in opposition to the Russian Federation remains a serious threat to its internal security. Recently, in March 2024, the attack by ISIS-Khorasan at the Crocus City Hall in Moscow killed over 130 people.²⁵

Objective data exist to measure the potential for internal resistance to current governance in the Russian Federation. We start with data derived from the *Global Economy*. This data ranks Russia in comparison with other nations, with 0% indicating little to no potential resistance to authority and 100% indicating the highest. Using this dataset: (a) in terms of current governance not adhering to the rule of law, 87.05%; (b) in political instability, 82.90%; (c) in the perception of the Federation not controlling corruption, 77.40%; (d) in a poor record on political rights, 86.17%; (e) in not respecting civil liberties, 84.57%, and (f) in its inability to regulate the shadow economy, 71.52%.²⁶

For additional indicators, we evaluate liberty, crime, and food security. *Vision of Humanity* maintains a global peace index which places Russia as 158 out of 163 (or 96.93% unpeaceful in comparison with others).²⁷ Also, *Freedom House* ranks Russia as categorically "unfree" and one of the worst at 87% in comparison with others.²⁸ In terms of organized crime, Russia ranks the 19th worst among 193 states (placing it in the 90th percentile).²⁹ Lastly, food insecurity does not appear a relevant factor in the Russian resistance environment, assessed as a 25% potential contributor.²⁹ Averaging all nine of the preceding data figures equally, the Russian Federation scores high in resistance potential at 78.87%, implying ample opportunity for resistance to change or reform current forms of governance. The following figure illustrates Russia's resistance potential in comparison with other European states.

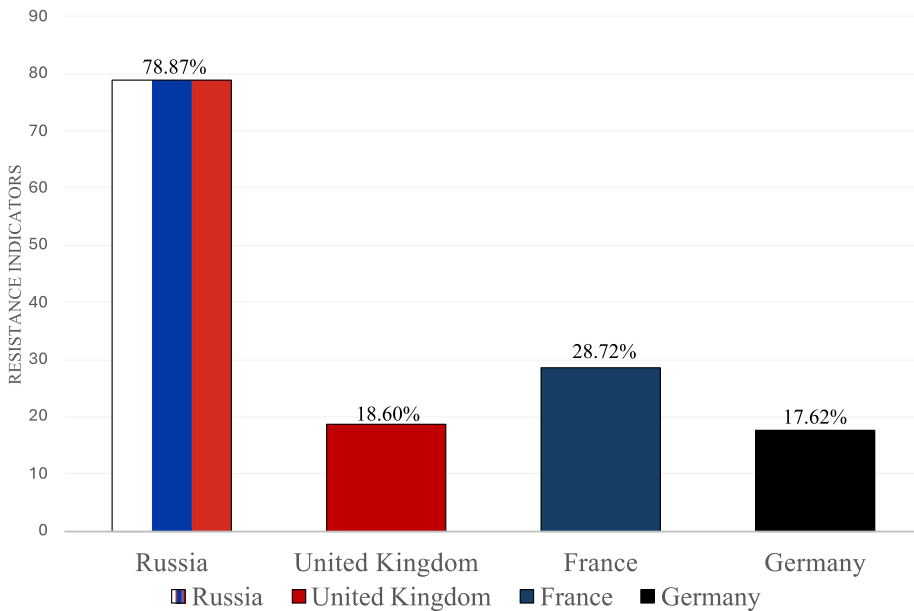


Figure 1: Comparison of Russian resistance potential with the U.K., France, and Germany³⁰

In comparison with the United Kingdom, France, and Germany, Russian resistance potential is over two and a half times that of France, and over four times that of the United Kingdom and Germany. The Russian Federation exudes corruption, crime, unrest, and oppression far more than its neighbors in Europe and appears ripe for resistance.

Measuring the Potential for External Support to Resistance in Russia

In this last step of phase one, we analyze the potential success of an external actor in supporting Russian resistance to the Putin regime. While the United States maintains diplomatic relations with the Russian Federation, it also lists Russia as a competitor and an antagonist to the current world order in its *National Military Strategy*.³¹ Considering Russia’s unfriendly and confrontational relations with the West, we rank the Russian Federation as a possible target of external support to resistance from an adversary as 100% plausible.³²

The historical case study analysis completed by the Study of Internal Conflict at the Army War College poses four important questions to indicate the possible success or failure of an insurgency.³³ (1) Firstly, 15% or more of Russia’s population does not identify as a citizen of the state. The answer to this is clearly no, as an opinion poll in 2024 revealed “94% expressing pride in their identity” as Russians.³⁴ (2) Secondly, 15% or more of the population does not acknowledge the legitimacy of the regime. With 85% of Russians

approving of Vladimir Putin, it remains clear that most Russians find the regime legitimate.³⁵ (3) 15% or more of the population have meaningful communication with a resistance movement. No violent resistance groups currently have sustained communication to this extent.³⁶ (4) Sanctuary exists for an armed component of resistance in a neighboring state. The answer here is likely no. Russia could be expected to use economic, military, and diplomatic means to ensure any Russian guerilla movement could not move back and forth across international boundaries (cyber offers access across international boundaries previously unrealized, which could prove important and in need of further study).

Examining all the data points presented regarding resistance potential, we assess that external support to a Russian-based resistance movement within the Federation has a possible success rate of 33%, with nonviolent and cyber-centric movements offering distinct advantages over those utilizing violent methods but also vulnerable to violent suppression by the totalitarian regime.

Phase One: Summary

In summation of phase One, based upon the information presented, the Russian Federation can be judged as having fundamental flaws in its current resiliency, primarily due to its poor metrics in governance (24.46%). Meanwhile, strategic partners of Russia, particularly China, have a good chance to reinforce the resiliency of the Putin regime should they desire to do so (75%). At present, the potential for internal resistance to the Putin regime is high due to poor indicators of proper governance (78.87%). Simultaneously, external support for resistance appears possible but risky, with a 33% probability of success.

Phase Two: Identifying Russia's Resistance Movements

While Russia has a low record of success regarding resistance movements, since the collapse of the Soviet Union, Russia has experienced civil unrest, generally emerging in waves, highlighting dissatisfaction with the government and its policies. From anti-corruption rallies to anti-war demonstrations, the country's streets have echoed with voices of dissent, despite the government's stringent measures to curb such activities. During the period from 1990 through 2019, major outbreaks of Russian resistance mobilized six times, with only one success (the pro-democracy movement 1990-1991), a success rate in the post-Soviet period of 17%.³⁷

Nonviolent Resistance

Despite the pro-democracy movement's triumph, most Russians view the changes it brought as a disaster. During the Presidency of Boris Yeltsin, the new Russian Federation embarked on a series of radical economic and political reforms intended to transition Russia to a market economy and democratic governance. This period was characterized by widespread corruption, economic hardship, and substantial political instability – paving the ground for the rise of newcomers, and oligarchs, to take over a large portion of Russia's economy and financial resources. Additionally, the vacuum of power left behind by the collapse of the Soviet Union triggered major disruptions to national security, including two

generations of brutal wars in Chechnya, which further entrenched the perception that democracy has brought disorder and suffering.

Thus, for many Russians, the concept of democracy is indelibly linked with instability, economic collapse, and social unrest. The collective memory of the hardships endured during these periods has led to a preference for stability and security over the uncertainties of democratic change. This perspective is often reinforced by Putin's narratives that any attempt to undermine the state's authority, not only would destabilize the current affairs and livelihood of Russians, but it also could endanger Russia's territorial integrity and its very existence. As a result, the idea of a stable and secure Russia, even under an authoritarian regime, is more appealing to many Russians than the perceived chaos of a democratic system. Understanding this historical context is crucial for comprehending the complexities of Russia's political landscape and the deep-seated resistance to democratization efforts within the country.

Between 1999 and 2020, approximately 2.2 million people mobilized on more than a hundred occasions in nonviolent protests during Vladimir Putin's dictatorship.³⁸ Between 2020-2024, eleven protests and demonstrations occurred, which add up to an additional 187,302 protesters seeking changes in governance.³⁹ In total, during Putin's regime, nonviolent protesters opposed to his leadership or policies totaled 916,876 mobilized. For contemporary events, we highlight a few recent waves against the Putin Regime, starting with the Russian invasion of Ukraine in 2014.

First Invasion of Ukraine: Anti-War Protests (2014)

The annexation of Crimea in March 2014 sparked a new wave of demonstrations, this time focused on Russia's aggressive foreign policy. Although smaller in scale compared to previous protests, these anti-war rallies underscored a growing unease with the Kremlin's actions on the international stage. Protesters hit the streets in Moscow twice in March and once in September, totaling around 112,000.⁴⁰ The government's swift crackdown on these protests reflected its zero-tolerance approach to dissent.

Anti-Corruption Protests (2017-2018)

The fight against corruption took center stage in March 2017 when opposition leader Alexei Navalny published a damning report on Prime Minister Dmitry Medvedev's alleged corrupt practices. This investigation ignited nationwide protests, drawing thousands into the streets and resulting in mass arrests. The momentum continued into June 2017, with further demonstrations on Russia Day seeing significant police action against protesters. Navalny's influence persisted in 2018, as he called for a boycott of the presidential election after being barred from running. January 2018 saw supporters rallying in Navalny's favor, demanding a fair electoral process and transparency. Putin arrested Navalny in May, and protesters emerged again throughout the country referring to Putin as Russia's new Czar.⁴¹ The total number mobilized during this period on ten occasions was around 122,000.⁴²

Election Protests (2019)

In the summer of 2019, Moscow witnessed large-scale protests demanding fair local elections. Opposition candidates had been disqualified, prompting citizens to take to the streets in June, July, and August. The total number mobilized on nine occasions equates to roughly 97,000.⁴³ The authorities' response was marked by mass arrests and police violence, revealing the state's determination to maintain control over the electoral process.

Constitutional Changes (2020-2021)

The announcement of proposed constitutional changes in January 2020, which would allow Putin to potentially remain in power until 2036, triggered a new series of protests. Demonstrators expressed their frustration with what they saw as an erosion of democratic principles in Russia. The return of Alexei Navalny to Russia in January 2021, and his immediate arrest, led to some of the largest protests in recent memory. Thousands took to the streets across the country, demanding his release and an end to political repression. The government's response was severe, with widespread detentions and a heavy police presence. Total numbers were around 122,000 mobilized.⁴⁴

Second Invasion of Ukraine (2022-2023)

The invasion of Ukraine in February 2022 brought a new wave of anti-war protests. Demonstrators decried the military action and called for peace, facing significant repercussions from the authorities. Protesters numbered around 10,000.⁴⁵ Through March 2023, anti-war protests continued sporadically, although participation waned due to the heavy-handed crackdowns and severe legal consequences for demonstrators.

Nonviolent action between 2014 to 2023 reveals major activity by four primary organizations. (1) The *Russian United Democratic Party* (Yabloko) is currently led by Nikolai Rybakov. While representation remains small, *Yabloko* remains an official party in Russia and desires "a liberal, progressive, and a European perspective for Russia."⁴⁶ (2) *The People's Freedom Party* (Parnus) has a long history of dissent towards Putin and therefore subject to continuous attacks by the regime, including the assassination of its leaders. In May 2023, Russia's Supreme Court dissolved Parnus as an official Russian party to ensure it could not compete in the 2024 election. Seeking sanctuary, Parnus' President, Mikhail Kasyanov, left Russia in 2022 to live in exile in nearby Latvia.⁴⁷ (3) *Russia of the Future* remains an unregistered political party under the former leadership of internationally recognized activist Alexei Navalny. Navalny faced suppression, imprisonment, and recent execution by the regime.⁴⁸ It remains to be seen if Navalny is erected in martyrdom to mobilize resistance or if his death terminated the viability of *Russia of the Future*. (4) An interesting and budding political rival to Vladimir Putin's regime remains the *Communist Party of the Russian Federation* (KPRF).⁴⁹ In apprehension, it appears Putin has begun to defraud KPRF of many votes.⁵⁰ Reporter Robyn Dixon for the *Washington Post* wrote that the KPRF is "starting to behave like genuine opposition" to Putin.⁵¹ In summary, despite the disparate groups operating through legal activities directly or indirectly in opposition to the regime, nonviolent legal resistance appears fairly disunified in terms of cooperation

with each other (i.e. there exists no united front).⁵² While this might imply that these movements do not constitute a threat to the Putin regime, the violent suppression of most of these groups demonstrates that Putin views them as real threats to his power.⁵³

Violent Resistance

A major factor contributing to Putin's resilience is the paradoxical effect where violent resistance against the government can sometimes lead to Putin expanding his power. The Chechen resistance, a violent struggle for independence of the Chechnyan Republic (1994-2009), exemplifies this dynamic. Chechen insurgents directly challenged the Russian Federation's control over the region. The resistance of the Chechen minority threatened the Russian national identity, leading to a rally-around-the-flag effect, where the general populace supported stronger measures. Putin's administration used the war to introduce laws that enhanced the powers of law enforcement and security agencies, allowing for greater monitoring and suppression of opposition activities. These measures were often framed as necessary for national security, gaining broad public support despite their erosive impact on democratic freedoms. By framing the Chechen resistance as a dire threat to national unity, Putin was able to consolidate his power and extend his influence over the Russian state. The centralization of authority during this period set a precedent for how the government could respond to other forms of resistance, using similar tactics to bolster its resilience in the face of opposition.

The Chechen example highlights a broader pattern where resistance movements, particularly those involving minority groups, can inadvertently empower the government's resilience. When the state successfully frames such resistance as a threat to national security, it can garner widespread support for measures that would otherwise be seen as severe. This dynamic creates a double-edged sword: while resistance seeks to challenge the government's power, it can also provide the government with the justification it needs to strengthen its control.

Understanding this paradox is crucial for formulating effective foreign policies and strategies to support opposition movements in Russia. Simply, while resistance against the Russian government is a necessary and legitimate response to authoritarianism, it is vital to recognize the potential for such movements to inadvertently strengthen the very regime they oppose. Any support for resistance must be carefully calibrated to avoid reinforcing the government's narrative of threat and justification for increased repression. Strategic support for resistance must be nuanced and aware of these dynamics, aiming to undermine the government's power without reinforcing its claims of defending national integrity and security.

While generally unsuccessful in creating change, several nonviolent groups utilizing illegal methods, as well as organizations using violent resistance, have been pervasive in Russia. Since Putin's ascendency in 1999 through June 2024, 19,459 Russians have died in internal hostilities (the vast majority occurring in Chechnya).⁵⁴ Three nonstate groups remain significant: (1) the *Chechen Republic of Ichkeria*, a loosely organized coalition with continued ambitions for Chechen independence; and (2) the *Caucasus Emirate*, an umbrella term for several armed groups in the North Caucasus which have lain fairly dormant for

several years, with the exception of one offshoot, *Islamic State – Caucasus Province*.⁵⁵ (3) Another Islamist resistance group includes *Islamic State – Khorasan Province*, which conducted the attack on a Moscow concert hall with 93 people killed and 145 wounded on 22 March 2024.⁵⁶ Several other resistance organizations in Russia have emerged following the invasion of Ukraine in 2022. The largest includes (4) *Wagner Group*, which conducted a short but prominent rebellion under the leadership of Yevgeny Prigozhin in June 2023.⁵⁷ Smaller groups include (5) *Military Organization of Anarcho-Communists*, which practices illegal forms of resistance, particularly disseminating subversive propaganda, sabotaging railways in Russia and Belarus, and conducting twenty arson attacks on military registration and enlistment offices.⁵⁸ Another resistance group choosing illegal methods includes (6) *Stop the Wagons*, an anti-war organization that has used explosive devices on railways.⁵⁹ Similarly, (7) *Black Bridge* has targeted Russian government offices, including the arson of a Federal Security Service building in March 2023.⁶⁰ Another illegal and subversive organization is (8) *Atesh* (meaning “fire” in Tatar), whose agents collect information on Russian military activities in Siberia and send that intelligence to Ukraine. In contrast, there are several insurgent groups directly attacking Russia as paramilitary organizations, three have politically unified while fighting in Ukraine in the Irpin Declaration which includes (9) the *Russian Volunteer Corps*, (10) the *National Republican Army*, and (11) the *Freedom of Russia Legion*.⁶¹

Irregular Support

Under Putin’s dictatorship, he has collaborated with several nationalist and illicit organizations to implement his ambitions abroad and suppress dissent at home. The full array of these irregular cohorts was exhibited, and invigorated, during the Russian annexation of Ukraine in 2014, where paramilitary groups, illicit organizations, and private military companies took a primary role in the front lines. (1) Wagner Group continues to work for the Kremlin as a counterforce to the liberal order, with activities in Libya, the Central African Republic, Mali, Mozambique, Sudan, Madagascar, Cameroon, the Democratic Republic of Congo, Zimbabwe, Kenya, Venezuela, and others.⁶² Wagner continues to fight alongside the Russian Army in Ukraine. Putin has also collaborated with nationalist paramilitary organizations that suppress Russian dissent at home, act as auxiliaries to fight in Ukraine and support U.S. and European white nationalist extremist groups. A major nationalist paramilitary organization includes the (2) Russian Imperial Movement (RIM), a monarchist Orthodox movement, which supported Russian resistance in Donetsk, Ukraine (2014-2022), fights alongside the Russian Army in Ukraine (2022-present), and was designated a terrorist organization by the U.S. Department of State in 2020 (particularly for its collaboration and training with white supremacist groups internationally).⁶³ In his early administration, Putin treated the (3) Russian mafia (*Vory*) as a criminal organization, but the war in Ukraine has witnessed a growing collaboration between the two.⁶⁴ Wagner Group certainly recruited members of *Vory* from Russian prisons to fight on the front lines. More disturbing, *Vory* wields a strong and effective global underground, and Russia is utilizing it “as an arm in its intelligence apparatus,” including the carrying out of targeted assassinations abroad.⁶⁵ To surmise, Wagner Group, Russian Imperial Movement, and *Vory* should not be considered simply proxies of the

Putin regime, as they have their own motives and ideologies, but they do currently act as his grey-zone allies.

Phase Two: Summary

The following figure illustrates prevalent Russian resistance movements across a resistance continuum, including (from left to right) nonviolent legal, nonviolent illegal, rebellion, and insurgency. Additionally, on the far right of the scale, no known insurgent groups have yet to rise to the level of belligerency by exhibiting the functions of an opposing state.⁶⁶ Irregular organizations supporting the Putin regime are not illustrated (Wagner Group, Russian Imperial Movement, and Vory).

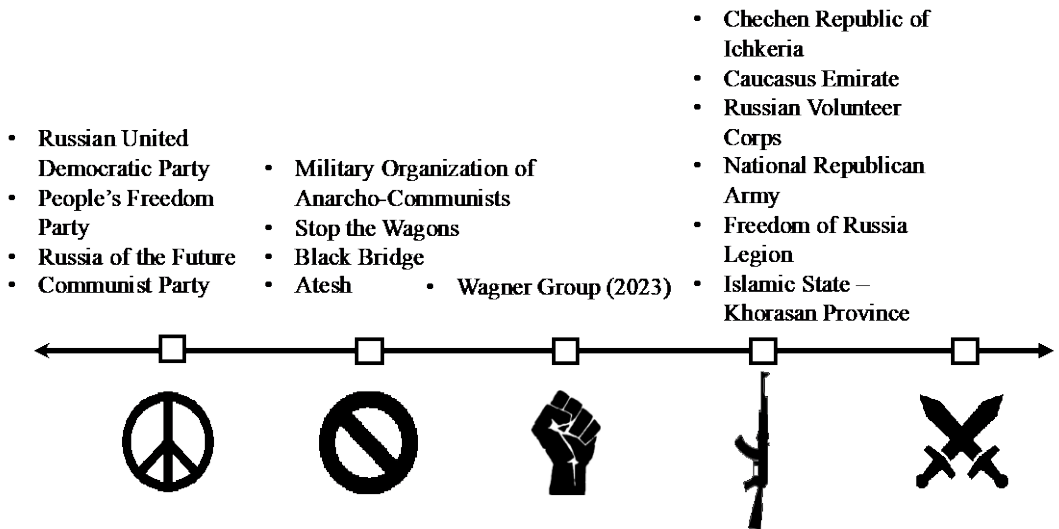


Figure 2: Diagram of the Russian Federation’s resistance continuum

Phase Three: Assessing Russia’s Resistance Movements

After identifying resistance movements along a continuum, we present a deeper investigation into Russia’s communist party – KPRF. In assessing the Communist Party, we examine five attributes: (1) actors, (2) causes, (3) environment, (4) organization, and (5) actions.⁶⁷

The Actors in the Communist Party of the Russian Federation (KPRF)

The actor category includes types of leaders in KPRF, its participants, how KPRF interacts with the population, its relations with other resistance movements, and sources of external support. As background, KPRF was founded in 1993 as a successor to the Communist Party of the Russian Soviet Federative Socialist Republic when the Soviet Union fell. KPRF remains the viable and overt political opposition to United Russia and the Putin regime.⁶⁸ It is the second-largest party in Russia, representing 57 of the 450 delegates in the State Duma. The current and long-standing General Secretary remains Gennady Zyuganov, who

assumed office in 2001. Zyuganov had a strong chance of winning the presidency in 1996 but sought to nationalize major industries. In response, several Russian oligarchs made the “Davos Pact” that same year to fund propaganda against him.⁶⁹ Nevertheless, Zyuganov nearly won with 40% of the vote, demonstrating great popularity.⁷⁰ He ran again for President in 2008, showing less than half his previous popularity with 17.76% of the vote. Still retaining at least some political strength, Zyuganov’s current platform rests on three primary principles “Stalinism, nationalism, and social-democratic paternalism.”⁷¹

Zyuganov’s leadership role appears that of an agitator. While he supports the current war in Ukraine,⁷² Zyuganov has demonstrated harsh criticism of Putin as well. In 2008, he made the following remarks to the Central Committee of the Communist Party: “The ruling group has neither notable successes to boast of, nor a clear plan of action. All its activities are geared to a single goal: to stay in power at all costs...Its social support rests on the notorious ‘vertical power structure’ which is another way of saying intimidation and blackmail of the broad social strata and the handouts that power chips off the oil and gas pie and throw out to the population in crumbs, especially on the eve of elections.”⁷³ Scholar Katlijn Malfliet describes KPRF as a mutant, an adaptor, and a chameleon-like actor, facilitating change in Russia as it simultaneously evolves to the conditions.⁷⁴ It has demonstrated great resiliency, clinging to communist ideals of a foregone era while participating in a strangely semi-democratic form of governance in which communism now speaks as the minority.

KPRF has three major ideological lines: (1) a Marxist-Leninist orthodoxy, espousing socialist ownership of the means of production in order to redistribute wealth to the people; (2) a national-socialist and clearly anti-western agenda; and (3) a social-democratic discourse highlighting the need for popular sovereignty by means of free and fair elections.⁷⁵ However, over the past decade, the third line of effort (social-democratic discourse) has become more prominent, with frequent calls for election transparency, increased rule of law, and respect for the constitution.⁷⁶ As such, KPRF serves with increasing frequency as opposition to the corruption of the current regime, while it simultaneously plays a game of survival, which it has done adeptly since the fall of the Soviet Union.

In terms of demographics, KPRF represents an estimated 12% of voters. In the regional committees, 54% of the Communist Party leadership is over 60 years old. This figure does not imply that KPRF consists of Soviet era politicians, as 55% of the regional leadership started their careers in the party after the dissolution of the USSR. All are highly educated with 99% college graduates. KPRF includes many professional lawyers, representing 29% of the regional committees. Only 9% of this leadership is female.⁷⁷

We explore here how viable KPRF is to the Russian ingroup within the general population. Jonathon Cosgrove and Erin Hahn propose a scale, with participants in the resistance on the left, loyalists to the regime on the right, and a spectrum of popular support in the middle.⁷⁸ The following figure illustrates current support for the Putin regime and resistance to it based on election results in 2024. Active resistance includes all banned parties in Russia, of which there have been dozens since 1991. The most prominent and

recent ones include Russia of the Future (dissolved in 2021) and several others, all considered resistance participants. On the surface, these numbers appear to be about 1% or less of the population (subsurface undergrounds remain undetermined). Five active parties sitting in the Duma include: (1) KPRF, considered passive supporters of resistance; (2) A Just Russia for Truth (SZRP), also included as passive support for resistance (particularly considering KPRF and SZRP have discussed merging in 2022);⁷⁹ (3) the New People (NP) party is expected to behave as Putin sympathizers, (4) Liberal Democratic Party of the Russian Federation (LDPR), considered passive support for Putin; and (5) United Russia, considered Putin loyalists. Additionally, 22% of Russians did not vote in 2024 and are listed as indifferent bystanders or fence-sitters.⁸⁰

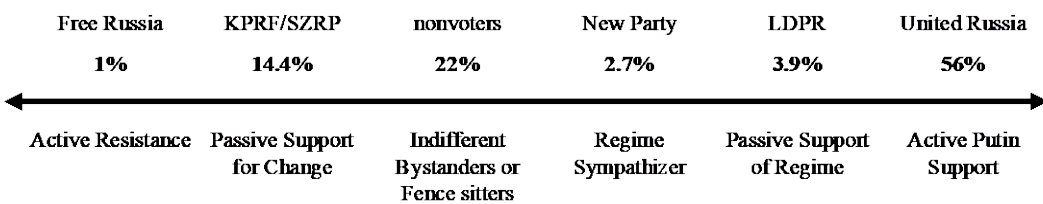


Figure 3: Scale of popular support for and against resistance

While elections illustrate a scale of opposition to and support for the current regime, a large segment of the Russian population continues to regard Putin as a hero. This cult of personality has varied from 60% of the population considering Putin a hero in 2008 and dropping to 38% in 2021.⁸¹ Polling over the past two decades indicates that Russians remain extremely patriotic and nationalistic, with two prominent communists, Stalin and Lenin, rating them as the “most outstanding people of all time.”⁸² Russians hold deep contempt for traitors, greed, and dishonesty, all three characteristics that could feed a negative narrative against the Putin regime.⁸³ Thus, the espoused values and platform of the Communist Party should remain appealing to most Russians, and given the right conditions, the popularity of KPRF could rise indirectly in opposition to United Russia, while direct opposition to Putin remains a challenge.

KPRF’s relations with other resistance organizations vary. We regard those not in the ingroup as incompatible with KPRF, including the Chechen Republic of Ichkeria, the Caucasus Emirate, Islamic State – Khorasan Province, and Russian paramilitary groups in Ukraine. In contrast, A Just Russia for Truth (SZRP) presents an opportunity for KPRF to expand its ranks. Other underground opposition organizations could align with KPRF, but those desiring change to align with Western Europe would likely find those ideals incompatible.

KPRF attempts to align with communist and socialist movements worldwide, a continuation of the type of powerful alignments that evolved in the early twentieth century. KPRF attends the International Meeting of Communist and Workers’ Parties annually. In 2023, this meeting included delegations from 54 nations.⁸⁴ The communist and socialist

front worldwide remains quite significant and provides agency and legitimacy to these ideologically aligned movements. While communism has generally declined since the fall of the Soviet Union, several nations continue to uphold communist ideals, the most powerful of which is China. Other organizations, particularly those acting as resistance within Europe, might prove important in garnering external support for KPRF. Meanwhile, overt support from Western governments could prove subversive to the KPRF cause.

Cause of the Communist Party of the Russian Federation.

KPRF remains a Marxist-Leninist organization, espousing social justice, collectivism, freedom, and equality.⁸⁵ Its ideals are directly spelled out by its program and approved by the KPRF Congress. Socialism remains the evolved and fair system of human governance. Capitalism is viewed as unjust, which the West forced upon Russia when it subverted the USSR and resulted in catastrophe.⁸⁶ The KPRF seeks to build a renewed and advanced 21st-century socialism in Russia. The principles of KPRF have some alignment with the domestic and foreign policies of Putin, in that it maintains a nationalistic and anti-Western ideology that espouses the restoration of the Russian people as a great world power. However, KPRF adopts a socialist Russia, one in which private ownership, particularly of natural resources and industry, is severely curtailed, and that runs counter to a system of powerful oligarchs backing the Putin regime.

Several scholars have begun to recognize KPRF's growing schism with the Putin regime. As stated by political scientist Oleksiy Bondarenko in 2023, "Although the party is considered to be a member of the so-called 'loyal' opposition, the increasing volatility of the party system and growing political instability have implications for future relations between the KPRF and the regime."⁸⁷ In contrast to the direct support of Putin, the KPRF appears to vacillate between direct opposition to regime proposals and/or bargaining indirectly for concessions. Opposition has grown more frequently, primarily because for KPRF to remain a viable political entity, it needs popular support, while election fraud erodes its representation. Hence, as Putin attempts to consolidate power by co-opting the democratic process, this inevitably sets him at odds with the Communist Party.

The Resistance Environment in the Russian Federation.

Assessing the resistance environment for KPRF includes the evaluation of environmental, socio-political, and relationship factors. KPRF will likely continue to utilize legal (and sometimes illegal) but nonviolent activities as opposed to Putin's regime. Bondarenko states that "KPRF is not only the most likely to engage in street activism and protests but is also the party with the most autonomous network of activists at the sub-national level."⁸⁸ As a nonviolent resistance, the physical geography of Russia has less impact on KPRF's potential success, making the space and information domains the most influential. The cyber domain remains essential, particularly for maintaining KPRF's messaging, recruitment, and propaganda.

Russians' access to the internet (or RUNET) has skyrocketed. In 2008, 38 million Russians could access the internet (or 27% of the population).⁸⁹ By 2024, that estimate has risen to 132 million or 88% of the population.⁹⁰ Most scholars agree, however, that

television remains the primary information source for Russians. When polled, 86% consider television their primary medium for news; however, only 56% of those say they trust the news provided on television.⁹¹ As such, RUNET remains primary as an alternative means of getting information and of particular use for resistance messaging. Under the Putin regime, Russia has instituted “an intricate multi-layered system of surveillance and excessive control over online content,” all under the guise of protecting national security.⁹² Russian users have resorted to virtual private networks (VPN) to hide their signatures. In April 2022, one Russian VPN provider (AtlasVPN) recorded a 2,000% increase in usage.⁹³ In March 2024, Putin banned VPN advertising, but VPN companies continue to operate under Russian legislation.⁹⁴ For now, KPRF is harnessing RUNET for its purposes while staying in compliance with regulations.

Since its inception in 1993, KPRF has skillfully navigated Russia’s socio-political environment, surviving when most Western and even domestic pundits believed communism was dead. It has survived by remaining in compliance with the Russian constitution and reserving its nonviolent actions (like unscheduled protests) for specific, and popular, agenda items. KPRF has also wedded its narrative to a belief in Russian exceptionalism, or greatness, which nests well with traditional ideals of Russian foreign policy, going back to the Czars period.⁹⁵ As such, it has harnessed Russian patriotic history, including the Soviet era – to a greater extent than its competitors. Communism, however, does not generally appeal to the Russian business sector. In a positive economic climate, one might expect KPRF membership to remain stagnant. However, should the Russian economy suffer, the KPRF’s socialist agenda may increase its popularity.

KPRF leadership and membership offer an excellent case study for social network analysis and a scientific approach to understanding its relationships domestically and internationally. One scholar, Jan Matti Dollbaum, conducted a study on KPRF’s use of social media to politicize grievances towards Russia’s pension reform legislation in 2018. Both KPRF and Aleksey Navalny’s Free Russia party sought to block these measures through legal forms of resistance, and both utilized the platforms of Twitter and VKontakte (Russia’s version of Facebook) to mobilize protest.⁹⁶ This demonstrates that KPRF can align its narrative at times with outspoken critics of the Putin regime.

Organization of the Communist Party of the Russian Federation

Jonathon Cosgrove and Erin Hahn generally categorize resistance organizations into two bins: (1) mass organizations and (2) elite organizations.⁹⁷ KPRF obviously resembles a mass organization. It claims 160,000 members and organizes its activities with a headquarters in Moscow. It maintains a Central Committee, made up of 188 members. It has 89 regional committees headed by first secretaries. Gennady Zyuganov serves as both the General Secretary of the party itself as well as its parliamentary leader in the Duma.⁹⁸ In the 2021 elections for the State Duma, exit polling suggests that only 55% of people voted, but that 24% of them voted for the KPRF, only slightly less than United Russia with 38%.⁹⁹ If so, KPRF currently retains more popularity in Russia than its representation in the Duma suggests. Currently, KPRF has 57 of the 450 seats, which equates to 12.7%, while United Russia has 325 seats (72%).

KPRF utilizes several methods to communicate with its members and the general population. Unlike illegal organizations, it retains “legally guaranteed airtime before elections and press coverage of its parliamentary activities.”¹⁰⁰ Additionally, it leverages social media, with posts coming directly from the party headquarters and not from individual accounts.

KPRF also advocates for a youth movement called Movement of the First. Although President Putin officially appointed the leadership and funding for the Movement of the First, KPRF argues that this organization traces its lineage to the Soviet Union’s Young Pioneers. KPRF is attempting to indoctrinate and recruit future communists from this group.¹⁰¹ In fact, both Gennady Zyuganov and Vladimir Putin can be seen meeting with these young people at various events, essentially competing for influence.

Resistance movements can be sub-organized in a myriad of ways. In most military doctrines, these can include (a) a public component, (b) an auxiliary, (c) an underground, and (d) an armed component.¹⁰² The Communist Party likely wields three of these currently: a public component, an auxiliary, and an underground. The public component is the outward workings of the party itself as discussed. In terms of an auxiliary, the party has 160,000 members but millions of supportive voters behind secret ballots. From 2014-2022, KPRF successfully organized a communist underground in Donetsk, Ukraine.¹⁰³ The Donetsk People’s Republic communist organization merged with KPRF following Russia’s annexation of the region in 2022. KPRF has the history, capacity, ideology, and tradecraft to effectively organize an underground if desired.

Actions of the Communist Party of the Russian Federation

As previously discussed, KPRF seeks nonviolent but legal forms of resistance to establish its goals of a democratic and socialist Russia. It leverages its voting power to assure concessions from the Putin regime, particularly to placate its constituents regarding social welfare programs. When needed, it harnesses nonviolent action to protest and harness public support. It consistently utilizes information operations domestically and internationally to garner support for its cause. It walks a thin line between passive protest of the Putin regime and acquiescence to United Russia.

Phase Three: Summary

In phase three, we summarized one of the fifteen resistance organizations identified in phase two. The Communist Party of the Russian Federation (KPRF) comprises a substantially sized organization with a discernable counter-vision for Russia to that of President Vladimir Putin’s regime but also some solidarity in terms of nationalism and re-establishment of a greater Russia. KPRF has broad support and opportunities to expand its influence, particularly in coalition with A Just Russia for Truth. The poor performance of Putin’s military in the current war in Ukraine, as well as the inevitably negative economic fallout for Russia after it, offers opportunities for KPRF to expand its representation in the State Duma. Any actions by the Putin regime to hijack the democratic process in Russia will inevitably lead to a clash between the two.

Phase Four: Options in Support of Resilience or Resistance

In phase four, we utilize the data gathered in the previous three phases to better inform the foreign policies of nation-states regarding the Russian Federation. The typical suggestion for action formulates a proposal for one of three options: (a) support the resilience of the Putin regime, (b) support resistance to the Putin regime, or (c) choose to support neither, but prepare the environment for future policy.

Supporting the Resilience of Putin's Russia

Two nations overtly support the resiliency of Russia – Iran and North Korea, as both sell vital arms and equipment to fuel Russia's war in Ukraine. Meanwhile, China is providing tacit support to Russia, and India is continuing military and economic collaboration, maintaining an overt alliance. Russia maintains more diplomatic support globally, particularly in Africa.¹⁰⁴ Meanwhile, the West has instituted broad sanctions to stifle the Russian economy, as well as giving billions of dollars of military support to Russia's rival in Ukraine. European opposition to the Putin regime remains strong, but the support of the United States in funding the war in Ukraine appears to be waning. Compounded by a war weariness of two decades fighting in Iraq and Afghanistan, 45% of Americans polled in 2024 believe the U.S. is spending too much in Ukraine.¹⁰⁵ Many pundits believe the U.S. presidential election in November 2024 will decide future U.S. policy towards Russia.¹⁰⁶

There remains the option for the West to support Russia's resilience, but little appetite for it, particularly for strengthening institutions in Putin's Russia. The current approach concentrates only on the near-term consequences of holding Russia accountable for invading Ukraine—essentially building a broad coalition to ensure Russia cannot oppose the international order. The long-term implications of Russia's resiliency, or lack thereof, have not been given much consideration in Western foreign policies yet remain vital to European and global security. The grand strategy should consider the implications of a resilient Russia versus a fragile one and offer a contrarian foreign policy option to deliberate.

Supporting Russia's Resistance

While the United States and most European nations remain in staunch opposition to the Putin regime, they have not offered external support to domestic resistance to him. Supporting the war in Ukraine and supporting domestic resistance to Putin in Russia remain two distinctly different, although complementary, foreign policy options. Western countries might consider sponsoring either nonviolent or violent forms of Russian resistance. Despite the applause in Western media sources for activists like Alexei Navalny, anyone deemed as pro-West has not proven popular in Russia. Violence includes insurgent groups in the Caucasus region, but the tactics utilized by many of these opposition movements remain incompatible with Western values. Additionally, the Russian paramilitary groups operating in Ukraine may appear acceptable, but they are too small to be considered serious opposition, and they are Western-leaning – an unpopular characteristic for Russian support.

KPRF proves an intriguing option for Western support. On the one hand, it is the sole organization currently wielding the potential to oppose Putin. On the other hand, the United States and other nations placed sanctions on KPRF leaders Gennady Zyuganov and Ivan Melnikov following the invasion of Ukraine in 2022. Western policy has not progressed to distinguish a difference between Putin's regime and its most powerful opposition – KPRF.

One strategic approach might be to support nationalist movements within Russia, not just KPRF but possibly others. Yevgeny Prigozhin's rebellion with Wagner Group in June 2023 exemplifies the potential of such organizations to challenge the Putin regime. This recommendation is grounded in several key considerations. First, nationalist movements have strong ties with a significant portion of the Russian population, which grants them some support. This grassroots backing makes them a potent force for change, capable of mobilizing segments of society against the current regime. However, while supporting nationalist movements within Russia might seem like a strategic way to weaken Putin's regime, this approach comes with significant drawbacks. A major concern is the problematic ideologies these groups often espouse, including racism, anti-Semitism, and xenophobia. Additionally, provoking instability in Russia without a clear objective could prove a disastrous course of action with unanticipated results.

Choose to Support Neither but Prepare the Environment for Future Policy

While supporting Putin's regime appears undesirable, aiding resistance poses a significant risk. In the absence of a strategy to support resilience or resistance, Western foreign policy should avidly attempt to prepare the environment for a positive transition to future foreign policy. Despite the fifteen Russian resistance movements identified, Vladimir Putin remains strongly entrenched as the leader of Russia, with no real opposition identified in our data as capable of replacing him. Consequently, maintaining dialogue with Putin allows for a future policy in which strengthening Russian institutions makes sense. Conversely, the West should maintain an open dialogue with the many resistance organizations in Russia. Maintaining sanctions on the primary opposition party in the State Duma (KPRF members) might not comprise the best long-term strategy in terms of dialogue with the opposition. As several European countries endorse socialist perspectives, making inroads with KPRF collaboratively could prove constructive or at least identify more possibilities.

Conclusion

Our analysis of Russia in terms of resilience and resistance highlights significant weaknesses in governance under Putin's Russian Federation, with resistance potential remaining high. However, support for resistance movements has a low probability of success, whereas bolstering Putin's resilience may offer strategic possibilities. Of the many resistance groups, none provides an ideal alternative to Putin. Nonviolent resistance has been suppressed, political opponents eliminated, and violent opposition met with military force. Moreover, Putin has increasingly collaborated with militant and illicit groups to counter dissent and challenge opponents abroad. This volatile domestic environment pushes

Putin toward aggressive foreign policies to placate a largely nationalistic population, making positive change in relations with the West unlikely during his rule.

As outlined in this paper, nationalist movements in Russia possess significant potential to challenge the government. However, their diverse and decentralized nature makes them difficult to analyze or support as a coherent entity. By contrast, the Communist Party of the Russian Federation (KPRF), with its centralized structure, offers a clearer subject for analysis, using established metrics. While the KPRF remains the most organized and potentially viable alternative, it is far from an appealing choice. These factors warrant Western concern about the future trajectory of Russia.

Endnotes

- ¹ Robert Coalson, "Seeing Red: Russia's Communist Party Makes Gains In New Duma, But Does It Matter?," *Radio Free Europe/Radio Liberty*, September 22, 2021, <https://www.rferl.org/a/russia-communist-party-duma/31473164.html>.
- ² *CIA World Factbook*, <https://www.cia.gov/the-world-factbook/>, accessed May 13, 2024.
- ³ Richard Sakwa, "Putin's Leadership: Character and Consequences," *Europe-Asia Studies* 60, no. 6 (2008): 879–97, <https://www.jstor.org/stable/20451564>.
- ⁴ "Gross Domestic Product," *World Bank*, found at https://databankfiles.worldbank.org/public/ddpext_download/GDP.pdf, accessed on 13 May 2024.
- ⁵ *CIA World Factbook*.
- ⁶ *The World Bank*, "Worldwide Governance Indicators," <https://www.worldbank.org/en/publication/worldwide-governance-indicators>, accessed April 2, 2024.
- ⁷ *Fragile States Index*, <https://fragilestatesindex.org/>, accessed April 2, 2024.
- ⁸ Delbert C. Miller, "The Measurement of National Morale," *American Sociological Review* 6, no. 4 (August 1, 1941): 487–98. Ben Connable et al., *Will to Fight: Analyzing, Modeling, and Simulating the Will to Fight of Military Units* (Santa Monica, CA: RAND Corporation, 2018). Ben Connable, "Structuring Cultural Analyses: Applying the Holistic Will-to-Fight Models," *Journal of Advanced Military Studies: Special Issue on Strategic Culture* (2022): 153–67.
- ⁹ Dina Meltz et al., "Generation Putin: Proud but Politically Disengaged Russians," *Chicago Council on Global Affairs*, March 2024, <https://globalaffairs.org/sites/default/files/2024-04/Generation%20Putin.pdf>, accessed May 15, 2024.
- ¹⁰ *Ibid.*, 6.
- ¹¹ "Do You Approve of the Activities of Vladimir Putin as the President (Prime Minister) of Russia?," *Statista*, April 2024, <https://www.statista.com/statistics/896181/putin-approval-rating-russia/>, accessed May 15, 2024.
- ¹² Nate Ostiller, "Poll: 77% of Russians Support War in Ukraine," *Kyiv Independent*, February 7, 2024, <https://kyivindependent.com/poll-77-of-russians-support-war-in-ukraine/>, accessed May 15, 2024.
- ¹³ Meltz et al., "Generation Putin."
- ¹⁴ These metrics do not include the Swiss Re Institute's Resilience Index as it accounts for only 31 nation states.
- ¹⁵ U.S. Department of State, *U.S. Bilateral Relations Fact Sheets*, <https://www.state.gov/u-s-bilateral-relations-fact-sheets/>, accessed May 20, 2024.
- ¹⁶ Leo Chiu, "Explained: Who are Russia's Allies? A List of Countries Supporting the Kremlin's Invasion of Ukraine," *Kyiv Post*, October 23, 2023, <https://www.kyivpost.com/post/13208>, accessed May 20, 2024.
- ¹⁷ We considered the following in determining this percentage. If Russia had only adversarial or limited diplomatic relations internationally, it is assigned 25%; if Putin's Russia had at least one recognized partner, 50%; and if Putin has established and maintained multiple partnerships with other nations, 75%.
- ¹⁸ Foreign Assistance. *U.S. Agency for International Development*. Accessed May 20, 2024. <https://www.foreignassistance.gov>.
- ¹⁹ "Russia and the World Bank: International Development Assistance." *The World Bank*. Accessed May 20, 2024. <https://www.worldbank.org/en/country/russia/brief/international->

development#:~:text=The%20current%20cooperation%20between%20the,security%2C%20and%20global%20health%20-%20thereby.

²⁰ To subjectively determine if foreign aid would increase the regime's ability to provide for human security functions, the following criteria were applied: If human insecurity appears endemic, foreign aid will likely not provide long-term security (25%). If aid reinforces sound governance structures that are temporarily at risk, it is assessed at 50%. If the regime receives little aid due to the strength of endogenous resources, the assessment is 75%.

²¹ Cullen Hendrix, "Russia's Boom Business Goes Bust," *Foreign Policy*, May 30, 2023.

²² To subjectively determine if security sector assistance would increase the regime's ability to provide for national security functions, the following factors were considered: If military insecurity appears endemic, the success rate is assigned 25%. If military aid reinforces somewhat reliable security forces that require temporary external support, it is assessed at 50%. If the regime is self-reliant in meeting its security needs, the success rate is assigned 75%.

²³ Carnegie Endowment for International Peace, accessed May 21, 2024,

<https://carnegieendowment.org/>.

²⁴ Global Terrorism Database, accessed April 3, 2024, <https://www.start.umd.edu/gtd/>.

²⁵ Katherine Bucker, "On the Terrorist Attack at the Crocus City Hall in Moscow," *U.S. Department of State*, April 11, 2024, accessed May 21, 2024, <https://osce.usmission.gov/on-the-terrorist-attack-at-the-crocus-city-hall-in-moscow/>.

²⁶ The Global Economy, accessed May 21, 2024, <https://www.theglobaleconomy.com/>.

²⁷ Vision of Humanity, *Global Peace Index*, accessed May 21, 2024,

<https://www.visionofhumanity.org/maps/#/>.

²⁸ Freedom House, accessed May 21, 2024, <https://freedomhouse.org/>.

²⁹ In subjectively assessing the population's access to food as a measure of resistance, the following assumptions were made: If the country is on the CIA food insecurity list, the assessment is 75%, as food insecurity exists. If not, the measure is 25%, as the potential for food insecurity remains.

³⁰ Robert S. Burrell and John Collision, "A Guide for Measuring Resiliency and Resistance,"

Illustration by Authors.

³¹ The White House, *National Security Strategy*, October 2022.

³² For determining support to resistance as a foreseeable policy option, the following considerations were applied: If the regime is a strategic rival of a strong competitor, the probability is 100%. If the regime faces strong opposition from rivals, 75%. If the regime is not on good terms diplomatically with other states but is not a declared rival, 50%. If the regime maintains good terms with most states, 25%. If the regime is an ally of the United States, the assessment is 0%.

³³ For additional information on this methodology, see Chris Mason, "Measuring and Quantifying State Fragility: Why Governments Lose Internal Conflicts and What That Means for Counterinsurgency," in *Resilience and Resistance: Interdisciplinary Lessons in Competition, Deterrence, and Irregular Warfare*, ed. Robert S. Burrell (Tampa, FL: Joint Special Operations University Press, 2024).

³⁴ Vadim Volos, "Russian Opinion Poll in Wartime," *National Opinion Research Center*, University of Chicago, November 2023, accessed May 21, 2024,

<https://www.norc.org/research/projects/russian-public-opinion-wartime.html#:~:text=Additionally%20>, accessed on 21 May 2024.

³⁵ "Do You Approve of the Activities of Vladimir Putin as the President (Prime Minister) of Russia?"

Statista.

- ³⁶ “Do You Approve or Disapprove of Alexey Navalny’s Activity?,” *Statista*, March 2, 2022, accessed May 31, 2024, <https://www.statista.com/statistics/1109765/attitude-toward-activity-of-alexei-navalny-russia/>.
- ³⁷ Erica Chenoweth and Christopher Wiley Shay, “List of Campaigns in NAVCO 1.3,” *Harvard Dataverse*, 2020, accessed May 22, 2024, <https://dataverse.harvard.edu/dataverse/navco>.
- ³⁸ *Harvard Dataverse, Mass Mobilization Protest Data*, accessed May 22, 2024, <https://dataverse.harvard.edu/dataverse/MMdata>; *The Times* (London), “Foreign Ways,” October 18, 2005.
- ³⁹ *Carnegie Endowment for International Peace, Global Protest Tracker*, accessed May 22, 2024, <https://carnegieendowment.org/features/global-protest-tracker?lang=en>.
- ⁴⁰ Nonviolent and Violent Campaigns and Outcomes (NAVCO).
- ⁴¹ Tom Parfitt, “He Is Not Our Tsar, Anti-Putin Protesters Tell Russia,” *The Times*, May 7, 2018, 30.
- ⁴² Nonviolent and Violent Campaigns and Outcomes (NAVCO).
- ⁴³ Nonviolent and Violent Campaigns and Outcomes (NAVCO).
- ⁴⁴ Total numbers include 22,000 protestors against constitutional reforms in February 2022 and 100,000 protestors following the arrest of Aleksei Navalny in January 2021. See Carnegie Endowment for International Peace, *Global Protest Tracker*, accessed June 24, 2024, <https://carnegieendowment.org/features/global-protest-tracker?lang=en>.
- ⁴⁵ *Carnegie Endowment for International Peace, Global Protest Tracker*, accessed May 22, 2024, <https://carnegieendowment.org/features/global-protest-tracker?lang=en>.
- ⁴⁶ “Yabloko Congress Elects Leaders and Calls for Ceasefire,” *Alliance of Liberals and Democrats for Europe*, December 12, 2023, accessed May 23, 2024, https://www.aldeparty.eu/yabloko_congress_elects_leaders_and_calls_for_ceasefire.
- ⁴⁷ “Russia Dissolves Oldest Opposition Party,” *The Moscow Times*, May 25, 2023, accessed May 23, 2024, <https://www.themoscowtimes.com/2023/05/25/russia-dissolves-oldest-opposition-party-a81282>.
- ⁴⁸ Pjotr Sauer, “Putin Had Navalny Killed to Thwart Prisoner Swap, Allies Claim,” *The Guardian*, February 26, 2024, accessed May 23, 2024, <https://www.theguardian.com/world/2024/feb/26/vladimir-putin-had-alexei-navalny-killed-to-thwart-prisoner-swap-allies-claim>.
- ⁴⁹ *Harvard Dataverse, Mass Mobilization Protest Data*, accessed May 22, 2024, <https://dataverse.harvard.edu/dataverse/MMdata>; *The Times* (London), “Foreign Ways,” October 18, 2005.
- ⁵⁰ In 2021, communist candidate Mikhail Sergeyevich Lobanov lost an election in the Kuntsevo Constituency of Moscow to a United Russia candidate, Yevgeny Popov. Lobanov subsequently claimed election fraud.
- ⁵¹ Robyn Dixon, “Russia’s Rising Young Communists Pose an Unexpected New Threat to Putin’s Grip,” *The Washington Post*, October 6, 2021.
- ⁵² “Russian Activist Missing In Georgia May Be In Russian Custody,” *Radio Free Europe*, November 8, 2023, accessed May 22, 2024, <https://www.rferl.org/a/russia-georgia-artpodgotovka-missing/32676325.html>.
- ⁵³ “Greenpeace Challenges Gazprom: Prevents Oil Production at Prirazlomnaya Field, 2012,” *Global Nonviolent Action Database*, Swarthmore College, accessed May 22, 2024, <https://nvdatabase.swarthmore.edu>.
- ⁵⁴ *Uppsala Conflict Data Program*, Uppsala University, accessed May 24, 2024, <https://ucdp.uu.se/exploratory>.

⁵⁵ Ibid.

⁵⁶ Jason Burke, “Who Is Thought to Be Behind the Moscow Attack?,” *The Guardian*, March 23, 2024.

⁵⁷ Kevin Shalvey, “Russian Rebellion Timeline: How the Wagner Uprising Against Putin Unfolded and Where Prigozhin Is Now,” *ABC News*, July 10, 2023, accessed May 22, 2024, <https://abcnews.go.com/International/wagner-groups-rebellion-putin-unfolded/story?id=100373557>.

⁵⁸ Alisa Zemlyanskaya, “This Train Is on Fire: How Russian Partisans Set Fire to Military Registration and Enlistment Offices and Derail Trains,” *Europe Solidaire Sans Frontières*, July 6, 2022, accessed May 23, 2024,

<https://web.archive.org/web/20220810092620/https://theinsider.pro/politika/252389>.

⁵⁹ Jack Dutton, “Russian Anti-War Group Claims Responsibility for Train Crashes,” *Newsweek*, October 26, 2022, accessed May 23, 2024, <https://www.newsweek.com/russian-anti-war-group-claims-behind-explosions-stop-wagons-1754898>.

⁶⁰ Isabel van Brugen, “What Is ‘Black Bridge’? Anti-Putin Group Claiming FSB Building Fire,” *Newsweek*, March 21, 2023, accessed May 23, 2023, <https://www.newsweek.com/black-bridge-russia-fsb-building-fire-rostov-don-1789215>.

⁶¹ *Kyiv Post*, “‘Irpin Declaration’ on the Cooperation of the Russian Opposition Against Putin’s Regime,” September 1, 2022, accessed May 23, 2024, <https://www.kyivpost.com/post/5321>. David Axe, “Pro-Ukraine Russian Fighters Are Marching Deeper Into Russia but Taking Territory Isn’t the Goal: The Goal Is to Embarrass Vladimir Putin,” *Forbes*, March 17, 2024. Anna Kruglova, “The National Republican Army: A Potential Force of Resistance in Russia?,” *RUSI*, May 2, 2023, accessed May 22, 2024, <https://rusi.org/explore-our-research/publications/commentary/national-republican-army-potential-force-resistance-russia>. Jim Geraghty, “How Russians Are Joining the Fight Against Putin,” *The Washington Post*, March 22, 2024, accessed May 22, 2024, <https://www.washingtonpost.com/opinions/2024/03/22/freedom-russia-legion-ilya-ponomarev-putin-ukraine/>.

⁶² Katja Lindskov Jacobsen and Karen Philippa Larsen, “Wagner Group Flows: A Two-Fold Challenge to Liberal Intervention and Liberal Order,” *Politics and Governance* 12 (2024).

⁶³ “Russian Imperial Movement,” *Mapping Militants Project*, last updated 2023, accessed June 26, 2024, <https://mappingmilitants.org/profiles/russian-imperial-movement#narrative>. Michael R. Pompeo, “United States Designates Russian Imperial Movement and Leaders as Global Terrorists,” *U.S. Department of State Press Release*, April 7, 2024. Anna Kruglova, “For God, for Tsar and for the Nation: Authenticity in the Russian Imperial Movement’s Propaganda,” *Studies in Conflict & Terrorism* 47, no. 6 (October 19, 2021): 645–667.

⁶⁴ Federico Varese, et al. “The Resilience of the Russian Mafia: An Empirical Study.” *British Journal of Criminology*, vol. 61, no. 1, 2021, 143–166.

⁶⁵ Ben Makuch, “Russian Assassinations a Growing Worry as War Nears Second Year,” *Vice News*, February 9, 2023, accessed June 26, 2024, <https://www.vice.com/en/article/v7vwa9/russia-assassinations-putin-ukraine-war>.

⁶⁶ The figure illustrates significant Mexican resistance movements across a resistance continuum. The prominent nonviolent legal groups include political opposition parties: (1) Movimiento Ciudadano, (2) Partido Acción Nacional, and (3) Partido Revolucionario Institucional. Nonviolent illegal movements include (4) a well-organized women’s activist underground. Although violent rebellions (short-duration interruptions) are not currently apparent, insurgent groups include: (5) Cártel de Jalisco Nueva Generación, (6) Beltrán Leyva, (7) Cártel del Noreste and Los Zetas, (8)

Guerreros Unidos, (9) Cártel del Golfo, (10) Cártel de Juárez, (11) La Línea, (12) La Familia Michoacána, (13) Los Rojos, and (14) Cártel de Sinaloa.

⁶⁷ Jonathon Cosgrove and Erin Hahn, *Conceptual Typology of Resistance* (Fort Bragg, NC: U.S. Army Special Operations Command, circa 2018), 6.

⁶⁸ Katlijn Malfliet, “The Communist Party of the Russian Federation: Not Communist Per Se,” *Revue d'études comparatives Est-Ouest* 42, no. 1 (March 2011): 37–63.

⁶⁹ Matthew Bodner, “Russia’s 8 Most Memorable Davos Moments,” *The Moscow Times*, January 22, 2014, accessed May 23, 2024, <https://www.themoscowtimes.com/2014/01/22/russias-8-most-memorable-davos-moments-a31309>.

⁷⁰ Gennadii Andreevich et al., *My Russia: The Political Autobiography of Gennady Zyuganov* (Armonk, NY: M.E. Sharpe, 1997).

⁷¹ Ilya Budraitskis, “Russia Has a New Socialist Movement,” *Jacobin*, October 2, 2021, accessed May 23, 2024, <https://jacobin.com/2021/10/mikhail-lobanov-russia-communist-party-new-left-putin>.

⁷² “Putin Meets Russian Communist Party Leader Gennady Zyuganov,” *BBC Monitoring Former Soviet Union*, February 14, 2023.

⁷³ Gennady Zyuganov, “Political Report of the CPRF Central Committee to the 13th Party Congress,” November 29, 2008, accessed May 23, 2024, https://kprf.ru/party_live/61739.html.

⁷⁴ Malfliet, 5.

⁷⁵ Ekaterina Levintova, “Being the Opposition in Contemporary Russia: The Communist Party of the Russian Federation (KPRF) among Social-Democratic, Marxist–Leninist and Nationalist–Socialist Discourses,” *Party Politics* 18 (August 2011): 732.

⁷⁶ *Ibid.*, 739–740.

⁷⁷ A. G. Naronskaya, “Comparative Analysis of Regional Elite of The Communist Party and ‘Just Russia’: Social Characteristics and Channels of Recruitment,” *Sravnitel'naia Politika* 12, no. 2 (2021): 55–64.

⁷⁸ Jonathon Cosgrove and Erin Hahn, 14–15.

⁷⁹ Ivan Zhukovsky, “Zyuganov Agreed to the Unification of the Communist Party of the Russian Federation and A Just Russia. On One Condition,” *Gazeta.ru*, July 28, 2022, accessed May 31, 2024, <https://www.gazeta.ru/politics/2022/07/28/15192800.shtml>.

⁸⁰ Derek S. Hutcheson, “National Elections in Russia,” in *Routledge Handbook of Russian Politics and Society*, ed. Graeme Gill (London: Routledge, 2023), 111–26; Statista, “Turnout at the Presidential Election in Russia for June 1991 to March 2024,” accessed May 28, 2024, <https://www.statista.com/statistics/1456966/presidential-election-turnout-russia/>.

⁸¹ Irina Trotsuk and Marlia Subbotina, “Russians’ Ideas of Heroes and Heroism: Stable and Changing Components,” *RUDN Journal of Sociology* 23, no. 33 (2023): 525–45.

⁸² *Ibid.*, Table 6.

⁸³ *Ibid.*, 540–541.

⁸⁴ This includes Australia, Austria, Azerbaijan, Bahrain, Belarus, Belgium, Bolivia, Brazil, Canada, China, Croatia, Cuba, Cyprus, Czech Republic, Denmark, El Salvador, Finland, Georgia, Germany, Greece, Hungary, India, Iran, Iraq, Ireland, Italy, Kazakhstan, North Korea, Laos, Latvia, Lebanon, Luxembourg, Macedonia, Mexico, Netherlands, Norway, Pakistan, Palestine, Paraguay, Portugal, Russia, Serbia, South Africa, Spain, Sweden, Switzerland, Syria, Turkey, Ukraine, United Kingdom, Uruguay, United States, Venezuela, and Vietnam. See “The 23rd International Meeting of Communist and Workers Parties Kicks Off in Izmir, Turkey,” In Defense of Communism: The Marxist-Leninist Blog, October 20, 2023, accessed May 28, 2024,

<http://www.idcommunism.com/2023/10/the-23rd-international-meeting-of-communist-and-workers-parties-kicks-off-in-izmir-turkey.html>.

⁸⁵ Communist Party of the Russian Federation, “About Us,” accessed May 28, 2024, <https://cprf.ru/about-us/>.

⁸⁶ Ibid.

⁸⁷ Oleksiy Bondarenko, “Between Loyalty and Opposition: The Communist Party of Russia and the Growing Intra-Party Cleavage,” *Communist and Post-Communist Studies* 56, no. 4 (December 2023): 143–65.

⁸⁸ Ibid., 154.

⁸⁹ Ronald Deibert and Rafal Rohozinski, “Control and Subversion in Russian Cyberspace,” in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert et al. (Cambridge, MA: MIT Press, 2010), 19.

⁹⁰ Central Intelligence Agency, *The World Factbook*, accessed May 28, 2024, <https://www.cia.gov/the-world-factbook/countries/russia/>.

⁹¹ Elena Vartanova, “The Internet in the Structure of the Russian Media System,” in *Internet in Russia: A Study of the Runet and Its Impact on Social Life*, ed. Sergey Davydov et al. (Cham: Springer International Publishing AG, 2020), 25.

⁹² Elena Sherstoboeva, “Regulation of Online Freedom of Expression in Russia in the Context of the Council of Europe Standards,” in *Internet in Russia: A Study of the Runet and Its Impact on Social Life*, ed. Sergey Davydov et al. (Cham: Springer International Publishing AG, 2020), 93.

⁹³ Chiara Castro, “Russia VPNs: How to Stay Safer Online and Avoid Censorship,” *TechRadar*, January 23, 2024, accessed May 28, 2024, <https://www.techradar.com/vpn/vpn-in-russia>.

⁹⁴ Leo Chiu, “Russia Implements Ban on VPN Advertisement Ahead of Presidential Election,” *Kyiv Post*, March 4, 2024, accessed May 28, 2024, <https://www.kyivpost.com/post/28993>.

⁹⁵ Alicija Curanović, *The Sense of Mission in Russian Foreign Policy: Destined for Greatness!* (Abingdon, Oxon: Routledge, 2021).

⁹⁶ Jan Matti Dollbaum, “Social Policy on Social Media: How Opposition Actors Used Twitter and VKontakte to Oppose the Russian Pension Reform,” *Problems of Post-Communism* 68, no. 6 (2021): 509–20.

⁹⁷ Paul J. Tompkins Jr. and Robert R. Leonhard, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare* (Fort Bragg, NC: U.S. Army Special Operations Command, 2012), 10–12.

⁹⁸ Communist Party of the Russian Federation (CPRF), “About Us,” *Communist Party of the Russian Federation*, accessed May 29, 2024, <https://cprf.ru/about-us/>.

⁹⁹ Levada-Center, “Election Results,” *Levada-Center*, October 11, 2021, accessed May 29, 2024, <https://www.levada.ru/en/2021/10/11/election-results/>.

¹⁰⁰ Jan Matti Dollbaum, “Social Policy on Social Media: How Opposition Actors Used Twitter and VKontakte to Oppose the Russian Pension Reform,” *Problems of Post-Communism* 68, no. 6 (2021): 512.

¹⁰¹ “Russia’s Communist Party Leads Red Square Induction for Youth Movement,” *The Moscow Times*, May 20, 2024, <https://www.themoscowtimes.com/2024/05/20/moscow-claims-control-of-ukrainian-stronghold-in-luhansk-region-a85172>, accessed May 29, 2024.

¹⁰² Army Technical Publication 3-05.1: *Unconventional Warfare at the Combined Joint Special Operations Task Force Level* (Fort Bragg, NC: U.S. Army Special Operations Command, April 2021).

¹⁰³ Simon Pirani, “The Russian Statelets in the Donbas Are No ‘People’s Republics,” *Jacobin*, March 2, 2022, <https://jacobin.com/2022/03/donbas-donetsk-luhansk-ukraine-russia-putin>, accessed May 29, 2024.

¹⁰⁴ Leo Chiu, “Explained: Who Are Russia’s Allies? A List of Countries Supporting the Kremlin’s Invasion of Ukraine,” *Kyiv Post*, October 23, 2023, <https://www.kyivpost.com/post/13208>, accessed May 29, 2024.

¹⁰⁵ Monica Potts et al., “Two Years into the War, American Support for Ukraine Is Down,” *ABC News*, February 26, 2024, <https://abcnews.go.com/538/years-war-american-support-ukraine/story?id=107488095#>, accessed May 29, 2024.

¹⁰⁶ “Year Three of Russia’s Invasion of Ukraine May Be Zelenskiy’s Toughest yet; Political Pressure at Home, Splintering International Support and Prospect of Trump’s Re-Election Make for Existential Threats,” *The Guardian* (London), 2024.

Philosophy of the Individual and an American Theory of Special Operations

Adam T. Biggs, U.S. Naval Special Warfare Command, San Diego, California, USA

Lanny F. Littlejohn, U.S. Naval Special Warfare Command, San Diego, California, USA

ABSTRACT

Developing theoretical frameworks to foster critical thinking in Special Operations has been a persistent challenge, likely due to its diverse tasks requiring a unifying principle. The American theory of special operations describes its nature, value, and applications as a component of military power but lacks a defining ethos. This discussion proposes the “philosophy of the individual,” which builds on the idea that special operations forces cannot be mass-produced. It identifies four elements behind their success: 1) high-quality recruits, 2) training as an individual journey, 3) reliance on individual initiative, and 4) diversity fostering adaptability. Rooted in U.S. cultural strengths, this philosophy highlights why American special operations excel. Finally, the discussion evaluates the role of special operations theory and offers insights for its future development.

KEYWORDS

Special operations;
American theory;
ethos; innovation

Introduction

Special operations forces (SOF) demand special attention due to the unique challenges and requirements faced by the community. As such, many efforts focus on developing capabilities to support these operations, ranging from enhanced human performance programs to doctrine that underpins a complex cycle of training and redeployment. One question strikes at the heart of all efforts and doctrine to utilize special forces in support of national defense: what is the purpose of special operations? Ask three different people, and you may get at least four different answers in return. For example, Navy SEALs devote significantly more time to training for amphibious operations than Army Rangers or Marine Corps Raiders. Still, the question of purpose goes beyond a requisite list of mission capabilities. Purpose demands a strategic vision that bridges the operational realities of today with the future state of operations required to defend the nation.

CONTACT LCDR Adam T. Biggs | adam.t.biggs.mil@socom.mil

The views expressed in this article are solely those of the author(s) and do not necessarily reflect the views, policy, or position of the Department of the Navy, Department of Defense, or the U.S. Government.

© 2025 Arizona Board of Regents/Arizona State University

The American theory of special operations is a critical piece of this strategic vision¹. Its roots can be traced to warfare concepts such as relative superiority and Clausewitzian friction.² As originally conceived, the core content revolved around premises and principles guiding the success of American special operations. Each stated proposition within the American theory expounds upon a concept critical to ongoing operations, including ideas such as emphasizing the value of the human element in warfare and the reliance of special operations on combat support services. Several ideas similarly overlap with the five SOF truths.³ However, the theory has not been directly linked to, nor translated into, doctrine. Nor is it without flaws—with one major flaw apparent in its namesake. Namely, although it is called an American theory, there is nothing uniquely American about it. The likely inspiration stems from observations primarily drawn from United States special operations. Pragmatic observations may produce a simple list of connected training principles, yet a list lacks synthesis and identity, leaving the American theory unable to answer critical questions. Is the U.S. success unique? What makes this theory different from other positions? Are some elements more central to the theory than others?

The primary purpose here is to identify the ethos underlying an American theory of special operations. Applying a philosophical purpose to this theory will underscore its message and define it among competing theoretical stances on special operations. In particular, the argument will focus on the philosophy of the individual, a core tenet of U.S. special operations that has implicitly guided selection and training throughout its history. Such foundational ideas will provide support and character to the development of the American theory and further set it apart from peer competitors.

The discussion will begin with an overview of the premises stated within the American theory. Next, the core philosophy of the individual will be presented in contrast to the SOF truth from which it is derived—special operations forces cannot be mass-produced. This contribution will be compared with other theoretical positions on special operations, as well as a debate on the value of theoretical inquiry in the field. Taken together, the goal is to advance the development of an American theory of special operations by proposing a foundational principle for its strategic vision.

Special operations represent a critical component of the military infrastructure, especially as the focus on strategic competition with peer and near-peer adversaries increases and integrated deterrence becomes a prime goal of US military strategy. Many explorations have examined the contributions of training procedures or the historical accomplishments of various SOF units. By contrast, theoretical evaluation delves into the purpose of special operations forces. Although there will be a later discussion about the relative value of theory in special operations,⁴ an early and highly influential theory of special operations is the theory of relative superiority.⁵

According to relative superiority, SOF personnel achieve a decisive advantage despite numerical inferiority by reducing the frictions of war, which represent the disparity between the actual and ideal performance conditions in combat⁶. Chance and action interact to produce difficulties during conflict that may or may not be anticipated by military forces. With advanced training, specialized equipment, and small numbers, SOF personnel can reduce potential friction points to ensure higher-quality performance during missions. Other

scholars have similarly sought to extend Clausewitzian ideas into SOF-specific contexts.⁷ Still, McRaven's theory of relative superiority could be argued as the first, most fully formed, or at least the most influential theory describing the purpose of training and maintaining special operations personnel.

Recent discussions have attempted to expand upon the purpose and functions of special operations. Spulak⁸ and Kiras⁹ both explored the strategic contributions of SOF capabilities, which remain a critical consideration, but do not independently represent the type of theoretical contribution describing SOF functions as well as relative superiority. Another perspective builds upon foundations laid by McRaven's theory of relative superiority, as well as the philosophy of SOF truths and SOF imperatives that define successful operations. This American theory of special operations "explains the nature, uniqueness, value, and application of this instrument of military power and the tensions that are inherent to it".¹⁰ Its full review outlines 26 premises and 14 principles that provide an intellectual framework for debating the future evolution of special operations. These principles incorporate several ideas put forth in the theory of relative superiority, which is, in part, why an American theory of special operations should be seen as founded upon the ideas of Admiral William McRaven.

There is an inherently intriguing reason to develop an American-specific theory. Although specialized military personnel have existed throughout the history of warfare, American personnel have achieved monumental successes through special operations with historic implications, most notably Operation Neptune Spear.¹¹ The American concept has come to define what the world currently views as special operations. In turn, when developing a theory of special operations, it makes logical sense to explore the successes and occasional failures of the most successful organization. This approach likens theoretical explorations of special forces to developing theories of business and management, more so than the hypothesis-driven empirical sciences of chemistry or physics. Essentially, an American theory extracts factors common to success in special operations and interprets them as causal influences on operational success.

There is a logical flaw in this approach, however, as correlation does not equal causation. Despite the value in mining successful experiences of successful organizations for good behaviors and best practices, this approach describes what worked best in the past—not what will work in the future. There is some overlap between these concepts, yet the purpose of theoretical development for special operations has less to do with training successes today and more to do with anticipating future states that will ensure operational success tomorrow. Different theories provide contrasting ideas that enable critical thinking skills, thereby making the development and exploration of special operations theory essential for future operational success. Because the nature of special operations involves tackling emerging challenges and priorities, a retrospective-focused approach is insufficient without a more prospective integration of emerging challenges.

Another flaw is that the American theory largely describes a series of premises without truly synthesizing this information into an overarching concept. This method sometimes limits clarity because the premises overlap, if not they become fully redundant. For example, the first two premises state that "special operations represent a distinct military

capability of strategic value to national security” and “special operations have strategic utility”.¹² These two premises appear to describe the uniqueness of special operations and their utility within the military structure, respectively, but they are insufficiently distinguished from one another. Additional analysis and synthesis will be necessary to refine the principles.

To compare where the theory currently stands in terms of educational development, Bloom’s taxonomy describes various educational levels based on learning objectives.¹³ Earlier levels begin with knowledge and observation before progressing to synthesis and eventually creation. An American theory of special operations would currently be considered in the lower stages of this taxonomy, as the existing version lists a series of sometimes redundant premises with limited synthesis into a cohesive idea. Further synthesis would require aligning different premises within a suitable structure, such as connecting multiple premises to the first SOF truth: humans are more important than hardware. This delineation would emphasize the role of the human operator in special operations as a definitive dimension of the theoretical premises.¹⁴ Despite the value in pursuing an American theory, this type of development remains a necessary next step.

The primary purpose of the current discussion is to explore one foundational problem with the American theory that requires refinement—its ethos. It is difficult to describe why an American theory is different from other positions, or even why its namesake should permit it to be described as an American theory. Our intent is to provide an answer to why we need an American theory. Once we have a characterization of the theory that differentiates it from other positions, further refinement of the premises and principles in future work will be possible. So, what makes this idea an American theory of special operations, and is the theory unique to the U.S. and its society?

Special Operations Forces Cannot Be Mass Produced—Or Can They?

There is no more compelling set of guiding philosophical principles in special operations than the five SOF truths. These truths provide a concrete, concise, and easily repeatable framework underscoring the myriad complexities that distinguish special operations from general-purpose forces. However, four of these truths address general issues related to the success of special forces. Although each has internal validity and influences the development of an American theory, one core truth defines the ethos of this theory more than the others: special operations forces cannot be mass-produced.

But why not? The metaphorical comparison here is a pipeline. The volume of oil pumped from one end to the other depends on the length of the pipe and its diameter. These dimensions metaphorically represent the functional challenges in mass-producing competent special operations forces.

One possibility is the time investment required to produce special operations personnel. Any military force requires time to train and prepare its members for combat. Wars, most notably World War II, demonstrated that general-purpose military forces can be mass-produced. While the quality of the product may vary, the process itself is feasible. By comparison, special operations personnel require proficiency in a diverse set of specialized

mission responsibilities, making it necessary for fully capable SOF units to undergo years of training. Hastening this process would inevitably degrade their ultimate capability.

In this metaphor, the length of the training pipeline illustrates the time required for special operations training, which extends the process of moving someone from recruit to Sailor to SEAL. However, the length of the training pipeline does not inherently diminish force capacity if the proper investments are made early in the training cycle. The length of the pipe does not dictate its diameter, and length alone does not prohibit mass production. To build a better force, a longer pipeline is often required.

Pushing the metaphor further, transcontinental pipelines exist to supply vast continents with oil and natural gas. Similarly, twelve-year-old scotch takes, by definition, twelve years to age, yet it can still be mass-produced and found in stores worldwide. Thus, the timeline is not, in and of itself, a prohibitive factor in mass production—it is a limiting factor, certainly, but not an insurmountable one. So why can't special operations forces be mass-produced?

The first question of timeline leads naturally to a follow-up question about infrastructure. Mass production requires a robust investment in facilities and other resources. Special operations training demands significant material investments, including infrastructure to support explosive breaching, diving, and jump training under various conditions. Here, the diameter of the pipe in the metaphor represents the scope of resources required to support the process.

A larger pipeline capable of moving more material necessitates a more robust foundation. Returning to the transcontinental pipeline example, enormous amounts of material can be moved if the process is appropriately supported. The supporting elements, however, represent feats of engineering and logistical complexity that are daunting if starting from scratch. Yet logistical challenges, like timeline constraints, are not inherently prohibitive factors in mass production.

The American military-industrial complex, for instance, represents a similarly Herculean feat of funding and organization, and its existence proves that such investments are possible. Therefore, the mass production of special operations forces ultimately becomes a question of resource investment. While SOF personnel are limited by the quality of training and facilities available to them, with sufficient resources, a nation could theoretically establish programs to support robust special operations training. So, neither timeline nor infrastructure alone sufficiently answers the question: why can't special operations forces be mass-produced?

A more practical response might focus on the overall logistical burden. The complexity and scale of the required investment could render the process untenable or unsustainable as part of a national military strategy. This argument holds merit, yet for an American theory of special operations, it does not fully explain why American special operations adhere to the SOF truth that special operations forces cannot be mass-produced. Instead, a more philosophical argument underlies this truth and implicitly provides the ethos that differentiates the American theory from other special operations theories.

Philosophy of the Individual within an American Theory of Special Operations

Special operations cannot be mass-produced because there are individual elements inherent to the development of SOF personnel. The conceptual addition to an American theory of special operations can be described as the philosophy of the individual. This philosophy emphasizes several distinct components (see Table 1). Foremost, there must be quality in the initial product. Mass production is prohibited because there are insufficient materials to produce the desired end state of a trained special operator.

Next, the process of special operations development is an individual journey. Success or failure is a test of individual willpower that cannot be mass-produced, as every journey is different. Additionally, SOF personnel train as individuals first and then integrate and succeed as members of a team. The inherent contradiction between the individual process and the team mentality demands a level of individual investment for a selfless reward, which limits the pool of people who can succeed in these positions. Finally, the philosophy of the individual fosters diversity. Individual differences enable adaptability and the ability to overcome challenges in ways that best support relative superiority.

Since complex operational problems cannot be precisely forecasted before they arise, a diversity of approaches and perspectives within a team focused on a common goal allows for improvisation that ultimately leads to success. U.S. special operations have benefitted from a spirit that embraces this concept as part of national identity, uniquely situating U.S. forces to excel in special operations.

This combination—encapsulated in the philosophy of the individual—produces an ethos that distinguishes the American theory of special operations from its peers and fosters the desired operational effectiveness of special operations. Each aspect also contributes to the critical answer to why special operations forces cannot be mass-produced.

Philosophical Aspect	Why Mass Production Fails
Quality of Candidates	While infrastructure and timelines limit production, the true constraint is the availability of highly qualified candidates.
Training as an Individual Journey	Training outcomes vary based on personal effort and willpower, much like education. Mass production would dilute this individualized process.
Individual Initiative Drives Team Success	Effective teams rely on independent decision-making and selfless initiative—qualities that cannot be mass-produced.
Diversity Fuels Adaptability	A diverse pool of experiences fosters innovation and adaptability. Mass production enforces uniformity, reducing effectiveness in unpredictable scenarios.

Table 1. Key components of the philosophy of the individual and why Special Operations Forces cannot be mass-produced.

The first step in the philosophy of the individual involves the quality of raw materials. In the pipeline metaphor, the length and diameter of the pipeline say nothing about the product entering it. Even if such an infrastructure has logistical burdens that might limit its application, a robust pipeline is inherently unnecessary if there are not enough materials to move from one end to the other. Diamonds, for instance, could theoretically be mass-produced since carbon is plentiful, but the material produced by the process is relatively rare in comparison. Similarly, special operations training faces the challenge of sufficient raw materials, which prohibits mass production.

The most obvious example of this challenge involves physical fitness. Many individuals capable of military service lack the physical fitness requirements necessary to enter the special operations training pipeline. While this reality precludes mass production of special operations forces, it is actually a byproduct of a more critical component of the American theory. After all, there is a distinction between the physical fitness capabilities (potential) of the human body and the physical fitness capabilities (actual) of the individual.

The second aspect precluding mass production is the crux of the American theory: special operations development depends on the individual journey. Someone must desire to become an operator enough to engage in physical training that sufficiently prepares them for the special operations pipeline. This process creates a self-selection among individuals who may desire the prestige of operator status versus those who have the willpower to become operators.

However, as evidenced by the attrition rates in special operations training, physical fitness and desire alone are insufficient to produce SOF personnel. Willpower and grit are the critical differentiators. The training itself is a test of the mind more than a test of the body—that is, the flesh can endure the process, but will mental fortitude buckle under the pressure? This aspect precludes mass production because each journey is unique. Consider the process akin to education, albeit with an emphasis on special operations. Educational systems allow high performers and hard workers to rise through the ranks, but applying the same teaching methods to every student does not yield the same outcomes.¹⁵ Education cannot be forced. It is the product of individual learning and volitional effort, rather than mass production. Even if many people receive an education from the same institution, individual education is always unique.

Special operators train in much the same way, where the result depends on individual initiative rather than mass production. Every moment of Hell Week in Basic Underwater Demolition and SEAL training (BUD/S) adds to the physical burden placed on the individual. However, the body can endure the training—a robust cadre of special operations medical personnel carefully observes and supports the process to ensure survivability. Instead, the challenge lies in individual willpower. No one else can do it for you. All candidates face the little voices telling them to quit, to go home, to take the easy route. The answers to these little voices cannot be mass-produced because the individual experience leading up to that point is different for every candidate.

This individual demonstration of willpower differentiates those who become SEALs from those who drop out. More importantly, the individual process and experience form the

core—and the most crucial component—of the training pipeline. If an individual has the willpower to endure this experience, they have the willpower to become an operator. Late-night runs, freezing swims, and extreme exhaustion are merely tools to challenge the mind's will. As such, special operations forces cannot be mass-produced because it is the individual reaction that matters. Experience and process can be mass-produced, much like any roller coaster experience, but an American theory of special operations emphasizes that the individual experience inherent to special operations training is what ultimately determines operational success.

The third aspect of this philosophy of the individual highlights how the process can succeed or fail due to either selflessness or hubris. Admiral William S. McRaven, then commander of USSOCOM, summarized the nature of this selflessness in a commencement speech where he described the value of making your bed every day.¹⁶ Recalling his training anecdotes, Admiral McRaven spoke about a night spent in the mudflats between San Diego and Tijuana after his training class committed some “egregious” training infraction. The mud swallowed each man until only their heads bobbed above the surface. The instructors offered everyone a way out: the group could leave if only five men would quit, ring the bell, and leave SEAL training.

Several individuals wavered as they weighed the prospect of eight more hours in bone-chilling cold against the comfort of the easy path. Then, one voice began to sing. Another followed, and then another, and another. Admiral McRaven recalled how the mud began to seem a little warmer, and the dawn no longer felt so far away. This moment encapsulates the duality of special operations training. Individual willpower determines whether one becomes an operator, but the success of special operations depends on the team. No individual is as strong as the team. As Kipling aptly wrote: “For the strength of the pack is the wolf, and the strength of the wolf is the pack.”

Within an American theory of special operations, and according to the philosophy of the individual, success depends on individual initiative working within a team. In the mudflats example, individual initiative promoted team success. Every individual had the same experience while shivering in the mud, but one man decided to start singing. No one told him to sing. Loud, off-tune renditions of popular songs might seem like yet another environmental hazard in an already challenging situation. Even so, one person recognized the moment and chose to innovate—undertaking an action that would enable mission success.

The team succeeded because of this individual initiative. This person received no special accolades for the action but did it because team success mattered more than personal glory. An individual focus accepts that personal success is not always possible, yet individual initiative and sacrifice can drive team success. Would the same act have carried the same value if the class had been instructed to sing? Likely not. This selflessness is integral to success in special operations. Within the philosophy of the individual, success arises from the seeming contradiction of team success driven by individual initiative and selfless action.

Failure is also explained within this philosophy. A focus on the individual can lead to substantial hubris when this egocentric approach is not tempered by selfless attributes. A trained special operator may have succeeded where others failed, but when this accomplishment is pursued for personal glory, the result is entitlement. Entitled individuals seeking personal accolades create toxic environments. Conversely, individual achievement and initiative focused on team success foster a collaborative environment where the whole becomes greater than the sum of its parts—where team capabilities surpass the capabilities of any individual operator.

The fifth SOF truth—most special operations require non-SOF support—acknowledges the broader contributions of the team. An individual operator may possess incredible skills and qualifications, but personal success ultimately depends on team support. The potential failure carried by the philosophy of the individual is the toxic environment that arises when individual success takes precedence over team success. Both scenarios require individual initiative, yet one focuses on personal recognition, while the other centers on collective achievement. Admiral Wyman Howard, as Commander of Naval Special Warfare Command, best summarized the double-edged philosophy of the individual with the motto he signed at the end of every message: *“The deed is all—not the glory.”*

This combination of individual initiative and selfless focus on team success further precludes mass production. A suitably contradictory attitude for special operations under an American theory cannot exist among the masses. Moreover, achieving the status of a special operator does not inherently confer such an attitude upon the servicemember. Developing and fostering a culture that embraces this mindset is a focus on the individual, expressed through action, not something mass-produced through policy.

The fourth and final aspect of the philosophy of the individual explains why the American theory achieves such success in special operations: diversity. Specifically, mass production creates a uniform product, where one soup can is intended to be identical to the next, or the oil coming down the pipeline today is the same as the oil tomorrow. While this process creates volume, it also creates vulnerability. Enemies can anticipate and adapt to operational capabilities because they know in advance what they will encounter. Lateral thinking becomes a tool by which enemies can exploit the predictability of mass production.¹⁷ Relative superiority demonstrates this principle: a numerically inferior force can achieve disproportionate results by applying relative strength at the optimal point of vulnerability.¹⁸ Mass production creates organizational vulnerabilities in universal tactics and training—vulnerabilities that special operations are designed to exploit, not emulate.

Moreover, a powerful yet uniform force undermines the nature and function of special operations. There is a philosophical debate about whether mass production contradicts the very definition of special operations and instead represents a shift in the training capabilities of general-purpose forces. For instance, modern infantry may well exceed the definition of special operations forces as understood during the World War II era. Instead, the philosophy of the individual posits that valuing the individual as the fundamental unit inherently promotes diversity within the force. Emphasizing the individual journey during training produces varied experiences among those who succeed. These individual skills can then be tailored to mission responsibilities for optimal advantage. Furthermore, diversity

inherently fosters adaptability. Special operations will always face missions with emerging challenges that demand the ability to adapt and overcome. If a mass-production pipeline creates a mass-produced product with similar thinking patterns, it follows that responses to new situations will also be similar.

The result is that ten thousand people reach the same conclusion. Logistically, such uniform thought simplifies managing a large organization, but it also leads to innovative stagnation—the inability to adapt and overcome novel encounters—which is self-defeating in a special operations environment. Different perspectives generate different options, enabling a more holistic understanding of situations and a more complete evaluation of operational possibilities. Diversity drives innovation, and the ability to create new solutions for unexpected circumstances is a key factor in the success of special operations. An American theory of special operations embraces success through diversity by focusing on the experiences and capabilities of individuals rather than the mass-production capabilities of the training pipeline.

How U.S. Culture Enabled the American Theory of Special Operations

Other theories exist to describe the nature of special operations. Each position offers a unique perspective on the value or role of SOF personnel, such as the importance of relative superiority¹⁹ or the strategic applications of SOF capabilities²⁰. Although the relative merits of these different positions could be discussed in turn, the purpose of creating a unique theory is to capture something fundamentally different about its tenets. These ideas have, over time, evolved into something entirely new. For an American theory of special operations, the philosophy of the individual provides a distinctive ethos that sets it apart from competing perspectives. This philosophy adds depth and distinction to the theory, but it does not fully explain its namesake. So, what makes this position an “American” theory?

A straightforward interpretation, based on the original monograph²¹ suggests that the theory is named “American” because its evidence comes primarily from U.S. special operations. In this sense, the name reflects its nation of origin, much as a historian might describe a “Hellenistic theory” of phalanx formation rather than a “Roman theory.” We propose a different interpretation for the naming. The evidence may primarily derive from American sources not by coincidence, but because American culture aligns exceptionally well with the philosophy of the individual. This perspective suggests a unique origin for the name while also attributing the success of American special operations, in part, to the cultural and societal characteristics of the United States.

To understand this position, one must first recognize what makes the U.S. distinct from many other nations. Perhaps the most obvious link is the diversity of the American population, which directly ties into the diversity aspect of the philosophy of the individual. Few cultures involve such a wide array of people with different ethnic, religious, and social backgrounds. Even the American landscape is marked by a diverse array of terrains. Diversity is a core strength of the American experience. If diversity fuels adaptability, then the blending of perspectives and cultures inherent to the American experience generates an array of approaches to problem-solving that are nearly impossible to anticipate.

Operationally, this dynamic allows American operators to adapt to various viewpoints based on their interactions, making them inherently suited to novel conditions. This evolutionary “natural selection” of ideas, perspectives, and frameworks fosters a progressive refinement in operational power. Theoretically, this concept suggests that American operators embrace adaptive expertise over procedural expertise during training.²² Adaptive expertise enables individuals to excel in both expected and unexpected conditions, while procedural expertise allows strong performance only within familiar or practiced conditions. Diversity underpins adaptation, and adaptive skill is arguably the most critical component of expertise.

This adaptability also carries an inherent tactical advantage: it is difficult to disrupt performance when operators can excel even as circumstances change. Disrupting a procedural expert is often a straightforward application of relative superiority, but disrupting adaptive experts poses a much greater challenge, especially when special operations personnel face true peer competitors—other special operations forces. Another point emphasizing the uniqueness of the American theory is that the U.S. is built primarily upon a spirit, rather than blood or soil. Unlike many nations whose identities are shaped by lineage or conquest, America’s identity revolves around an ideal—a belief in crossing oceans in pursuit of a better life. This ethos reflects individual initiative aimed at producing team success.

Despite the challenges of building a society composed of native-born citizens and immigrants from around the globe, the benefits to special operations are profound. Immigrants often carry a spirit of adventure and a willingness to seek change to improve their lives. This drive distills into the essence of the American spirit, which transcends being born in California or Texas. Moreover, the American Dream emphasizes upward mobility, offering abundant opportunities for prosperity and success.²³ There is no entrenched class system dictating an individual’s social responsibilities. Instead, there is a pervasive belief that anyone can achieve anything through effort—and perhaps a bit of luck. These ideas align with the individual journey and opportunity central to the American experience.

An American theory of special operations embraces this individual journey to overcome adversity as a defining feature of its training philosophy. The combination of these cultural characteristics suggests that U.S. society is uniquely positioned to produce special operators who excel through adaptability and individual initiative.

This view offers a compelling, if optimistic, explanation for why American special operations have garnered such success and earned their reputation for combat prowess. However, the same cultural traits that have fostered this success also present risks. Failures in special operations training parallel some broader issues within American society. Individual initiative pursued for personal glory, rather than self-sacrifice, can lead to the kind of hubris often displayed across social media platforms. Such selfishness can fuel a cycle of toxicity and entitlement that undermines both special operations and the culture at large. The same cultural idioms that create an environment ripe for success could also serve as a blueprint for its potential downfall.

Future Development for an American Theory of Special Operations

Although the current discussion has focused on proposing ideas that establish an ethos underlying an American theory of special operations, it is important to emphasize that these ideas are intended to move the theory forward—they do not represent an endpoint. Special operations theory requires substantial additional exploration, and the American theory of special operations is merely one avenue for future consideration. Several critical considerations arise when addressing theoretical questions about special operations.

The foremost concern is the value of the theory itself. A debate exists regarding whether there should be an overarching theory of special operations or even a subset of theoretical emphasis.²⁴ One position argues that “an emergent theory of special operations, or SOF power, particularly one sponsored by the special operations community, is an indicator of an expansion of bureaucratic confidence and political influence”.²⁵ The idea is that, if unchecked, special operations theories could risk promulgating myths or hyperbole, taking on political or conspiratorial tones. Applying the descriptive label of “theory” to something based solely on logical deduction risks elevating its perceived validity beyond its actual value. This critique highlights a potential pitfall in developing theoretical positions without sufficient empirical evidence.

Another challenge in developing theory is that special operations theory may be inherently self-limiting, or even self-defeating, given that special operations must remain at the cutting edge of warfare. Theory development builds on existing evidence and concepts, meaning that any current theory risks becoming outdated as new ideas and innovations emerge. Special operations theory could be considered analogous to the uncertainty principle: it is difficult to know the exact nature of a current capability and its future trajectory.²⁶ The more precisely one examines current special operations capabilities, the more difficult it becomes to predict future trends, and vice versa. This analogy suggests that narrowly focusing on the present risks obscuring broader trends, while a more generalized approach may dilute the specificity needed to address the unique challenges of special operations.

However, there are counterpoints to these concerns. First is the issue of feasibility. Developing a theory of special operations is inherently complex, as the field encompasses a wide range of activities. Attempting to create one overarching theory of special operations is akin to creating a unified theory of psychology. Just as psychology includes multiple theories addressing specific topics—such as social learning²⁷ or moral development²⁸—special operations theory should approach the field through focused, topic-specific frameworks. Individual theories might address areas such as training, selection, or operational methodologies, differentiating special operations from general military practices.

Second, theoretical debate in special operations serves an important purpose: fostering critical thinking within the field. Some knowledge is developed intuitively through individual experience, but such insights are often difficult to convey to others as more than anecdotal stories. The challenge lies in ensuring that the listener can extract the same value and meaning from these stories as the person who experienced them. By contrast, an

instructor presenting a structured theory and illustrating it with a story allows students to gain a deeper understanding of the situation and apply that knowledge to future scenarios. In this sense, a “theory” provides a formal framework for organizing and communicating knowledge, making it more accessible and actionable. Developing theoretical postulates for special operations is thus an exercise in translating intuition into structured, teachable concepts. While this process carries risks, it offers significant value when the resulting theory is aimed at enhancing critical thinking around topics relevant to special operations.

These considerations underscore the challenges and opportunities of theoretical development in special operations. For an American theory of special operations, each of these points provides meaningful guidance. While speculative ideas should be approached with caution to avoid promoting myths, the primary purpose of an American theory should be to stimulate critical thinking on issues central to special operations. Such theories need not address every aspect of the field or apply universally across all missions and time periods. Instead, targeted theories focusing on specific aspects—such as the factors behind American special operations’ successes or the unique traits distinguishing U.S. SOF from other forces—can encourage creative thinking with practical implications for recruiting, selection, and training. The current discussion aims to enhance the American theory by providing it with a defining ethos. Further development could refine its premises or expand on the principles of McRaven’s theory of relative superiority. At its core, an American theory of special operations should highlight attributes unique to or heavily influenced by U.S. history and culture. Developing such a theory based on historical evidence from American special operations is just one of many potential approaches.

One intriguing area for future research is exploring whether there is something unique about U.S. culture that predisposes individuals to success in special operations. A potential avenue is examining how this cultural influence shapes the SOF mindset. As Johnsen and Christensen describe, “the term ‘SOF mindset’ has become a catchall term that encapsulates current enthusiasm and the notion that SOF has special qualities in terms of adaptability, risk tolerance, and dedication to mission success.”²⁹ Some individuals may enter training with a mindset conducive to success, while others develop it through training. The connection between cultural predisposition and individual mindset requires further scrutiny, considering both positive and negative implications—such as being goal-oriented but potentially resistant to authority.³⁰ While the SOF mindset is not unique to U.S. special operations, future research could examine whether U.S. culture predisposes individuals to this mindset, whether it is cultivated during training, or if success arises from a combination of the two. Investigating the SOF mindset represents a significant opportunity for further research, with implications for the philosophy of the individual and broader social science applications to special operations.³¹

Summary

Special operations occupy a distinctive and critical role in U.S. military operations. Their unique characteristics introduce equally unique challenges in fostering the critical thinking needed to support these activities. The American theory of special operations offers one framework to encourage creative thinking in the field. Although this idea builds on McRaven's theory of relative superiority, it requires significant further development. This discussion proposed an ethos underlying the American theory—the philosophy of the individual—which identifies key factors contributing to its uniqueness: 1) the quality of individuals entering the training pipeline, 2) the training process as an individual journey, 3) the interplay between individual initiative and team success, and 4) the value of diversity. Together, these elements explain the successes of U.S. special operations while drawing on American history and culture to support the theory. Each aspect reinforces why this framework should be called an American theory of special operations. Ultimately, any special operations theory should aim to enhance critical thinking within the field, thereby improving future operational performance.

Endnotes

- ¹ Harry Yarger, *21st Century SOF: Toward an American Theory of Special Operations* (MacDill Air Force Base, FL: Joint Special Operations University, 2013).
- ² W. H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (Novato, CA: Presidio Press, 1996). Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, [1832] 1984).
- ³ J. M. Collins, *U.S. and Soviet Special Operations*, House Armed Services Committee (Congressional Research Service, Library of Congress: Washington, D.C., 1986). United States Special Operations Command, "SOF Truths," accessed July 13, 2021, <https://www.socom.mil/about/sof-truths>
- ⁴ James D. Kiras, "The Dangers of Theory," in *Special Operations Research: Out of the Shadows*, ed. Christopher Marsh, James D. Kiras, and Patricia J. Blocksome (Boulder, CO: Lynne Rienner Publishers, 2020), 11–26. Christopher Marsh, Matthew Kenny, and Nicholas Joslyn, "SO What? The Value of Scientific Inquiry and Theory Building in Special Operations Research," *Special Operations Journal* 1, no. 2 (2020): 89–104.
- ⁵ W. H. McRaven, "Commencement Speech," speech given at the University of Texas, May 17, 2014.
- ⁶ von Clausewitz, *On War*, 1984.
- ⁷ James D. Kiras, "A Theory of Special Operations: 'These Ideas Are Dangerous,'" *Special Operations Journal* 1, no. 2 (2015): 75–88. G. S. Lauer, "Broken Windows: Special Operations and Clausewitz—Theory, Politics, and State Military Violence in the Limited Wars of the Twenty-First Century," *Special Operations Journal* 5, no. 2 (2019): 103–110. R. Lillbacka, "Parameters of Simplicity as a Principle of Special Operations," *Special Operations Journal* 3, no. 2 (2017): 94–110.
- ⁸ R. G. Spulak Jr., *A Theory of Special Operations* (MacDill Air Force Base, FL: Joint Special Operations University, 2007).
- ⁹ James D. Kiras, *Special Operations and Strategy: From World War II to the War on Terrorism* (New York: Routledge, 2006).
- ¹⁰ Yarger, 21st Century SOF.
- ¹¹ Mark Bowden, *The Finish: The Killing of Osama bin Laden* (New York: Atlantic Monthly Press, 2012).
- ¹² Yarger, 21st Century SOF.
- ¹³ Benjamin S. Bloom et al., *Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain* (New York: David McKay Company, 1956). David R. Krathwohl, "A Revision of Bloom's Taxonomy: An Overview," *Theory into Practice* 41, no. 4 (2002): 212–218.
- ¹⁴ Alan Biggs and Robin Lee, "The Role of the Human Operator in the Third Offset Strategy," *Naval War College Review* 71, no. 3 (2018): 96–120. Kristian L. Parker, "Locating the Human in Doctrine," *Special Operations Journal* 3, no. 2 (2017): 88–93.
- ¹⁵ P. F. Cuthbert, "The Student Learning Process: Learning Styles or Learning Approaches?," *Teaching in Higher Education* 10, no. 2 (2005): 235–249. Anthony F. Grasha, "A Matter of Style: The Teacher as Expert, Formal Authority, Personal Model, Facilitator, and Delegator," *College Teaching* 42, no. 4 (1994): 142–149. Anthony F. Grasha and Natalia Yangarber-Hicks, "Integrating Teaching Styles and Learning Styles with Instructional Technology," *College Teaching* 48, no. 1 (2000): 2–10. Frédéric Guay, Catherine F. Ratelle, and Julien Chanal, "Optimal Learning in Optimal

Contexts: The Role of Self-Determination in Education,” *Canadian Psychology/Psychologie canadienne* 49, no. 3 (2008): 233.

¹⁶ W. H. McRaven, "Commencement Speech," speech given at the University of Texas, May 17, 2014.

¹⁷ Edward de Bono, *Six Thinking Hats* (Boston: Little, Brown, 1985); Edward de Bono and Eric Zimbalist, *Lateral Thinking* (London: Penguin, 1970); Nicole Dobson-Keefe and Warren Coaker, "Thinking More Rationally: Cognitive Biases and the Joint Military Appreciation Process," *Australian Defence Force Journal* no. 197 (2015): 5–16.

¹⁸ McRaven, *Spec Ops*.

¹⁹ McRaven, *Spec Ops*.

²⁰ Robert G. Spulak Jr., *A Theory of Special Operations* (MacDill Air Force Base, FL: Joint Special Operations University, 2007).

²¹ Yarger, 21st Century SOF.

²² Arthur J. Baroody, "The Development of Adaptive Expertise and Flexibility: The Integration of Conceptual and Procedural Knowledge," in *The Development of Arithmetic Concepts and Skills: Constructing Adaptive Expertise Studies*, ed. Arthur J. Baroody and Ann Dowker (Mahwah, NJ: Lawrence Erlbaum Associates, 2003), 1–44; Patrick Ward, Jonathan Gore, Ryan Hutton, Garry E. Conway, and Robert R. Hoffman, "Adaptive Skill as the *Conditio Sine Qua Non* of Expertise," *Journal of Applied Research in Memory and Cognition* 7, no. 1 (2018): 35–50.

²³ James Truslow Adams, *The Epic of America* (Boston: Little, Brown, and Company, 1931); Jim Cullen, *The American Dream: A Short History of an Idea That Shaped a Nation* (New York: Oxford University Press, 2004); Robert D. Putnam, *Our Kids: The American Dream in Crisis* (New York: Simon and Schuster, 2015).

²⁴ James D. Kiras, "A Theory of Special Operations: 'These Ideas Are Dangerous,'" *Special Operations Journal* 1, no. 2 (2015): 75–88; Christopher Marsh, Matthew Kenny, and Nicholas Joslyn, "The Value of Theory," in *Special Operations Research: Out of the Shadows*, ed. Christopher Marsh, James D. Kiras, and Patricia J. Blocksome (Boulder, CO: Lynne Rienner Publishers, 2015), 27–46; Christopher Marsh, James Kiras, and Patricia Blocksome, "Special Operations Research: Out of the Shadows," *Special Operations Journal* 1 (2015): 1–6; Christopher Marsh, James D. Kiras, and Patricia J. Blocksome, eds., *Special Operations: Out of the Shadows* (Boulder, CO: Lynne Rienner Publishers, 2020).

²⁵ James Kiras, "The Dangers of Theory," in *Special Operations Research: Out of the Shadows*, ed. Christopher Marsh, James D. Kiras, and Patricia J. Blocksome (Boulder, CO: Lynne Rienner Publishers, 2020), 11–26.

²⁶ Werner Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik" [About the Graphic Content of Quantum Theoretic Kinematics and Mechanics], *Zeitschrift für Physik* 43 (1927): 172–198; Masanao Ozawa, "Position Measuring Interactions and the Heisenberg Uncertainty Principle," *Physics Letters A* 299, no. 1 (2002): 1–7; Masanao Ozawa, "Universally Valid Reformulation of the Heisenberg Uncertainty Principle on Noise and Disturbance in Measurement," *Physical Review A* 67, no. 4 (2003): 042105.

²⁷ Albert Bandura and Richard H. Walters, *Social Learning Theory*, vol. 1 (Englewood Cliffs, NJ: Prentice Hall, 1977).

²⁸ Jeremy I. M. Carpendale, "Kohlberg and Piaget on Stages and Moral Reasoning," *Developmental Review* 20, no. 2 (2000): 181–205. Lawrence Kohlberg and Richard H. Hersch, "Moral Development: A Review of the Theory," *Theory into Practice* 16, no. 2 (1977): 53–59. Jean Piaget, "Piaget's Theory," in *Piaget and His School*, ed. A. Scharmann, 11–23 (Berlin: Springer, 1976).

²⁹ Aksel Johnsen and Geir Christensen, “Clarifying the Antisystemic Elements of Special Operations: A Conceptual Inquiry,” *Special Operations Journal* 2 (2016): 106–123.

³⁰ Annette Dalgaard-Nielsen and Kristoffer F. Holm, “Supersoldiers or Rulebreakers? Unpacking the Mind-Set of Special Operations Forces,” *Armed Forces & Society* 45, no. 4 (2019): 591–611.

³¹ Eyal Ben-Ari, John G. Turnley, and Kobi Michael, “A Social Scientific Agenda for the Study of Special Operations Forces,” in *Special Operations Forces in the 21st Century*, ed. Jessica Glicken Turnley et al. (London: Routledge, 2017), 285–301.

A Framework for Cyber Foreign Internal Defense

James Robert Oxford, Department of Defense, Washington, D.C., USA

ABSTRACT

U.S. Special Operations Command (USSOCOM) seeks to better understand the intersection of special operations and cyber. This research focuses on foreign internal defense (FID)—a core function of Special Operations Forces (SOF)—by proposing a novel cyber-FID framework. SOF employs FID to protect U.S. interests in foreign competition and conflict environments, not through resource-intensive military force but by defending forward, equipping allied forces to counter emerging threats. Establishing a cyber-FID framework enhances USSOCOM’s understanding of how FID integrates with cyber operations, providing a structured approach for planning and training. This article first examines the need for a cyber-FID framework, then reviews traditional FID, and finally introduces a cyber-FID model aligned with the three core categories of FID: indirect support, direct support, and U.S. combat operations. It concludes with recommendations for future research.

KEYWORDS

Cyber-FID; U.S. Special Operations Command; cyber warfare; security cooperations; gray zone conflict

Introduction

U.S. Special Operations Command (USSOCOM) seeks to understand the relationship between special operations and the cyber domain. This research narrows the focus to a single Special Operations Forces (SOF) core function—foreign internal defense (FID)—by proposing a novel framework for cyber-FID. According to the Joint Staff’s Joint Publication (JP) 3-05, *Special Operations*, “FID refers to U.S. activities that support a host nation’s (HN) internal defense and development (IDAD) strategy and program, designed to protect against subversion, lawlessness, insurgency, terrorism, and other threats to its security and stability.”¹

CONTACT James Robert Oxford | jamesroxford@gmail.com

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense

© 2025 Arizona Board of Regents/Arizona State University

Importantly, SOF employs FID to protect U.S. interests in foreign competition and conflict environments—not through resource-intensive military force, but by defending forward to equip allied forces to address these threats. Furthermore, over the past few years, the U.S. government has engaged in cyber capacity-building efforts with many foreign partners and allies, yet the Department of Defense (DoD) lacks a formal structure to guide these initiatives. Creating a cyber-FID framework will enhance USSOCOM's understanding of this core function's relationship with cyber, contributing to the “operational art” of FID in shaping operations and providing a structure that can be integrated into planning and training activities.²

This article first explores the need for a cyber-FID framework and highlights the importance of defining one now within the current geopolitical environment. It then provides a brief overview of traditional FID and examines the effectiveness of cyber-FID in countering state-on-state cyber threats. Finally, the article proposes a cyber-FID framework aligned with the three categories of traditional FID: indirect support, direct support (excluding combat operations), and U.S. combat operations. The article concludes with final thoughts on future research.

Problem Statement

Colonel Patrick Duggan (USA), a career Special Forces officer with cyber expertise, emphasized the importance of this topic in a 2015 *Joint Force Quarterly* article, stating, “Today’s global environment impels the United States to adopt cyber-enabled special warfare as a strategic tool of national military strategy.”³ Colonel (Ret.) Duggan argues that Iran and Russia surpass the U.S. in the strategic use of cyber-enabled special warfare. He presents three concepts of operation (CONOPs) for closing this gap, including one for cyber-FID. Despite a handful of references to the cyber-FID concept, the current literature offers no clear description of what cyber-FID should or could entail. In fact, the nearly 200-page *Joint Publication 3-22, Foreign Internal Defense*, mentions the term *cyber* only three times.⁴ Since FID is a core activity of special operations and cyber is a critical warfighting domain, USSOCOM needs a cyber-FID framework.⁵

Working with partners and allies is imperative to achieving U.S. and partner interests and is emphasized in many official government documents, including the National Security, Defense, and Military Strategies. This article is not the first to suggest that these efforts should extend into the cyber domain. In 2019, William Smith of the U.S. Marine Corps Communications and Information Systems Division proposed the creation of Cyber Engagement Teams (CETs) to “expand on current Foreign Internal Defense (FID), Security Force Assistance (SFA), or other cooperation and engagement apparatuses.” He explained that “working ‘by, with, and through’ friendly nations, [and by developing] lasting relationships, CETs are a logical tool to contend with cyber adversaries through friendly engagement, collective security, and partnering.”⁶ To better align these concepts, Smith’s CET construct would benefit from a cyber-FID framework.

Before introducing the cyber-FID framework, this article will set the stage by outlining key concepts of traditional FID. First, two critical questions arise and merit discussion: Why create a cyber-FID framework? And why now?

The Need for a Cyber-FID Framework

“Foreign internal defense capability sets must increase capacity-building efforts in areas such as cyber.”⁷ — *James M. DePolo, Former Director of Special Operations, U.S. Army Special Warfare Center*

USSOCOM needs a cyber-FID framework for three reasons. First, a cyber-FID framework will outline a consistent approach to cyber-FID, ensuring continuity across theaters of operation and creating a foundation for advancing cyber-FID theory and best practices. The framework will be flexible enough to adapt to specific partner needs while remaining structured enough to provide a common operating concept that operational and tactical teams can use as a starting point.

Second, publishing a cyber-FID framework will reassure allies and partners of the U.S. commitment to global cyber resiliency and contribute to the layered cyber deterrence advocated in the *Cyberspace Solarium Commission* report.⁸ Smith notes that it will:

signal to adversaries the close ties between the U.S. and a friendly nation... working continually ‘by, with, and through’ our allies and partners would establish and maintain the necessary habitual relationship required for continued shaping and posturing of the environment, provide a level of deterrence, and may even prevent open conflict between adversaries.⁹

The *2014 Quadrennial Defense Review*’s executive summary stated, “Building security globally not only assures allies and partners and builds partner capacity but also helps protect the homeland by deterring conflict and increasing stability.”¹⁰ This connection between FID and deterrence is also relevant in the cyber domain.

Lastly, defining a cyber-FID framework will communicate the importance of these efforts in addressing the changing character of war and enrich the public conversation on conflict in the *gray zone*—a term often used to describe “competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality.”¹¹ Most cyber operations fall within this category. In the *2016 USSOCOM White Paper* from which this definition is drawn, the author briefly explores the opportunity for a new lexicon, suggesting that it would “help us understand and engage challenges in the gray zone better... [and] help yield better decisions.”¹² The cyber-FID framework presented in this article takes a step in that direction.

The Time for Cyber-FID Is Now

“Adapt Now, or Lose Later”¹³ — *General Mark A. Milley, Chairman of the Joint Chiefs of Staff*

It is helpful to consider an analogy to aviation FID. In his Spring 1997 *Airpower Journal* article, “Whither Aviation Foreign Internal Defense?” Wray Johnson wrote, “It is the identification of links between the past and present which enables us to comprehend our actions in context. In that light, the concept of aviation-centered FID is not original: it is a response to the void created in SOF FID capabilities following the Vietnam War.”¹⁴ Johnson traces the history of aviation FID from its origins in “rudimentary

counterinsurgency (COIN) doctrine” after the Second World War to its role in addressing the “low-intensity conflict” of post-Vietnam Central America, and ultimately to its formalization in *Air Force Operational Doctrine* in 1992. He makes the following salient point:

Although the Air Force nominally continued to perform the FID mission after Vietnam, it was as an adjunct to its conventional mission and was accomplished on an ad hoc basis. In other words, extant resources were tapped to perform FID activities. However, several studies had conclusively documented that ‘the lack of sustained, coordinated effort by individuals dedicated to the [aviation] FID mission is the principal reason we [AFSOC] have failed to achieve the long-term changes in the way developing countries support, sustain, and employ airpower.’¹⁵

Today, we see history beginning to repeat itself in the need to formalize cyber-FID.

Similar to aviation FID, this article argues that the concept of cyber-FID is not new; rather, it emerged from the void created in SOF FID operations toward the end of the Global War on Terror during the global shift to great power competition—particularly in the cyber domain.¹⁶ It is at this critical *inflection point*, as the United States faces two cyber-capable superpowers and the character of war continues to evolve, that the nation must move beyond ad hoc efforts to achieve long-term, systemic changes in how developing countries support, sustain, and employ cyber defense capabilities.¹⁷

In his proposal to create Cyber Engagement Teams (CETs), Smith estimates that full implementation would likely take more than five years. He urges that a CET or similar construct be “‘incorporated at the earliest in all activities” because “cyber operations support and are complementary to all levels of war and warfighting functions.”¹⁸ Thus, the time is now for a framework that can lead to a sustained, coordinated cyber-FID effort.

Unlike aviation FID, however, cyber-FID must account for the many unique challenges inherent in cyberspace. Cyber is now ubiquitous, reaching into all aspects of human society. Cyber threats are pervasive, and cyber actors range from individuals to nation-state-sponsored groups and everything in between. Aviation doctrine does not need to consider attribution and anonymity in the sky, and airspace and air capabilities do not evolve as rapidly as cyber does. Jurisdictional boundaries in cyberspace are not clearly defined, and even if they were, cyber actors frequently use infrastructure hop points between their command and control and their final target. These challenges, among many others, are unique to cyberspace. The cyber community continues to evolve and innovate to counter them effectively. A cyber-FID framework provides a tool to rapidly transfer these innovations to the host nation.

Literature Review

This article fills a gap in the current literature by proposing a new cyber-FID framework. In 2013, Colonel Brian Petit (USA, Ret.) made a seminal contribution to the Special Operations literature with his book *Going Big by Getting Small*, which examined the strategic use of SOF in peaceful, left-of-boom engagements. In the book’s foreword, Admiral Eric Olson (USN, Ret.) explains, “Much of the literature on special operations is

dominated by headline-making missions: deep raids, harrowing firefights, close combat actions... yet there is another narrative on special operations [of strategic peacetime engagements] told less often and with greater difficulty.”¹⁹ Although the former still dominates special operations literature, there is now a substantial body of work on special operations strategy, including *Special Operations: Out of the Shadows*, edited by Christopher Marsh et al.²⁰ There is also a growing body of literature on cyber strategy, such as *Cyber Persistence Theory* by Michael Fischerkeller and *Cybersecurity and Cyberwar* by P.W. Singer.²¹

However, literature on the intersection of cyber and special operations strategy remains limited. Most existing work consists of operational doctrine and contemporary news cases. Colonel (Ret.) Patrick Duggan wrote several articles on this topic between 2014 and 2016, Colonel the one referenced above. A few other works, such as *Expanding the Menu: The Case for CYBERSOC* by Benjamin Brown, argue for the creation of a cyber-SOF component and explore organizational design considerations.²² Additionally, the article *The Integration of Special Forces in Cyber Operations* by LTC Jonas van Horen of the Netherlands Ministry of Defense examines, using the Netherlands as a case study, three roles in which SOF could support the cyber domain, as well as three potential models for a SOF-cyber organization.²³

Methodology

Extensive academic research was conducted to determine whether a cyber-FID framework already exists—whether codified across multiple documents or referred to by a different name. Finding no such evidence, over a dozen SOF and/or cyber practitioners were interviewed to develop a deeper understanding of traditional FID and current capacity-building efforts in the cyber domain. Finally, leveraging personal cyber expertise and building on *JP 3-22*, this research proposes a new cyber-FID framework.

The Cyber-FID Framework

“I use the term ‘framework’ because it is less deterministic than a theory and not as prescriptive as a method. It is messy, full of contradictions, and much more art than science... There is nothing parsimonious about the cyber-FID framework I present.”²⁴ —
Marko Papic, Author (modified quote)

This section begins with the doctrinal definition of traditional FID and a brief explanation. It then addresses common critiques encountered during the research process regarding why cyber-FID is the appropriate construct for countering today’s threat of future global power conflict. Finally, the section concludes by defining the cyber-FID framework.

An Overview of Traditional FID

The Joint Staff’s *JP 3-22, Foreign Internal Defense*, is a 200+ page publication detailing the FID mission. This article does not attempt to cover all aspects of *JP 3-22* but instead establishes a baseline of traditional FID concepts as a foundation for exploring its extension into cyber-FID. From *JP 3-22*:

FID is the participation by civilian agencies and military forces of a government or international organization in any of the programs or activities taken by a host nation (HN) government to free and protect its society from subversion, lawlessness, insurgency, violent extremism, terrorism, and other threats to its security. The United States Government (USG) applies FID programs or operations within a whole-of-government approach to enhance the IDAD program of the HN by specifically focusing on an anticipated, growing, or existing internal threat.²⁵

There are two key components to emphasize in this definition. First, FID is conducted to “enhance a HN’s IDAD program”—the sole purpose of FID should never be solely about U.S. objectives, though it should always align with U.S. interests. Second, FID requires a *whole-of-government approach* and is not solely the domain of SOF or even the Department of Defense (DoD). In fact, FID involves all instruments of national power, as illustrated in JP 3-22’s Figure 1: *FID Instruments and Sources of National Power*. However, for simplicity, this article focuses exclusively on the military instrument.

Cyber FID and the State-on-State Threat

During the research for this article, practitioners held competing views on whether protecting against a state-on-state cyber threat truly falls under FID. Two main arguments suggest it does not.

The first argument centers on the stark contrast between traditional FID threats—terrorists, insurgents, and violent extremists—versus the stereotypical *hackers in hoodies* located somewhere in dark basements. However, as Mikko Hypponen highlights in his *linux.com* blog post, this stereotype obscures the significant threat posed by highly sophisticated, well-trained, and often state-funded cyber professionals.²⁶ Similarly, excluding cyber from the FID discussion simply because it operates in the digital rather than the physical realm would be a mistake, as modern conflicts increasingly span both physical and digital domains.

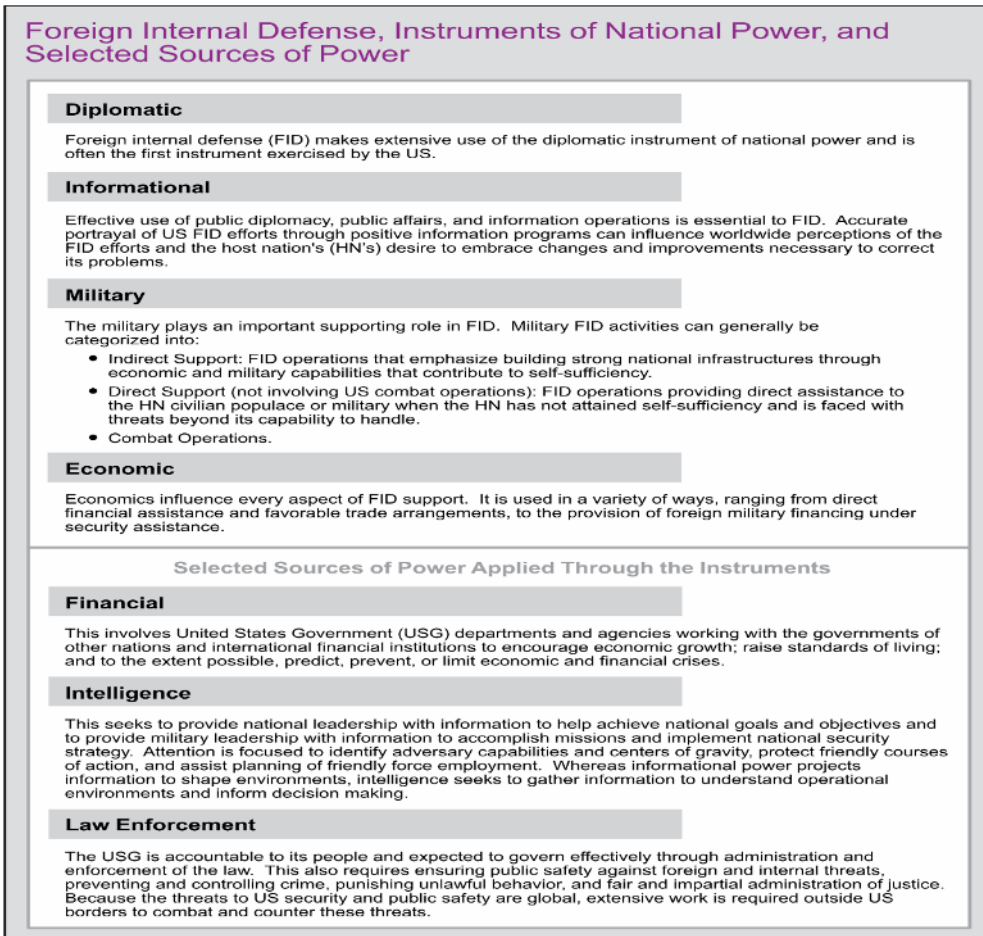


Figure 1 – FID instruments and sources of national power²⁷

The need for convergence between the cyber and physical domains—both in practice and in thought—is discussed in a Spring 2021 *Military Review* article by Maj. Anthony Formica, U.S. Army. He warns, “The United States has run out of time for developing approaches to compete in the cyber domain, and it must use the assets and forces currently available to prevent future strategic setbacks.”²⁸ Formica makes two key points. First, he concludes that the initial effects of future wars will occur in the digital information environment, as demonstrated by Russia’s annexation of Crimea. Second, he draws an analogy to Germany’s superior tank power in the Second World War, arguing that Russia has similarly embraced the cyber domain—adapting its entire concept of conflict around it—while the United States, in contrast, is slow-rolling convergence²⁹ and continuing “to focus on the men with guns and the tanks... and not on the host of hostile actions [in cyberspace] that precede them.”³⁰ Therefore, advancing the concept of cyber-FID is a necessary response to the growing cyber threat.

The second argument against classifying this as an FID problem focuses on the external nature of the threat, particularly within the context of great power competition. However, David Ueko addresses this concern in his article *The Role and Limits of Special Operations in Strategic Competition*:

In recent years, SOF has broadened its thinking on foreign internal defense (FID)... whereas FID traditionally meant aiding a friendly government against an insurgency, SOF now looks upon [FID] to boost a country's 'resilience' against foreign-sponsored proxies, modes of disinformation, or political infiltration.³¹

This shift toward resilience is equally necessary in the cyber domain, which is not constrained by borders and serves as a primary medium for disinformation.

Bradenkamp and Grzegorzewski effectively argue in their 2021 *Special Operations Journal* article that Russia has long employed cyber gray zone tactics to wage unconventional warfare (UW), first in Estonia (2007), then Georgia (2008), and most recently in Ukraine (2014 and 2022).³² The authors emphasize that Russia "used hackers, both native and foreign... to slow down [the defending] response to Russia's conventional invasion... [and] could use virtual applications and proxy forces to have real-world effects."³³ Not only do cyber operations have tangible implications for a country's internal security, but Russia's UW tactics and advanced preparation of the battlefield allowed them to "quickly activate opposition groups within Ukraine to achieve strategic objectives before anyone could respond."³⁴ Since cyber clearly poses a direct threat to a host nation's internal security, advancing the concept of cyber-FID is both relevant and necessary.

Details of Traditional FID

"Although on the surface, FID appears to be a relatively simple concept, that appearance is deceptive; FID is [more] nuanced and complicated... often confused [with] training foreign forces, when in reality, there is much more to it."³⁵ — *Colonel (Ret.) John Mulbury, Army Special Operations Forces*"

According to *JP 3-22*, as multi-domain transregional threats continue to grow, geographic combatant commanders rely on FID to "counter these threats in multiple countries, organized from an ideological credence [to support] each affected nation's security."³⁶ FID may take the form of a program, an operation, or a combination of both, integrated with interagency efforts as necessary and operating under the coordination of the U.S. embassy country team, as authorized by the Chief of Mission. Traditional FID falls into three categories, all requiring close coordination with interagency and international partners: direct support, indirect support, and U.S. combat operations. While FID is a core SOF function, it is not exclusively a military operation. Requiring a *whole-of-government approach*, it is also supported by conventional and multinational forces, as well as other U.S. Government (USG) departments and agencies.³⁷ The key characteristics of FID are illustrated in *Figure 2 - Characteristics of Foreign Internal Defense*.

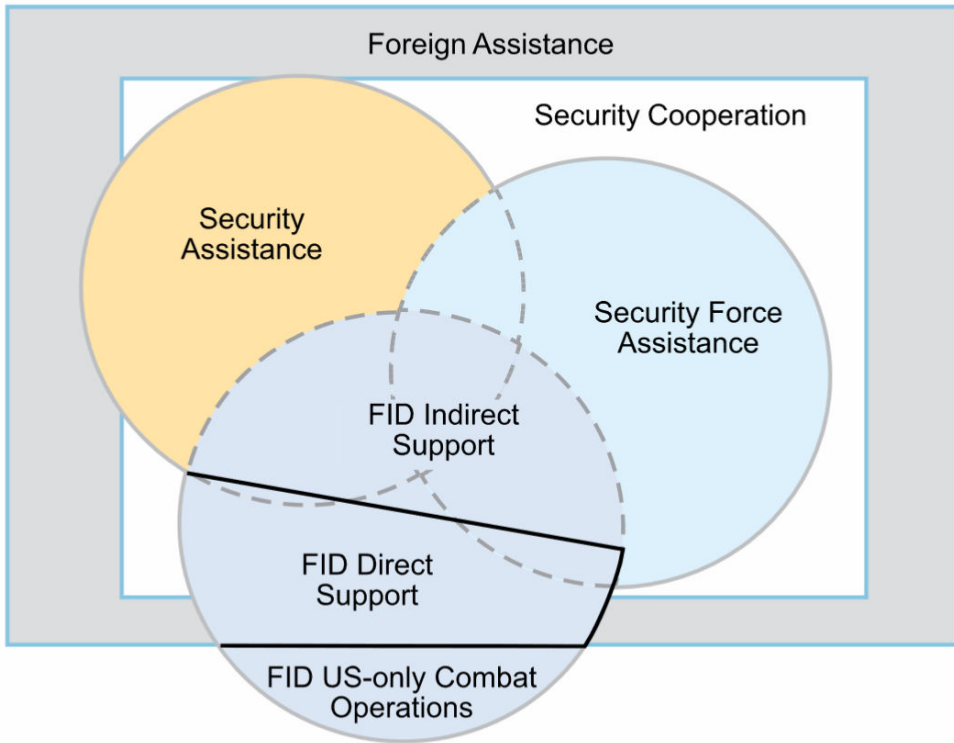
Characteristics of Foreign Internal Defense

- Involves all instruments of national power.
- Can occur across the range of military operations.
- Is conducted by both conventional forces and special operations forces.
- Supports and influences the host nation's internal defense and development program.
- Includes training, materiel, technical and organizational assistance, advice, infrastructure development, and tactical operations.
- Generally, the preferred methods of support are through assistance and development programs.

Figure 2 – Characteristics of Foreign Internal Defense³⁸

It is important to define where FID sits in relation to several related concepts, as illustrated in *Figure 3 - Functional Relationship of Concepts Related to FID*. Security cooperation is fully encompassed within foreign assistance. As a broad term describing all DoD efforts to “develop foreign defense and security capabilities and build defense security relationships,”³⁹ security cooperation addresses the root causes of violent extremist organizations. It includes security assistance activities conducted under *U.S. Code Title 22* (which covers diplomatic efforts) and forms a key element of FID by “providing many of the resources in the form of funding, materiel, and training.”⁴⁰ These efforts make up a significant portion of FID’s indirect support activities. Another major component of FID’s indirect support is security force assistance, which describes activities to “organize, train, equip, rebuild/build, advise, and assist”⁴¹ foreign forces. Together, security cooperation and security force assistance provide the foundational support structure for FID operations.

The Functional Relationships Among Foreign Assistance, Security Cooperation, Security Assistance, Security Force Assistance, and Foreign Internal Defense



Legend

- FID foreign internal defense
- Assistance to foreign nations ranging from the sale of military equipment to donations of food and medical supplies to aid survivors of natural and manmade disasters
- US Government programs that enable the provision of defense articles, military training, and other defense-related services by grant, lease, loan, credit or cash sales in furtherance of national policies and objectives
- Department of Defense interactions with foreign security establishments to build security relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access
- Department of Defense activities that support the development of the capacity and capabilities of foreign security forces and their supporting institutions
- Participation by civilian agencies and military forces of a government or international organization in any of the FID activities taken by a host nation to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security

Figure 3 – Functional relationship of concepts related to FID⁴²

FID also includes direct support activities short of combat operations. According to *JP 3-22*, direct support involves:

use of US forces to provide direct assistance to the HN civilian populace, or military. They differ from [security assistance] in that they are joint- or Service-funded, do not usually involve the transfer of arms and equipment, and do not usually (but may) include training local military forces. Direct support operations are normally conducted when the HN has not attained self-sufficiency and is faced with social, economic, or military threats beyond its capabilities to handle. Assistance normally focuses on civilian-military operations (primarily, the provision of services to the local populace), military information support operations (MISO), operations security (OPSEC), communications and intelligence cooperation, mobility, and logistics support. In some cases, training of the military and the provision of new equipment may be authorized.⁴³

Notably, this section of *JP 3-22* includes cybersecurity assistance as a component of direct support activities but does not provide details on what form this assistance might take. This article expands on that assistance, incorporating cyber's role in all three categories of FID: indirect support, direct support, and U.S. combat operations, forming the foundation of the cyber-FID framework.

The final category of FID, U.S. combat operations, requires a Presidential decision to introduce U.S. combat forces as a temporary measure until host nation (HN) forces regain the capacity to conduct independent operations. These efforts typically take the form of one or more of the following: counterinsurgency (COIN), counterterrorism (CT), counter-drug (CD), or stabilization operations.⁴⁴ Importantly, the HN maintains overall responsibility and initiative for all U.S. FID operations to “preserve its legitimacy and ensure a lasting solution to the problem.”⁴⁵ Command and control in these operations is complex and requires “judicious and prudent rules of engagement” to maintain the perceived legitimacy and sovereignty of the HN government.⁴⁶

According to *JP 3-05, Special Operations*:

FID operations are planned at the national and ministerial levels... in support of the HN IDAD strategy and in coordination with the [Chief of Mission],” who leads the overall FID effort. “FID planning is complex... FID planners must understand US foreign policy, focus to maintain or increase HN sovereignty and legitimacy, and understand the strategic implications and sustainability of US assistance to an HN... Military planning for unified action is essential to build unity of effort in the USG approach to FID.”⁴⁷

The same principles apply to cyber-FID, reinforcing the need for cohesive, well-planned integration of cyber capabilities into the broader FID mission.

The Cyber-FID Framework

“We have learned that we cannot live alone in peace. We have learned that our own well-being is dependent on the well-being of other nations far away. We have learned to be citizens of the world, members of the human community”⁴⁸ — *President Franklin Delano Roosevelt*

This article now turns to the creation of the cyber-FID framework. The old adage that *people are our greatest asset* is particularly relevant in this context, as in all others. SOF are often best positioned for FID operations “due to their extensive language capability, cultural training, advising skills, and regional expertise.”⁴⁹ This applies to the cyber domain as well. As one Cyber National Mission Force (CNMF) officer observed during Hunt Forward operations in Ukraine: “[Ukrainian partners] will have a certain way of drawing a network object, and the terminology gap had to be beaten before we could proceed [with the operations].”⁵⁰ In addition to personnel, physical hardware is also necessary and may be obtained through host nation purchase or U.S. security assistance as part of the cyber-FID effort. As with other SOF initiatives, cyber-FID requires time to mature the HN cybersecurity posture and to achieve IDAD objectives through a whole-of-government, multi-stakeholder effort.

Occurs During Adversary Gray Zone Activities		During HN “Failing State”
<p style="text-align: center;">Indirect Support</p> <p style="text-align: center;">Cyber Security Assistance Joint & Multinational Cyber Exercises Cyber Exchange Programs</p>	<p style="text-align: center;">Direct Support</p> <p style="text-align: center;">Cyber Intelligence Cooperation Ops in the Info Environment Cyber Training</p>	<p style="text-align: center;">US Combat Operations</p> <p style="text-align: center;">(e.g. Offensive & Defensive Cyber Operations)</p>
<p style="text-align: center;">U.S. Enabling HN Operations</p>	<p style="text-align: center;">U.S. Conducting Operations</p>	

Figure 4 – The Cyber-FID framework

Summarized in *Figure 4 - The Cyber-FID Framework*, the framework is structured similarly to traditional FID, dividing operations into three categories: indirect support operations, direct support operations, and U.S. combat operations. As illustrated in blue across the top of the figure, indirect and direct support operations may take place during adversary gray zone activities, whereas U.S. combat operations can only occur when the host nation is in a failing state. Additionally, as shown in gray at the bottom of the figure, indirect support operations are solely intended to enable the HN, whereas U.S. forces may conduct operations on behalf of the HN as part of direct support or U.S. combat operations.

The following sections explore how the traditional FID categories outlined in *JP 3-22* are adapted to the cyber context.

Indirect Support Operations

This category of cyber-FID focuses on providing equipment and training to enable the host nation (HN) to secure itself in cyberspace and conduct its own cyberspace operations (CO). It can be divided into three broad approaches, adapted from *JP 3-22*: (1) cyber security assistance, (2) joint and multinational cyber exercises, and (3) cyber exchange programs.⁵¹

The first approach, cybersecurity assistance, includes the provision of cyber equipment, training, and services to the HN. Cyber equipment may consist of computing and networking hardware for end users and national communications infrastructure. Unlike traditional FID, which covers mostly specialized defense articles, cyber-FID relies heavily on commercially available hardware, highlighting the crucial role of the private sector in cyber-FID operations. Cyber-FID efforts will train HN forces to conduct cyberspace operations, including network security operations and cyber threat hunting. Additionally, it will include “train the trainer” courses to teach HN personnel how to conduct future cyber training independently. Services encompass any: “service, test, inspection, repair, [or] training publication... used for the purpose of furnishing military [cyber] assistance... usually integrated with equipment support... to ensure the equipment is suitable for HN needs and the HN is capable of maintaining it.”⁵²

The next approach, joint and multinational cyber exercises, “offer the advantage of training US forces while simultaneously increasing interoperability with HN forces.”⁵³ Since 2016, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) has hosted Crossed Swords, an annual cyber training exercise encompassing various cyber disciplines.⁵⁴ This complex exercise covers multiple geographic areas, involves critical information infrastructure providers, and integrates cyber-kinetic engagements,⁵⁵ drawing participation from over 100 experts across more than two dozen countries. According to the CCDCOE’s report from Crossed Swords 2020, “the focus is on advancing cyber Red Team members’ skills in preventing, detecting and responding to an adversary in the context of full-scale cyber operations.” The report goes on to explain, “The main task and lesson is to understand the coordination between multiple disciplines... link cyber elements with conventional force... [train] penetration testers, digital forensic professionals, and situational awareness experts.”⁵⁶ U.S. cyber-FID efforts would benefit greatly from participating in and/or organizing similar exercises, enhancing both HN capabilities and interoperability with U.S. and allied forces.

The final approach to indirect support operations is cyber exchange programs, which may occur at an individual or unit level. These programs serve to: “foster greater mutual understanding and familiarize each force with the operations of the other.”⁵⁷ As described in *JP 3-22*, commanders can maximize the benefits of exchange programs by combining them with joint and multinational exercises. For example, in a cyber exercise such as Crossed Swords, key cyber personnel could be exchanged to work alongside the partner nation’s cyber and conventional forces. This approach is likely to be far more effective for improving interoperability than exchanges conducted during routine operations

Direct Support Operations

Unlike indirect support operations, which focus on enhancing the host nation's (HN) self-sufficiency, direct support operations involve U.S. forces actively conducting operations in support of the HN.⁵⁸ Under traditional FID, as discussed earlier, direct support is typically employed when the HN faces threats—such as ongoing kinetic attacks—beyond its ability to handle.⁵⁹ In the cyber domain, however, the threshold that shifts an HN's FID need from indirect to direct support may be less clearly defined.

According to Formica, citing the 2017 National Security Strategy:

America's rivals have 'become skilled at operating below the threshold of military conflict... with hostile actions cloaked in deniability.' Cyberspace operations... not only [set] the conditions for the employment of traditional forces but also [complement] their efforts by weaving a web of muddled facts and plausible deniability.⁶⁰

By the time an adversary has set the conditions to employ traditional forces against the HN, the U.S. may have little time to respond. To protect against a *fait accompli* attack, such as Russia's 2014 annexation of Crimea, direct support operations should be considered and conducted concurrently with indirect support operations.⁶¹ Cyber-FID direct support can be categorized into three areas: (1) cyber intelligence cooperation, (2) operations in the information environment, and (3) cyber training.

The bedrock of any cyber operation, including cyber-FID, is intelligence. As stated in *JP 3-22*, the following principles apply to cyber-FID and cyber intelligence:

The sharing of US intelligence is a sensitive area that must be evaluated based on the circumstances of each situation. Cooperative intelligence liaisons between the US and HN are vital; however, disclosure of classified information to the HN or other multinational FID forces must be authorized. Generally, assistance must be provided in terms of evaluation, training, limited information exchange, and equipment support."⁶²

This assistance is tailored to the HN's specific needs and capabilities, with the goal of helping the HN achieve self-sufficiency.

A notable example of cyber-FID intelligence cooperation, though not previously categorized as such, is USCYBERCOM's Hunt Forward Operations (HFO). In December 2021, Lt. Gen. Hartman, then head of the Cyber National Mission Force (CNMF), discussed HFO deployments to Ukraine weeks before the Russian invasion. What was intended as a standard initial assessment before deploying the full CNMF team for the HFO was quickly deemed insufficient: "Instead of executing the normal plan, the team lead immediately got on the phone and asked to deploy the rest of the team, and we immediately went into a hunt operation."⁶³ HFO are only conducted at the request of the HN, and it's easy to see how these conditions, with the imminent threat of 130,000 Russian soldiers amassed on the border, would classify this as a cyber-FID direct support operation.

In an interview, Lt Gen Hartman described the way intelligence "fits in for [the CNMF] first and foremost," stating that the CNMF "wants to execute an intelligence-driven

mission.” He also highlighted the role of private-sector cyber intelligence, calling it “extraordinarily powerful” in helping U.S. cyber forces locate adversaries. According to Hartman, all cyber intelligence gathered during HFOs is shared directly with the HN. On the ground in Ukraine, whenever the CNMF found evidence of a Russian cyberattack, the team immediately shared the information with Ukrainian counterparts. This intelligence-sharing partnership has continued even after the U.S. team left. As of the interview, Hartman estimated that “we’ve shared over 6000 indicators of compromise... that’s all stuff we’ve been able to see from industry partnerships... from activity on the ground.”⁶⁴ HFOs are an established practice of cyber intelligence cooperation with host nations and fit perfectly within the cyber-FID direct support framework.

Formica described another example of cyber intelligence cooperation, which would be the bedrock of what he referred to as a convergence fusion cell. The fusion cell would deploy the right personnel, resources, and authorities to, for example, establish NATO Force Integration Units as an early warning of adversary convergence between cyber and physical domains. The primary mission of convergence fusion cells would be to combine intelligence from cyberspace and the information environment with developing events in the physical world to detect a fait accompli attack in its infancy and to have the ability to respond quickly enough to prevent the attack from being carried out.⁶⁵ This intelligence cooperation model would broadly encompass multiple data streams across the U.S., HN, and regional intelligence and law enforcement agencies.

The second category of cyber-FID direct support is operations in the information environment.⁶⁶ Information is a main component of any military operation, and cyber-FID forces can leverage it to achieve national objectives in support of the HN Internal Defense and Development (IDAD) strategy. *JP 3-22* lays out considerations for the role of Military Information Support Operations (MISO) in traditional FID, which also applies to cyber-FID direct support operations. As in traditional FID, MISO can be used for cyber-FID direct support operations to “gain, preserve, and strengthen civilian support for the HN government and its IDAD program,” and “build and maintain the morale of HN forces” in the face of cyberattack.⁶⁷ MISO can also be employed to persuade the adversary that cyberattacks will fail or will not be worth the cost of carrying out. It can be used to “project a favorable image of the HN government and the US... inform the international community of US and HN intent and goodwill... [and] develop HN information capabilities.”

The final category of cyber-FID direct support operations is cyber training. According to *JP 3-22*, “the HN FID situation may intensify and increase the need for training beyond that of indirect support. Direct support operations should provide more immediate benefit to the HN and may be used in conjunction with various types of SA indirect support training.”⁶⁸ The illegal invasion of Ukraine and the associated Russian cyberattacks provide an example of conditions suitable for cyber-FID direct support cyber training. In an October 2023 article, the SOFREP News Team reported that Estonia and the European Union recently established a cyber classroom and military cyber facility in Kyiv, both designed to: “[prepare] Ukrainian specialists to defend against sophisticated cyberattacks and ensure the stability and functionality of the nation’s digital society during times of conflict.” Additionally, “the United States and Denmark announced a collaborative effort... [to] develop a skilled [Ukrainian] cybersecurity workforce.”⁶⁹ The article did not provide

details on the specifics of the cyber training, but this effort could be better coordinated within the broader cyber-FID framework proposed in this article.

U.S. Combat Operations

Finally, according to *JP 3-22*: “U.S. participation in combat operations as part of a FID effort requires Presidential approval” and may occur if “the condition of the [HN]... descend[s] into a failing state.” More information about defensive and offensive cyberspace operations (CO) that may be conducted can be found in *JP 3-12, Cyberspace Operations*:

Cyberspace capabilities are integrated into the Joint Force Commander’s plans and synchronized with other operations across the range of military operations... Effective integration of CO with operations in the physical domains requires the active participation of CO planners and operators... in coordination with other USG departments and agencies and national leadership.⁷⁰

Nothing in the unclassified literature suggests that Presidential approval was granted for Ukraine, or that the U.S. has participated in cyberspace operations associated with this conflict. However, such participation could be an option under the cyber-FID framework.

Conclusion

For USSOCOM, understanding the role of cyber in its FID mission is a crucial evolution in how the United States competes with its adversaries. The cyber-FID framework presented in this article provides a structured approach for U.S. forces, reassures allies and partners, and highlights the importance of cyber-FID efforts in addressing the changing character of war. As seen in the aviation FID case study examined earlier, the concepts of cyber-FID are not new—but formalizing them into a single framework is now necessary to compete and win in this era of great power competition.

The framework proposed in this article follows the same structure as traditional FID, divided into three main categories. First, indirect support operations, which include activities such as cybersecurity assistance, joint and multinational cyber exercises, and cyber exchange programs. Second, direct support operations, which encompasses cyber intelligence cooperation, operations in the information environment, and cyber training. Finally, U.S. combat operations, require Presidential approval and may include offensive or defensive cyber operations.

This framework should be viewed as a starting point for the cyber-FID discussion. It needs to be debated, operationalized, and refined. The framework was developed from a single, biased, American perspective, so evolving it with input from the partners it is meant to support will be critical to its success. Additionally, this article does not address the current legal and policy constraints on cyber operations, how these constraints may shift in times of competition, crisis, or conflict, or their potential impact on cyber-FID—particularly regarding host nation consent and compliance. Clearly, these issues require further research.

Finally, while this article focuses on cyber-FID within the military instrument of power, it is important to recognize that FID extends across all instruments of power. Future work should examine the role of other DIME-FIL instruments and interagency partners in cyber-FID efforts—perhaps starting with the U.S. Department of State and its existing cyber capacity-building initiatives. Further, USSOCOM should explore how private sector activities—particularly recent efforts to support Ukraine⁷¹—could be incorporated into the cyber-FID model.

Endnotes

- ¹ Joint Chiefs of Staff, *Special Operations*, JP 3-05 (Washington, DC: Joint Chiefs of Staff, 2020), II–10.
- ² Brian S. Petit, *Going Big by Getting Small: The Application of Operational Art by Special Operations in Phase Zero* (Parker, CO: Outskirts Press, 2013).
- ³ Patrick Duggan, “Strategic Development of Special Warfare in Cyberspace,” National Defense University Press, October 1, 2015, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/621123/strategic-development-of-special-warfare-in-cyberspace/>.
- ⁴ Joint Chiefs of Staff, *Foreign Internal Defense*, JP 3-22 (Washington, DC: Joint Chiefs of Staff, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_22.pdf.
- ⁵ Joint Chiefs of Staff, *Special Operations*, II–4.
- ⁶ William R. Smith, “Bytes, With, and Through: Establishment of Cyber Engagement Teams to Enable Collective Security.,” *Special Operations Journal* 5, no. 2 (July 1, 2019): 151, <https://doi.org/10.1080/23296151.2019.1658056>.
- ⁷ James M. DePolo, “Foreign Internal Defense and Security Force Assistance,” in *Special Operations: Out of the Shadows*, ed. Christopher Marsh, James D. Kiras, and Patricia J. Blocksome (Boulder, Colorado: Lynne Rienner Publishers, 2019), 164.
- ⁸ Cyberspace Solarium Commission, “Final Report,” March 2020, <https://www.solarium.gov/report>.
- ⁹ Smith, “Cyber Engagement Teams,” 154.
- ¹⁰ U.S. Department of Defense, *2014 Quadrennial Defense Review* (Washington, DC, 2014), V–VI, https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/2014_Quadrennial_Defense_Review.pdf.
- ¹¹ U.S. Special Operations Command, “White Paper: The Gray Zone,” September 9, 2015, 1, <https://publicintelligence.net/ussocom-gray-zones/>.
- ¹² U.S. Special Operations Command, 8.
- ¹³ Mark A. Milley, *National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, 2022), 1, https://www.jcs.mil/Portals/36/NMS%202022%20_%20Signed.pdf.
- ¹⁴ Wray R. Johnson, “Whither Aviation Foreign Internal Defense?,” *Airpower Journal*, March 1, 1997, 2–3, https://archive.org/details/DTIC_ADA360614.
- ¹⁵ Johnson, 5. This author quotes from a third source that could not be located and was cited as follows: “AFSOC Foreign Internal Defense (FID) Capability,” position paper, 25 November 1991.
- ¹⁶ See: Laura Jones, “The Future of Warfare Is Irregular,” *Fletcher Forum of World Affairs*, July 1, 2022, https://static1.squarespace.com/static/579fc2ad725e253a86230610/t/633fae96d4791b16affa5288/1665117846643/Jones-2a_APPROVED.pdf.
- ¹⁷ Milley, *National Military Strategy of the United States of America*, 1.
- ¹⁸ Smith, 161.
- ¹⁹ Eric Olson. Forward to *Going Big by Getting Small: The Application of Operational Art by Special Operations in Phase Zero*, by Brian Petit. (Parker, CO: Outskirts Press, 2013), iii-iv.
- ²⁰ Christopher Marsh, James D. Kiras, and Patricia J. Blocksome, eds., *Special Operations: Out of the Shadows* (Boulder, Colorado: Lynne Rienner Publishers, 2019).
- ²¹ P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014).
- ²² Benjamin Brown, “Expanding the Menu: The Case for CYBERSOC,” *Small Wars Journal*, January 5, 2018, <https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc>.

- ²³ Jonas van Hooren, “The Integration of Special Forces in Cyber Operations,” 2022, <https://nps.edu/documents/110773463/135759179/The+Integration+of+Special+Forces+in+Cyber+Operations.pdf>.
- ²⁴ Marko Papić, *Geopolitical Alpha: An Investment Framework for Predicting the Future* (Hoboken, New Jersey: Wiley, 2020), 3. The original quote: “there is nothing parsimonious about the *constraint* framework I present.” I liked how the author described the term ‘framework,’ so I modified the quote to apply to *cyber-FID*.
- ²⁵ Joint Chiefs of Staff, *Foreign Internal Defense*, ix.
- ²⁶ Mikko Hyppönen, “Real Hackers Don’t Wear Hoodies: Cybercrime Is Big Business,” *Linux.Com* (blog), June 8, 2016, <https://www.linux.com/news/real-hackers-dont-wear-hoodies-cybercrime-big-business/>.
- ²⁷ Source: Joint Chiefs of Staff, *Foreign Internal Defense*, I–9.
- ²⁸ Anthony M. Formica, “From Cambrai to Cyberspace: How the U.S. Military Can Achieve Convergence between the Cyber and Physical Domains,” *Military Review* (U.S. Army CGSC, March 1, 2021), 101, Gale Academic OneFile.
- ²⁹ Formica, 103.
- ³⁰ Formica, 106.
- ³¹ David H Ucko, “The Role and Limits of Special Operations in Strategic Competition: The Right Force for the Right Mission.,” *RUSI Journal: Royal United Services Institute for Defence Studies* 168, no. 3 (May 1, 2023): 12, <https://doi.org/10.1080/03071847.2023.2219701>.
- ³² Nicholas Bredenkamp and Mark Grzegorzewski, “Supporting Resistance Movements in Cyberspace,” *Special Operations Journal* 7, no. 1 (January 2, 2021): 17–28, <https://doi.org/10.1080/23296151.2021.1904570>.
- ³³ Bredenkamp and Grzegorzewski, 23.
- ³⁴ Bredenkamp and Grzegorzewski, 23.
- ³⁵ Joint Chiefs of Staff, *Foreign Internal Defense*, I–1.
- ³⁶ Joint Chiefs of Staff, I–1.
- ³⁷ Joint Chiefs of Staff, I-1-I–3.
- ³⁸ Source: Joint Chiefs of Staff, I–8.
- ³⁹ Joint Chiefs of Staff, I–14.
- ⁴⁰ Joint Chiefs of Staff, I–16.
- ⁴¹ Joint Chiefs of Staff, xxii.
- ⁴² Source: Joint Chiefs of Staff, I–15.
- ⁴³ Joint Chiefs of Staff, I–18.
- ⁴⁴ Joint Chiefs of Staff, I–24.
- ⁴⁵ Joint Chiefs of Staff, I–25.
- ⁴⁶ Joint Chiefs of Staff, I–25.
- ⁴⁷ Joint Chiefs of Staff, *Special Operations*, II–11.
- ⁴⁸ Quoted by: E. John Teichert, “The Building Partner Capacity Imperative,” *DISAM Journal of International Security Assistance Management* (Defense Institute of Security Assistance Management, August 1, 2009), <https://www.proquest.com/docview/197766575>.
- ⁴⁹ Joint Chiefs of Staff, *Foreign Internal Defense*, xviii.
- ⁵⁰ Ryan, interview by Dina Temple-Raston, “Exclusive: Inside an American Hunt Forward Operation in Ukraine,” June 20, 2023, in *Click Here*, produced by Recorded Future News, podcast, loc. 12:42–53, accessed May 10, 2024, <https://podcasts.apple.com/us/podcast/72-exclusive-inside-an-american-hunt-forward/id1225077306?i=1000617669131>.
- ⁵¹ Joint Chiefs of Staff, *Foreign Internal Defense*, chap. VI sec. B “Indirect Support.”

⁵² Joint Chiefs of Staff, VI–10.

⁵³ Joint Chiefs of Staff, VI–12.

⁵⁴ NATO Cooperative Cyber Defense Centre of Excellence, “Crossed Swords,” CCDCOE, accessed March 15, 2024, <https://ccdcoe.org/exercises/crossed-swords/>. According to the CCDCOE website, “recent iterations” have been jointly organized with CERT.LV which is the national cyber incident response institution of the Republic of Latvia.

⁵⁵ NATO Cooperative Cyber Defense Centre of Excellence. No US participation in this exercise could be found.

⁵⁶ NATO Cooperative Cyber Defense Centre of Excellence, “Exercise Crossed Swords 2020 Reached New Levels of Multinational and Interdisciplinary Cooperation,” CCDCOE, accessed March 15, 2024, <https://ccdcoe.org/news/2020/exercise-crossed-swords-2020-reached-new-levels-of-multinational-and-interdisciplinary-cooperation/>.

⁵⁷ Joint Chiefs of Staff, *Foreign Internal Defense*, VI–13.

⁵⁸ Joint Chiefs of Staff, VI–13.

⁵⁹ Joint Chiefs of Staff, chap. VI sec. C “Direct Support (Not Involving United States Combat Operations).”

⁶⁰ Formica, “From Cambrai to Cyberspace,” 104.

⁶¹ Formica, 104.

⁶² Joint Chiefs of Staff, *Foreign Internal Defense*, VI–27.

⁶³ Dina Temple-Raston, “Q&A With Gen. Hartman: ‘There Are Always Hunt Forward Teams Deployed,’” *The Record*, June 20, 2023, <https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here>.

⁶⁴ Temple-Raston.

⁶⁵ Formica, “From Cambrai to Cyberspace,” 107.

⁶⁶ For more information see: U.S. Department of Defense, *Strategy for Operations in the Information Environment* (Washington, DC, 2023), <https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF>.

⁶⁷ Joint Chiefs of Staff, *Foreign Internal Defense*, VI–21.

⁶⁸ Joint Chiefs of Staff, VI–23.

⁶⁹ SOFREP News Team, “Ukraine Enhances Cyber Defense with New Training Facility,” October 13, 2023, <https://sofrep.com/news/ukraine-enhances-cyber-defense-with-new-training-facility/>.

⁷⁰ Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2018), I–8.

⁷¹ For example, see the work done by the Cyber Defense Assistance Collaborative, which “came together to provide operational cyber defense assistance to Ukraine during the 2022 Russian invasion.” (<https://crdfglobal-cdac.org/>) How can USSOCOM leverage similar processes to respond to future crises?

COMMENTARY**For Want of a Nail, the Kingdom was Lost: The Struggle to Understand Irregular Warfare**

Robert C. Jones, U.S. Special Operations Command, MacDill AFB, Florida, USA

ABSTRACT

We have a new definition of irregular warfare, and to paraphrase Winston Churchill, we are “perhaps, at the end of the beginning.” Now, the real work begins—improving how we think about the many diverse challenges and activities encompassed within irregular warfare (IW). Ultimately, IW is a manmade, largely administrative construct created by the Department of Defense (DoD) for the DoD. Within IW, however, resides a diverse collection of naturally occurring human dynamics. These cannot be defined to suit our biases; rather, we must strive to understand them for what they are. At some point, we must ask: Are our manmade constructs and their definitions the problem? Or are we more hindered by our flawed understanding of the nature of the challenges we face and the growing limitations of state power to control them? This article argues that the latter is the greater issue—but both must be addressed.

KEYWORDS

irregular warfare, insurgency, unconventional warfare, deterrence, influence, special operations, populations, governance

“Look deep into Nature, and you will understand everything better.” —Albert Einstein

The principal reason the United States struggles with irregular warfare (IW) is its deeply flawed understanding of *insurgency*. Getting insurgency right is perhaps the most important intellectual challenge facing the Joint Force today. If we find ourselves in a war with a peer competitor, the centrality of insurgency will fade—but in the current era of increasingly contentious competition, effectively relieving or leveraging insurgency is key to nearly everything: from greater stability at home to reducing the threat of violent extremists abroad and more effectively deterring problematic acts of state competition. Getting insurgency right is indeed the proverbial nail, for want of which the kingdom might be lost.

CONTACT Robert C. Jones | robert.jones@socom.mil

The views expressed in this work are those of the author and do not necessarily reflect the views, policy, or position of the United States Government, Department of Defense, or United States Special Operations Command.

© 2025 Arizona Board of Regents/Arizona State University

In literature and doctrine, insurgency is a chameleon with a dozen names and infinite manifestations. Whether we call it “insurgency,” “insurrection,” “rebellion,” “revolution,” “resistance,” “instability,” “resilience,” “stability,” “civil resistance,” or even “violent extremist organizations,” we are ultimately describing shades of the same fundamental human dynamic. At its core, insurgency arises when a population, formed around a distinct identity, perceives itself to be in existential conditions of *legally irreconcilable political grievance*. An active insurgency occurs when that same population then acts illegally—under the laws of the government they are challenging—through violent or nonviolent means to address those conditions. Our world today is rife with both latent and active conditions of insurgency. The nation that best understands and addresses these conditions will hold the advantage in the current competition.

So, why is no one talking about insurgency? Frankly, we have moved on. State challengers like China, Russia, and Iran took full advantage of a United States distracted by the attacks of 9/11 to press their positions “around the edges”¹ of the empire. The Joint Force is now appropriately focused on deterring and, if necessary, confronting these major state actors. Meanwhile, insurgency has been tucked away, bundled into the much larger collective construct of *IW*.

One of the goals of this article is to clarify the role of *IW* as an organizing framework and highlight the critical importance of understanding, as clearly as possible, the fundamental nature of insurgency. This article is built around a proposed critical distinction between the nature of a problem and its character. One way to think about this distinction is that the nature of a problem encompasses everything that it must be—and nothing that it need not be. In 1905, Albert Einstein disrupted the world of physical nature by publishing works based on “thought experiments” rather than physical ones.² In thought experiments, he used his imagination to visualize how the variables in nature interacted with the constants to devise new theories to explain the challenges of our physical world. Here, we apply the same logic to human nature. If the constants of a problem constitute its nature, then the variables of the same problem provide its character. The doctrine and literature of the challenges associated with *IW* are heavily premised on the character, as historically, the application of overwhelming state power could typically shape the character of a situation into one deemed acceptable by the state. However, as the modern information age shifts relative power from states to populations, these character-based approaches are proving too difficult, costly, provocative, and fleeting. By first determining the distinct nature of a problem, we can better imagine how the variables of character might interact and then develop more accurate theories for understanding the myriad human dynamics within the family of challenges we call “irregular warfare.”

Let Us Be Clear: “Irregular Warfare” Is Not Something We *Do*; Irregular Warfare Is Something We *Made*

We are free to name and define manmade conceptual constructs like *IW* as we please. However, such is not the case with natural dynamics such as those found *within* *IW*. Fundamental human dynamics, such as insurgency, are rooted in the nature of mankind. These must be studied carefully, guarding against the pull of bias, emotion, and popular

trends. Ultimately, we must *understand* our way to greater success, but if we are not mindful, we run the risk of defining our way to failure. The Department of Defense (DoD) has redefined IW yet again, yet efforts to develop a more accurate understanding of the diverse human dynamics *within* IW remain largely unchallenged and unexplored.

IW is a bureaucratic fiction—but is it a useful one? To *know* the definitions³ of IW is a straightforward task. Over the past 20 years, the U.S. has paved a meandering path of definitions and doctrine to support this body of knowledge, and experts on IW abound. Yet, during this same era—guided, advised, and led by these experts—the U.S. has struggled mightily with a wide range of irregular challenges and adversaries. This is as true domestically as it is abroad and applies as much to state actors as to non-state actors. Clearly, a substantial gap remains between our knowledge of IW and our understanding of the diverse human dynamics bundled within. This is the gap between “the right answer” and “the good answer.” And in an era of unprecedented change, that gap between doing things right and doing things well has never loomed larger.

When creating a strategic construct, it should be simple, logical, necessary, and helpful to its intended purpose. It should provide a figurative table where diverse parties with shared problems but divergent missions can gather. It should stimulate new understanding, synergy, and opportunities for greater success. Unfortunately, IW has never quite met that standard. With the non-negotiable requirement that it be a form of *warfare*, the latest rendition of IW was purposely created *by* the DoD *for* the DoD. Rather than creating a table to gather around, it builds a wall that divides. Rather than fostering a greater understanding of the diverse dynamics within, it creates a false sense that IW is somehow a distinct entity unto itself.

The prescient challenge with IW lies in our understanding of the problems it seeks to address. These problems cannot be defined into submission, nor can our struggles in implementing IW solutions be redefined into success. Naturally occurring human dynamics are indifferent to what we wish them to be. Efforts to conform nature to bias are perhaps our greatest folly—and the central problem of conflicts inaccurately described as “endless wars the Generals can’t win.” These were not wars that could not be won; they were policies that could not be enforced. The essential failure occurred at the moments of decision but played out over decades of bloody, expensive, frustrating execution. A better understanding of underlying problems will inform better decisions.

Why? Because IW is not any one thing—it is a *collection* of things. While many of these share important characteristics, they vary tremendously in their *nature*. These nuances are becoming increasingly important, yet they are often ignored or misunderstood in doctrine. In a bygone era—prior to electronic communications, when much of our IW knowledge was formed—states could typically ignore and overcome these distinctions through the application of power and a monopoly on legal violence. And yes, through *warfare*. But that era has long since passed.⁴ In truth, this has not been the case for some time. Show me an “endless war the Generals can’t win,” and I will show you a situation where military power was applied in vain attempts to coerce a government or population into accepting policies or laws they deemed illegitimate, inappropriate, unjust, or intolerable. The inertia of outdated doctrine, literature, and experiences is strong, and we

have yet to fully grasp this modern reality: *where policy is impossible, all approaches are infeasible*. Our challenges are as much a matter of obsolete *direction* as they are outdated *definitions*. And in the military's "can do" culture, these two forces feed upon each other.

Evolving Conditions, Shifting Definitions

Rarely has the adage, "where one stands depends upon where one sits,"⁵ been more relevant than in the realm of IW definitions. This is reflected in the many redefinitions of IW by the DoD in recent years. For centuries, IW was simply warfare not conducted by regular forces. The DoD resurrected and repurposed the term to address the frustrations of the post-9/11 era.

In the early 2000s, we focused on the character of the contest at that time. In 2007, frustration set in, leading to the admission that "IW is a complex, messy, and ambiguous social phenomenon that does not lend itself to clean, neat, concise, or precise definition."⁶ By 2010, an attempt was made to impose a tighter framework, defining IW⁷ as "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)." This definition, like many before it, included embedded explanations: "Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will." At its core, IW was effectively defined as *a violent struggle for legitimacy and influence*.

By 2020, however, the emphasis on "violence" became problematic in the context of a new National Defense Strategy⁸ that emphasized "competition below armed conflict" and mandated the application of IW⁹ across every aspect of that competition. The solution was simple: delete the "violence" requirement. The new definition read, "Irregular warfare is a struggle among state and non-state actors to influence populations and affect legitimacy," while keeping the second sentence unchanged. At this point, IW was essentially everything—and therefore explained nothing. It was now framed as *a struggle to influence populations and affect legitimacy*. At this point, IW was beginning to sound more like *democracy* than warfare, while including both. The growing population within the Department of Defense who see everything as some form of warfare, and warfare as what the Department of Defense does, were unhappy with this definition. With the coming of a new administration, two things were made clear: IW would be redefined yet again, and any Pentagon definition of IW would emphasize the "warfare" aspect of the concept.

The latest effort to redefine IW is now complete. The *all is warfare*,¹⁰ and *warfare is all we do* contingent won out. Now, IW is "a form of warfare where state and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities."¹¹ Nearly every aspect of this definition raises cause for concern. It overstates the role of warfare, redundantly highlights the inclusivity of the concept, and artificially categorizes the ways in which IW must be conducted. To be fair, this definition will likely serve its intended administrative purpose. To take definitions like this literally for what they convey, however, is problematic. After 20 years of struggling with mis-framed problems, obsolete doctrine, and overly symptomatic solutions yielding

few durable, desired strategic effects, this is probably not the definition the nation needs to effectively address the challenges IW is intended to address.

Crossing the Rubicon: Not So Much Irregular as *Illicit*

We continue to struggle with the critical first step: identifying the problem. As a legitimate entity confronting illegal and often violent challenges, we carry an inherent bias. Viewing these challenges through a warfare lens naturally leads us to look for threats to defeat as a critical step to solving the problem. Too often, this results in waging warfare against symptoms while leaving underlying issues unaddressed—or worse, exacerbating them. We need to do better in understanding the challenges of IW.

The current landscape of IW challenges can be divided into four distinct categories: (1) transnational crime, (2) gray zone challenges, (3) insurgency-based challenges, (4) and terrorism. Each of these categories is fundamentally different by its nature but often overlaps or appears similar in character. Understanding these distinctions is critical for formulating the right strategic responses.

- **Transnational Crime:**¹² *Illegal for profit.* These activities, conducted by state or non-state actors, are illegal under the laws of the systems being challenged. Their primary purpose is for profit. Regardless of how violent or disruptive governance crime may become, it is not warfare or insurgency and cannot be resolved through warfare or counterinsurgency (COIN) approaches.
- **Gray Zone Challenges:**¹³ *Illegal to expand one's sovereignty.* These activities, conducted by state actors, are illegal under the laws of the systems being challenged. Their purpose is to advance sovereign privilege. When conducted legally, these challenges constitute competition, regardless of how frustrating they may be.
- **Insurgency-based Challenges:**¹⁴ *Illegal for politics.* These are population-based activities leveraged by state or non-state actors. They are illegal under the laws of the system being challenged.¹⁵
- **Terrorism:** *Illegal to coerce through fear.* These activities, carried out by discrete organizations or individuals, are illegal under the laws of the system being challenged. Their purpose is to generate fear to affect changes in law or behavior. Despite expansive lists of terrorist organizations, true terrorist entities are rare.¹⁶ Notably, organizations like al-Qaeda and the Islamic State are accurately classified as insurgency-based challenges rather than terrorism-based, as they wage unconventional warfare (UW) campaigns reliant on preexisting insurgencies.

Most of these challenges do not manifest as warfare, nor are their methods particularly irregular. However, these activities are problematic to U.S. interests and security, and the DoD must remain prepared to counter such activities.

To frame challenges accurately, we need to explore better questions. The nature of a challenge should drive policy and strategy, whereas its character (symptoms) should inform effective tactics. Certain questions are essential for understanding the nature of problems. When faced with a new situation, we should ask ourselves a series of framing questions:

- How much does this issue threaten or advance U.S. interests?
- Is this challenge legal under the laws of the system being challenged?
- Is this conflict within a single system of governance or between two or more?
- What is the primary purpose for the challenger(s)'s actions?
- What are the relationships between the parties?
- Are the laws and norms being violated necessary and just?
- What are the critical identities relevant populations are forming around?
- Have recent events shifted the priority of identities in significant ways?
- Do affected populations recognize both the legitimacy and character of the governance affecting their lives?
- How do populations feel about the governance affecting their lives and whom do they blame and/or credit?
- Do affected parties believe they have trusted, legal, and effective mechanisms to address their grievances or interests?

By asking better questions, we can more accurately classify and understand IW challenges to set the conditions for arriving at better answers.

A Pragmatic Alternative: An Alternative Definition and Recommendations

In pragmatic terms, IW is perhaps best understood as *a collection of problematic, illicit challenges deemed important by the Department of Defense and their legitimate solutions*. This perspective removes loaded, subjective words like “warfare” or “legitimacy” and instead focuses on the single, common aspect of the four distinct types of challenges bundled under the IW banner: *legality*—or, more accurately, their *illegality* under the laws of the system being challenged.

Shifting the focus to illicit activity moves attention away from a particular threat or preferred solution, opening the door to a more holistic and effective analysis of the fundamental problems at hand. The military is no longer a “hammer” that has preidentified “nails” with an implied leadership role. Instead, the military becomes a tremendous source of resources and capabilities, postured to support and advance U.S. national interests in this era of restive peace. Viewed through this lens, the following recommendations emerge:

- Shift the focus from the problematic symptoms labeled as “threats” and work to better understand the fundamental nature of the problems driving the current surge in illicit challenges.
- Clearly communicate that collectively, IW is much more an administrative construct than an operational one. IW ensures that the DoD remains prepared to assist in addressing illicit challenges today while maintaining the readiness to fight and win in potential future conflicts.
- Emphasize that most of these challenges are rarely acts of war and cannot be resolved through the application of warfare. These are not threats to “defeat,” nor are these conflicts to “win.” The primary role of the military is to help create time and space for relevant authorities to make appropriate adjustments, provide additional capacity where requested, and help deter, mitigate, and disrupt high-end illicit violence.
- Clarify that, outside the context of formal war, effective IW solutions are typically led by agencies other than the DoD or by other nations. The U.S. military does not “wage” IW; it conducts IW activities.

To this end, we must, to the best of our abilities, attempt to understand the implications of this rapidly evolving strategic environment—particularly, how these changes are shaping the character of competition and conflict. Most importantly, we must ensure that we understand the *nature* of the unique challenges we face.

What is nature? *The nature of a situation is a capture of everything it must be, and the release of everything it need not be.* However, determining the nature of a problem is not a reductionist process, it is a refining one. A refined understanding, free of unnecessary character-based impurities, serves as the foundation for durable, simple, and effective strategic concepts. Ultimately, all these challenges are human dynamics, and as such, like warfare, their strategic nature is rooted in human nature. The best safeguard against institutional, emotional, and situational bias is a clear understanding of the distinct and fundamental nature of various types of challenges. There is no substitute for getting the problem right from the outset. Why? Because standing in the emotional wake of events like 9/11, January 6, or October 7 is not the time to craft unbiased understanding or develop measured, effective responses given the outrageous character of what has occurred.

We stand at a historic inflection point, living in an era of unprecedented change where the advantage currently lies with the revisionists. Unlike the United States, which is wedded to sustaining a waning and increasingly challenged status quo, our revisionist adversaries recognize the opportunities inherent in the emergent strategic environment far better than we do. They intentionally dodge hard “red lines” and seek to provoke predictable responses to validate their narratives and advance their respective causes. When we cling to flawed or obsolete perspectives on the challenges we face, we accelerate our own decline. We must shift our efforts from redefining our solutions to reframing our problems. Once a problem is clear, new solutions will naturally follow.

Legitimate Solutions: Our Current Menu of IW Activities

Once we have identified the problems, we can then turn to the family of solutions. The latest version of IW includes a set of IW activities—each akin to musical notes that must be arranged and orchestrated to fit the nature and character of the problem at hand. Nuance is everything, and it begins with a fundamental understanding of the problem. Only once the problem is understood, and its objectives are clear and feasible, can we begin to design a campaign that purposefully orchestrates these activities. To say one “conducts irregular warfare” is a dangerous oversimplification—but we absolutely conduct IW *activities* and those must be tailored in ends, ways, and means for modern realities. These activities include:

1. Civil Affairs Operations (CA)
2. Counter Threat Network
3. Security Cooperation
4. Counter Threat Finance
5. Security Force Assistance (SFA)
6. Civil-Military Operations
7. Military Information Support Operations (MISO)
8. Counterinsurgency (COIN)
9. Counterterrorism (CT)
10. Foreign Internal Defense (FID)
11. Stability Operations
12. Unconventional Warfare (UW)

Each of these activities is defined and described in U.S. military doctrine. In this era of tremendous change, doctrine will naturally lag behind reality. Just as governments everywhere struggle with the friction of a governance gap, so too do militaries everywhere suffer from a doctrine gap. If our understanding of insurgency is indeed flawed, then the way we think about nearly all of these activities is flawed as well. Now is the time to ensure we understand the problems we seek to address in the most fundamental terms possible, by their respective natures. This will then allow us to tailor our activities to mitigate the problematic symptoms surrounding these problems while patiently advancing durable, desired solutions.

The Pursuit of Understanding

Figuratively speaking, the old playbook is obsolete. Throughout recorded history, nations have employed their power to exercise some degree of control over the people and places where they perceived their interests to lie. They aligned with, coerced, bought, or created governments willing to prioritize those foreign interests over those of their own people—and then protected those governments against all challengers, foreign or domestic. We think of ourselves as “exceptional,”¹⁷ but this distinction lies more in the character of our actions than in the nature of our approach. The character of one’s actions can soften the sting and mitigate the response, but it is the nature of those actions that shape the nature of the response. For example, until we can appreciate how the failed U.S. involvement in

Afghanistan shares fundamental similarities with the failed Soviet involvement in the 1980s, we will learn little from our experience. Some argue that we need to execute the old playbook more vigorously.¹⁸ Certainly, we have the power to force our will upon whomever we please, but is that the nation we imagine ourselves to be? Instead, we need to understand why modern efforts fall short, and adjust our ends, ways, and means accordingly.

The definition of “winning,”¹⁹ for most irregular problems has traditionally been defined as defeating a bad actor while ensuring challenged governments remain in power, unchanged, and uncoerced. This is not solving the problem; this is merely suppressing the symptoms. It is a measure of success drawn from 500 years of Western colonialism. Once success is framed in this context, it is natural to fixate on the problematic symptoms rather than the deeper causes. What was once, literally, “good enough for government work,” is no longer adequate to serve our interests at home or abroad. In fact, the pursuit of some degree of control has become an expensive, provocative, and unnecessary liability. The good news is that we can serve our interests far more effectively through relative positive influence, and the rules-based order advanced by the U.S. is uniquely suited to an influence-based approach. However, the bad news is that our current toolkit of IW activities is built on obsolete understandings of the problems they were designed to address. These tools are overly employed to create degrees of control rather than to foster shades of influence. If we are to remain effective in the modern era, we must update our toolkit, as well as our playbook.

A Hypothesis and Some Insights

A decade ago, when General Joseph Votel was the Commander of the United States Special Operations Command (USSOCOM), he faced a problem. With a growing gray zone challenge facing the nation, he had to find a way to shift Special Operations Forces (SOF) engagement to be less reactive. The challenge, however, was how to validate shifting efforts to the “left of bang” when the Special Operations Forces were already operating at full capacity—100 percent committed right of bang while meeting 50 percent of operational requirements. It was in this environment that Doctor Tom Nagle and I prepared the Strategic Appreciation²⁰ signed by General Votel in 2015. To achieve better answers, we needed to ask better questions. We needed a new theory of the case.

Our hypothesis was simple: we were living in an era of rapidly shifting power while wrestling with the friction caused by slowly adjusting policies, governance, and redistribution of sovereign privilege. In simple terms, *we were in a governance gap*. The resultant grievances from these perceived imbalances were creating a growing energy for conflict both within and between states. These challenges were as old as humankind, but in the modern information age, the speed, scope, and scale were unprecedented. Traditional approaches were proving too controlling, more provocative, and less effective. Governments everywhere were struggling to adapt, and revisionist actors saw opportunities where status quo actors saw threats. To get in front of these problems we had to think like a revisionist.

Thinking like a revisionist and conducting “thought experiments,” I have come to the following insights on population-based conflicts. Many of these perspectives challenge long-held positions and are difficult to prove correct—but they could easily be proven wrong if flawed. They are presented here for consideration, discussion, and challenge. These insights also inform the attached chart (see Figure 1) and are shaped, but not constrained, by U.S. military doctrine, professional literature on insurgency, and my experience as a Special Operator.

1. *Conflict within a single system is fundamentally different from conflict between two or more systems.* This distinction is a function of the relationships between the parties. War theory is rooted in conflicts between two or more systems and is largely sound. Where we run into trouble is applying war theory to non-war problems, particularly those occurring within a single system of governance, where relationships endure. Revolutionary insurgency, for example, may look like warfare by its character, but by its nature, internal revolution is more akin to *democracy*, albeit *illegal* democracy. While perhaps violent, it is an expression of democracy all the same. Revolutionary symptoms can be suppressed through warfare, but the drivers of revolutionary problems are invariably made worse by such efforts. Fully appreciating this single point of understanding is arguably the keystone to resolving most of our IW challenges.
2. *Population-based challenges are like water.* The character of water can be gas, liquid, or solid within a very narrow range of conditions. The same is true of challenges rooted in a population perceiving itself to be in legally irreconcilable political grievance. These conditions can shift rapidly in character—ranging from artificially stable to active illicit challenges to full-scale civil war. It is far easier to change the character of the conflict than it is to resolve the nature of the problem—particularly when solutions are designed to treat the population’s symptoms rather than addressing governance as the primary cause.
3. *The vast majority of IW is a derivative of insurgency.* Our doctrine and literature on insurgency are a collage of loose terms and overly descriptive definitions, replete with gaps and overlaps. We describe how things look, rather than seeking to understand what they are and why they occur. The heavy bias of colonialism and the outrage of governments and populations facing illegal, often violent challenges have historically cast the state as the victim, rather than the provocateur.²¹ Getting to a better understanding of the nature of insurgency is the most vital task for improving our ability to resolve irregular problems or implement irregular campaigns of our own.

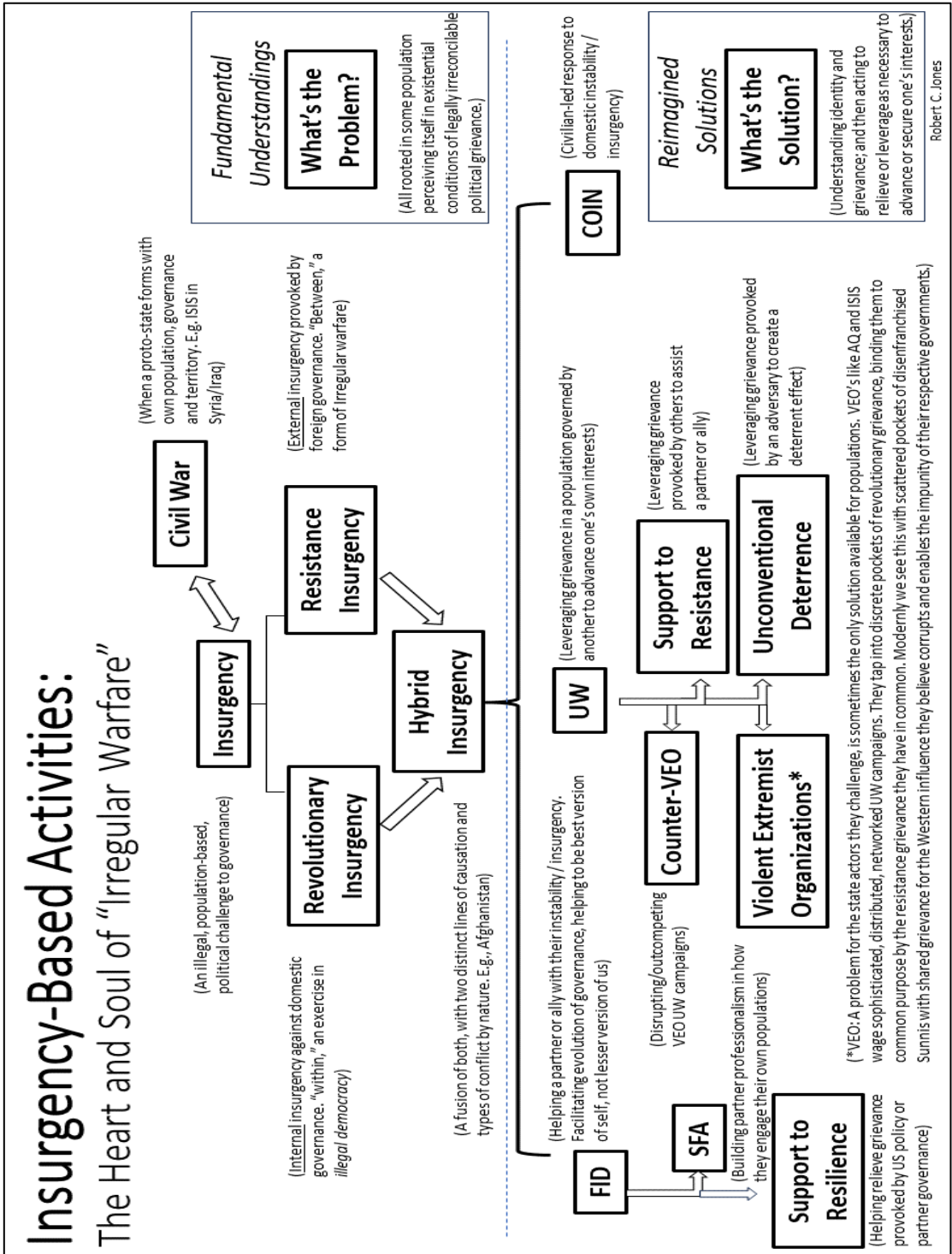


Figure 1: Insurgency-Based Activities

Some Insights on Insurgency

If one looks at insurgency in the way framed above, certain things become clear. First, *all insurgencies must possess the following three characteristics: illegal under the laws of the system being challenged; primarily political in purpose; and population-based in nature.* Though the character of insurgency takes on myriad forms, they fundamentally fall into two distinct types (along with a hybrid form):

- a. *Revolutionary insurgency*: Internal to a single system of governance and therefore best understood and addressed as an act of *illegal democracy*. If war is the final argument of kings, then revolution is the final vote of the people. Revolution is *within*. Perhaps the most critical insight for IW may be this: the only fundamental difference between revolutionary insurgency and democracy is legality!
- b. *Resistance insurgency*: Insurgency provoked by external sources of governance, and therefore a form of *irregular war*. Resistance is *between*.
- c. *Hybrid insurgency*: A fusion of revolutionary and resistance causation and reaction among the same populations. This demands recognizing *both* distinct problems in forming policy and solving for each in strategy. Tactically, it all looks the same on the ground. To solve for only one is folly (e.g., Afghanistan, 2001-2021).
- d. *Center of Gravity*: The driving energy behind insurgency is a population perceiving itself in existential conditions of legally irreconcilable political grievance. Understanding causation allows for early assessment of a population's relative resilience or exploitability long before conflict exists. A greater appreciation of political grievance allows governments to proactively reduce unnecessary provocations and foster natural stability.²²
- e. *Ideology*: A critical requirement to enhance, direct, or accelerate grievances, but is rarely causal in and of itself. An effective ideology speaks to the culture and grievances of the target population(s) and takes positions the challenged government(s) are unable or unwilling to adopt. (Therefore, the most effective way to disempower an insurgent narrative is not to "counter" it, but rather to agree with the rational aspects, incorporating them into one's own narratives and actions.)
- f. *Character*: Variable factors, such as geography, history, culture, the use of violence, the type of ideology employed, and the stated goals of the insurgent group all appear to be merely aspects of the character of an insurgency. These factors are important for refining tactics but are largely irrelevant in determining the nature of the problem at hand, or in shaping feasible policies or effective strategies.
- g. *Civil War*: Too often linked to the scale of a conflict or the degree of violence, civil war begins when a proto-state emerges from insurgency with its own

territory, population, governance, and security. This is the “ice” (solid) form of insurgency. To defeat the character of a civil war by deconstructing the proto-state, simply convert the conflict back to “liquid” (active insurgency) or “gaseous” (latent insurgency) forms—e.g., The Islamic State in Syria/Iraq.

- h. *Winning*: For a challenged government to truly win, it must address the governance factors driving the insurgency. Historically, focusing on defeating the insurgents while preserving an unchanged status quo has merely suppressed the symptoms of insurgency rather than resolving its root causes, an approach rarely viable in the modern information age. This is a lesson the U.S. should have learned from its post-9/11 misadventures, and one that Israel needs to strongly consider today as they respond to the attacks of October 7, 2023. While insurgents can win at any point in the contest if they can coerce the challenged government to change, a government can only win once it evolves sufficiently to bring grievance and trust within manageable norms.
- i. *Popular Legitimacy*: This is the recognition of a governing authority’s right to affect people’s lives. This is perhaps the most significant factor in the cure/cause of insurgency. U.S. doctrine overly fixates on *legal* legitimacy, which is the recognition of a government by external institutions and actors. This has been a particularly problematic issue for the U.S. in recent conflicts. Believing the foreign governments, we attempt to create and protect are *legitimate*, rather than appreciating them as *collaborative*, has blinded us to the infeasibility of policy decisions for regime change or nation-building. The reality is that any government born of a foreign power is *de facto* illegitimate—making it a natural target for revolutionary insurgency. Likewise, our own efforts as foreign actors are equally *de facto* provocative of resistance insurgency towards ourselves. While our valid motivations for engaging in such behavior, our good intentions, and efforts to avoid excessive violence and collateral damage are noble – it is the nature of our actions that drove the nature of the affected population’s response.

On the bottom half of Figure 1, proposed reimaged solutions are presented. Here, I apply the fundamental understanding of insurgency, as captured in the upper half of the figure, to the goals and guidance of our most recent strategic documents—all within the context of the modern information age. Viewed in this manner, IW—particularly the insurgency-based aspects of irregular warfare—becomes a powerful array of activities for advancing and securing interests in competition, as well as deterring gray zone challenges and major conflicts. These break out under three major headings: Foreign Internal Defense (FID), Unconventional Warfare (UW), and Counterinsurgency (COIN).

Historically, FID has been focused on preserving a partner government or keeping an ally in power, typically over the objections of a significant segment of its own population. This approach, straight out of the old colonial playbook, is premised on maintaining control to preserve foreign governments in power we see as favorable to our interests. However, in today’s modern world, this has been an increasingly expensive, confrontational, and unnecessary provocation. FID to control foreign political outcomes is nearly fully obsolete

in the post-Cold War era. Moving forward, FID must be more about fostering positive influence, respecting sovereignty, and promoting self-determination. It should be focused on empowering partners to become better, more inclusive versions of *themselves*—not lesser versions of us.

Additionally, SFA has historically sought to foster durable relationships through training, equipping, and advising foreign military. Yet, when conducted in developing countries, this approach too often resulted in creating smaller, lesser versions of U.S. forces that tended to be culturally unsuitable and fiscally unsustainable. When these forces were crafted for governments lacking a broad writ of popular legitimacy, they rarely possessed the fighting spirit of the insurgent forces they were meant to counter. One observation from Operation Enduring Freedom–Philippines was the power of respecting host nation sovereignty and focusing on improving the relationship between security forces and the populations they encounter. Our SFA efforts, severely constrained by narrow authorities, permissions, and funding, forced us to be more strategic than we otherwise wanted to be.²³ It turns out that showing a greater respect for the sovereignty of the host nation forced us to empower, rather than transform, thereby reducing the resistance-producing provocations of our efforts. Simply improving the professionalism and character of the interactions between Philippine security forces and the populations in remote areas soon resulted in dramatic improvements in the stability of the region.

There is also support to resilience. Historically, resilience efforts have tended to focus on basic human needs, and while this remains a vital area of assistance, moving forward, we must be far more attuned to political resilience. The former relates more to the lower half of Maslow’s Hierarchy of Needs, while the latter aligns with the upper half. Improving our understanding of the fundamental nature of insurgency allows us to more accurately assess whether a population is resilient or exploitable and adjust our efforts accordingly. Invariably, the political resilience of a society is far less about the conditions in which a population lives and far more about how they feel about living in those conditions—and whom they blame for their situation.

Next up is COIN. Our COIN successes are typically fleeting at best, and our COIN failures are humiliating disasters of epic proportions. Why? Because we relied on flawed and obsolete perspectives and applied the same term—“COIN”—to the activities of both the host nation and the external nations or forces involved. This may seem like a minor point, but the negative consequences of this conflation of roles cannot be overstated. When the roles are conflated, it is far too easy for a more capable external power to take an inappropriate leading role. This subjugation of the host nation invariably serves to validate the grievances of the relevant populations, amplify the narratives of the insurgent or UW organizations supporting those populations, and foster resistance energy towards the external power.

This is precisely why COIN is best thought of as a civilian-led, domestic operation, in which the role of the military is the same as in any civil emergency: to be last in and first out; to provide the necessary extra capacity; to never supplant civil authorities; and to always remember there is no military victory to be had. The military serves primarily to mitigate and disrupt the high end of violence and to help create the time and space civil

authorities need to adjust their governance, as necessary, to reduce provocations and restore order. Foreign powers do not conduct COIN, they conduct FID and must do so in a manner designed to foster positive influence, always careful not to provoke resistance or inadvertently enhance revolutionary grievances against the host nation.

UW – Leveraging Insurgency for Purpose

Perhaps the most misunderstood activity of all is UW. The reasons for this misunderstanding fall primarily on the special operations community. We have become so enamored with and trapped by our historical applications of UW that we struggle to free our understanding from the artificial constraints imposed by that bold history. While there are a handful of variations of the UW definition, they typically involve several artificial constraints drawn from historical examples, such as those in occupied Europe during WWII or the bold “horse soldiers” who leveraged the Northern Alliance to topple the Taliban government in Afghanistan. The standard components of these definitions focus on activities occurring in a denied space, working with some blend of local underground, auxiliary, or guerrilla organizations, and efforts to coerce or overthrow adversary regimes. But UW is far more than just supporting a resistance or revolutionary insurgency.

To fully appreciate both the challenges and opportunities of UW, we must first free this concept from unnecessary factors of its historic character and come instead to understand it in terms of its fundamental nature. *We must capture everything it must be and release everything it need not be.* UW is perhaps the most powerful tool in our IW activities tool kit and is simply, fundamentally, naturally, just this: ***UW is any activity designed to leverage the legally irreconcilable political grievance in a population governed by someone else, to advance one’s own interests.***

There is no adversary approach more frustrating to the U.S. in the post-Cold War era than the modern application of UW. The Russians employed UW when they seized Crimea without a fight and again through its use of social media to inflame political grievances, shape elections, or foster instability in the United States. Both al-Qaeda and the Islamic State have waged UW since their respective inception. Iran conducts UW in their support of Hamas in Gaza or the Houthis in Yemen. Yet, none of these adversaries care a whit what our special operations doctrine writers or senior leaders wish our nostalgic vision of UW to be. Our definitions and doctrine have become a trap we have built for ourselves and willingly climbed inside. The certainty of our knowledge blinds us to the unconstrained approaches applied with tremendous success by our adversaries. We are trapped by the “right answer,” while alternative approaches are in practice all around us.

One such alternative approach is *unconventional deterrence*.²⁴ In simple terms, this is posturing to create a credible threat of UW in the mind of an adversary. Traditional approaches to deterrence are of little use in deterring the illicit “gray zone” acts of competition that erode the sovereignty of important partners and allies and undermine the credibility of the rules-based international order. However, illicit competition and the corruption it fosters are also powerful sources of legally irreconcilable political grievances that SOF is uniquely trained to identify and leverage. This capability can be used to help an at-risk partner foster greater resilience or to create uncertainty in adversaries about SOF’s

abilities to destabilize dozens of global efforts they see as essential to their ambitions. By freeing UW from its artificial constraints, we empower SOF to create new lines of deterrence. These new forms of irregular deterrence help shrink the gray zone and integrate into broader deterrence strategies designed to reduce the risk of war.

Labeling organizations like al-Qaeda or the Islamic State as “terrorist” groups is perhaps our greatest modern example of framing a problem for how it looks, rather than for what it is. By recognizing that these Violent Extremist Organizations (VEOs) are most accurately illegal, non-state political action groups, waging sophisticated, distributed, and networked approaches to UW (and yes, employing terrorist tactics), we free our minds to craft new and more promising solutions.

VEO campaigns are wholly reliant upon hybrid insurgency. This involves a combination of populations desperate for help in addressing their revolutionary grievances with domestic governance, then uniting around common resistance grievances against foreign governance. Recognizing the nature of this problem empowers us to shift our focus from the problematic symptoms associated with these campaigns, focusing instead on solving the actual problems of obsolete and inappropriate policies and governance. We must disrupt these campaigns and mitigate their violence—but do so in ways that create time and space for civil authorities to address the policy and governance failures that resistance and revolutionary insurgency-based VEO UW campaigns exploit. We must create better narratives, rather than simply countering theirs. A key approach is to co-opt effective elements of the VEO narrative while presenting a superior alternative. Lastly, we must outcompete these organizations as the partner of choice for advancing the evolution of better and more inclusive governance for disenfranchised populations around the planet. We must *counter* their UW campaigns, not just their terrorist tactics.

One powerful way to improve IW, therefore, is to reframe and expand UW. Ultimately, whether one is conducting UW to coerce or overthrow some adversary; create new lines of deterrence; become more strategically effective in dealing with VEOs; or foster resilient populations at home and abroad, these actions are all rooted in insurgency and variations on a fundamental perspective of UW.

Special Warfare – That Distinct Subset of Irregular Warfare Unique to SOF

Competition is the framework for a whole-of-society effort to advance and secure our national interests. Irregular warfare nests within this framework as a responsibility of the entire Joint Force. One way to appreciate the role of SOF is to view special warfare as a distinct subset of IW. To be clear, special warfare is not a form of warfare, *per se*, but rather a mechanism for clarifying roles, missions, and activities appropriately tasked to our Special Operations Forces from those better executed by conventional forces or other entities.

From inception, USSOCOM was directed by law to focus only on certain activities “in so far as it relates to special operations.”²⁵ Joint Doctrine clarifies this mandate by explaining how “special” is situational and rooted in a unique set of conditions that must combine to make any activity a “special operation.”²⁶ This is enlightening on several levels.

First, no operation is inherently “special” simply because of the character of the unit performing the task or the type of task being performed. Secondly, this perspective challenges the idea that the conventional force somehow became “more SOF-like” during the post-9/11 era. As missions traditionally assigned to SOF units expanded to the rest of the Joint Force, it was SOF that inadvertently became more conventional, rather than the other way around.

By the time the U.S. left Afghanistan, SOF had evolved, taking on a hyper-conventional focus. We were far more focused on threats than problems, and our population-based roots had atrophied. USSOCOM was giving the nation the SOF it wanted, but were we giving the nation the SOF it needed? Even today the demand signal from our nation’s capital remains weighed toward the hyper-conventional. The challenges in breaking this inertia of expectations are significant. Yet, the question facing USSOCOM today is: What modern roles, missions, and activities are not only “special” but also relevant to addressing emerging challenges and serving current strategic guidance? Reshaping and refocusing our SOF presents challenges wholly distinct from the one of reimagining irregular warfare, but ones also demanding a firm grasp of the fundamental nature of the problems facing our nation and the world.

Conclusion

To be clear, man-made, administrative constructs like “integrated deterrence” or “irregular warfare” are all vitally important to the defense community. They help highlight challenges and organize our thinking. But when we create these constructs, they must be accurate, simple, and helpful for their intended purposes. We must also remain humble in our thinking and pragmatic in our actions. Too often we lose sight of this—particularly when the challenges before us appear overwhelming and unresponsive to our efforts. This is why we must strive to see through complexity and understand the fundamental aspects of these challenges. These are challenges that cannot be defined into submission, nor do they care a whit about our biases, fears, or preferences. They simply *are*, and we have a duty to understand them for what they are and address them accordingly. In the current environment—in the current era of competition—the most important human dynamic to understand accurately is that of “insurgency.” This is truly that proverbial nail, for want of which the kingdom might be lost.

Insurgency is a dynamic with many closely related cousins. Here, I write for the defense community in the context of irregular warfare, so I focus on the insurgency variant. If writing for other audiences, I could just as easily focus on *resilience* or *political stability*. Ultimately, we look at similar problems, describing them in differing terms, but we must understand them for what they truly are. When people perceive themselves to be in existential conditions of legally irreconcilable political grievances, a force for instability grows within them. These conditions cannot be wished or defined away or solely attributed to our adversaries—but they are conditions we can understand, resolve, or leverage for purpose.

Governments around the world are struggling with the growing challenge of populations, formed around discrete identities, perceiving themselves as trapped in

conditions of legally irreconcilable political grievance. When these conditions exist, the exploiters of grievance will emerge. Armed with clever narratives designed to raise those perceptions to existential levels, these exploiters seek to mobilize at-risk populations for malign purposes. It is natural to cast blame, perpetuate victimhood, and seek to punish, suppress, or defeat the actors, rather than to defuse the conditions. After all, the state will always be the legal actor and has the right and duty to enforce the rule of law. However, shifting blame and attacking only the symptoms primarily serves to validate exploiters' narratives and deepen the population's grievances. In the past, suppression of symptoms was often good enough. Increasingly, it is not.

Perhaps the greatest obstacle in getting *good* answers to modern challenges is the guardians of the *right* answers derived from pre-information age experiences. Recently, when General Fenton suggested that USSOCOM's contribution to a comprehensive scheme of integrated deterrence included fostering new lines of *irregular* deterrence,²⁷ it sent Pentagon staff officers scrambling for their military dictionaries. Because it was not in "the book," the concept was dismissed and left to wither. It is time to challenge "the book." It is time to re-examine long-standing assumptions—ideas believed to be facts—and question whether they are merely calcified assumptions colored by the biases of a bygone era. As the modern information age shifts the balance of power, new truths are being revealed, and many old practices are rendered obsolete.

At no time in history has there been a larger gap between the "right answers" of the past and the "good answers" needed for the future. This is particularly true in the inherently human dynamics of governance, competition, and conflict. Now is not the time to draw false comfort from doctrine and definitions. Now is the time to understand how the current information age is affecting the character of these dynamics and to craft new approaches that foster stability, which increasingly eludes our efforts. Ultimately, human dynamics are shaped by human nature and played out across countless scenarios—indifferent to what we wish them to be or what side we are on. Make no mistake: the challenges and solutions bundled within IW are incredibly important. We have a new definition but let us be clear-eyed about the work that remains. Now is the time to shift our focus to understanding problems for what they are—and to designing and applying solutions that will produce the results our security and interests demand.

Endnotes

- ¹ Admiral Eric T. Olson and Michele Flournoy, “Back to the Future: Resetting Special Operations Forces for Great Power Competition,” Podcast, Irregular Warfare Initiative, 2020.
- ² Norton, John (1991), “Thought Experiments in Einstein’s Work,” in Horowitz, Tamara; Massey, Gerald J. (eds.), *Thought Experiments in Science and Philosophy* (Maryland; Rowman & Littlefield; November 1991), 129–148. Archived from the original (PDF) on 1 June 2012.
- ³ Jared M. Tracy, “From “irregular warfare” to Irregular Warfare – History of a Term,” *Veritas*, Vol. 19, no. 1, (2023), https://arsof-history.org/articles/v19n1_history_of_irregular_warfare_page_1.html.
- ⁴ Lawrence Korb, “The Real Reason We Can’t Win Wars Anymore,” *National Review*, 21 March 2021, <https://news.yahoo.com/real-reasons-u-t-win-103057654.html?guccounter=2>.
- ⁵ Rufus Miles, “The Origin and Meaning of Miles’ Law,” *Public Administration Review*. 38 (5): 399–403, September 1978.
- ⁶ IW Joint Operating Concept (JOC) 1.0, 2007.
- ⁷ “Irregular Warfare: Countering Irregular Threats,” *Joint Operating Concept*, Version 2.0, 17 May 2010, https://www.jcs.mil/portals/36/documents/doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.
- ⁸ “Summary of the 2018 National Defense Strategy of the United States of America – Sharpening the American Military’s Competitive Edge.” <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>
- ⁹ “Summary of the Irregular Warfare Annex to the National Defense Strategy,” 2020. <https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF>
- ¹⁰ Micah Zenko, “How Everything Became War: A Conversation With Rosa Brooks,” *Council on Foreign Relations*, 7 November 2016, <https://www.cfr.org/blog/how-everything-became-war-conversation-rosa-brooks>.
- ¹¹ Joint Publication 1, Vol 1: *Joint Warfighting* (CJCS, August 2023).
- ¹² U.S. Department of Defense, *DoD Counter-Drug and Counter-Transnational Organized Crime Policy*, DoD Instruction 3000.14, (Washington, D.C.: Department of Defense, 2020) <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/300014p.pdf?ver=2020-08-28-112340-617>.
- ¹³ Summer Myatt, “2022 National Defense Strategy to Prioritize Gray Zone and Hybrid Warfare Plan, Optimized Data Sharing,” *GovConWire*, 25 January 2022, <https://www.govconwire.com/2022/01/2022-national-defense-strategy-to-prioritize-gray-zone-hybrid-warfare-and-data/>.
- ¹⁴ Joint Chiefs of Staff, *Counterinsurgency*, JP 3-24 (Washington, D.C.: Joint Chiefs of Staff, April 2008), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_24.pdf?ver=giaAj5fgP4SGt_BdkOrkNA%3d%3d.
- ¹⁵ Robert C. Jones, “Deterring ‘Competition Short Of War’: Are Gray Zones The Ardennes of Our Modern Maginot Line of Traditional Deterrence?” *Small Wars Journal*, 14 May 2019. <https://smallwarsjournal.com/index.php/jrnl/art/deterring-competition-short-war-are-gray-zones-ardennes-our-modern-maginot-line>
- ¹⁶ Terrorist Designations and State Sponsors of Terrorism - United States Department of State <https://www.state.gov/terrorist-designations-and-state-sponsors-of-terrorism/>
- ¹⁷ Mary McMahon, “What is American Exceptionalism?” *United States Now*, 6 November 2023, <https://www.unitedstatesnow.org/what-is-american-exceptionalism.htm>.

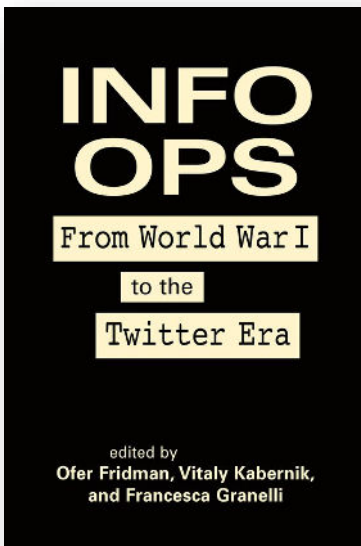
- ¹⁸ Jacqueline L. Hazelton, “Book Excerpt, ‘Bullets Not Ballots, Success in Counterinsurgency Warfare,’” *Military Times*, 17 May 2021, <https://www.militarytimes.com/opinion/commentary/2021/05/17/book-excerpt-bullets-not-ballots-success-in-counterinsurgency-warfare/>.
- ¹⁹ Christopher Paul, Colin P. Clarke, and Beth Grill, “Victory has a Thousand Fathers: Success in Counterinsurgency,” Rand Corporation, <https://www.rand.org/pubs/monographs/MG964.html>.
- ²⁰ United States Special Operations Command, “Strategic Appreciation,” 2015, <https://drive.google.com/drive/folders/0BzrcfrqF8zFVUXMydGUydWgzeVU?resourcekey=0-GmUIIUGWEp9LxmI4VL9u3w>
- ²¹ Joint Publication 3-24, “Counterinsurgency,” 25 April 2018.
- ²² Robert C. Jones, “Lies, Damn Lies and Assessments,” pp. 9-17, Strategic Multilayer Assessment White Paper “What Do Others Think and How Do We Know What They Are Thinking?,” Joint Staff J39, March 2018.
- ²³ David P. Fridovich and Fred T. Krawchuk, “Special Operations Forces: Indirect Approach,” *Joint Forces Quarterly*, 2007.
- ²⁴ Robert C. Jones, “Strategic Influence: Applying the Principles of Unconventional Warfare in Peace,” Strategic Multilayer Assessment, Joint Staff J39, June 2021.
- ²⁵ U.S. Code Title 10, Section 167: “special operations activities include each of the following insofar as it relates to special operations.”
- ²⁶ Joint Chiefs of Staff, *Special Operations*, JP 3-05 (Washington, D.C.: Joint Chiefs of Staff, July 2014), GL-11, https://irp.fas.org/doddir/dod/jp3_05.pdf. Special Operations is defined as “Operations requiring unique modes of employment, tactical techniques, equipment and training, often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk.”
- ²⁷ Katie Crombe, Steve Ferenzi and Robert Jones, “Integrating Deterrence Across the Gray - Making it More Than Words,” *Military Times*, 8 December 2021, <https://www.militarytimes.com/opinion/commentary/2021/12/08/integrating-deterrence-across-the-gray-making-it-more-than-words/>.

BOOK REVIEW

***Info Ops: From World War I to the Twitter Era* Edited by Ofer Fridman, Vitaly Kabernik, and Francesca Granelli**

ISBN 9781626379954, Lynne Rienner Publishers, 2022. 287 pages, \$38.50

Reviewed by: **James F. Slaughter**, Marshall University, Huntington, West Virginia, USA



Info Ops discusses and debates the nature and evolution of information warfare from the early twentieth century to the present conflict between Israel and Hamas in Gaza. Following the introduction by the editors, the work is divided into four sections: Formation, Evolution, Adaptation, and Conclusion. The framework of the book is well-structured, easy to follow, and flows smoothly, allowing readers with any level of knowledge on the subject to engage with relative ease.

In Part I: Formation, Ofer Fridman discusses "British 'Front Propaganda' in World War I," Vitaly Kabernik examines "Soviet Information Operations in World War II," and Aidan Winn explores "Inducement Strategies in the Vietnam War." In all three instances, the authors analyze the creation and structure of information (read: propaganda) campaigns designed to affect both civilian and military attitudes toward various war

efforts. They detail the efforts to create an information machine that produces quantifiable results, as well as the difficulties of developing information warfare tools in an age of rapid media expansion, increased literacy, and widespread access to technology that spreads media faster and further than ever before. These tools served as both offensive and defensive weapons beyond the battlefield.

In Part II: Evolution, Igor Orlov and Mikhail Mironyuk discuss "Soviet Propaganda in the War in Afghanistan, 1979–1989," Brett Boudreau examines "NATO's Information Campaigns in Afghanistan, 2003–2020," and Vitaly Kabernik, Igor Orlov, and Mikhail Mironyuk analyze "Russian and Georgian Operations in South Ossetia, August 7–12, 2008." These chapters explore the challenges of evolving information warfare, particularly in complex environments where domestic audiences are easier to reach, while foreign targets with vastly differing socio-cultural backgrounds present greater difficulties. The authors discuss the challenges of balancing military operations with information operations in both planning and execution. Additionally, they consider the role of civilian media in an

age of near-instant dissemination and feedback, as well as the rapidly evolving state of technology.

In Part III: Adaptation, Michael Milstein discusses " Hamas's Strategy Against Israel: From Information Ops to Influence Ops," while Roy Schulman and David Siman-Tov examine "Israel's Information Operations in Gaza: The Rise of the Digital Age." This section presents cutting-edge developments beyond speculation. The authors analyze the dynamic nature of current operations and the rapidly evolving means of delivery in a pervasive media landscape shaped by traditional media outlets and ever-changing social media platforms. They explore how these tools influence the outside world in a highly interconnected information space, where international public opinion is largely entrenched yet still shifting. This chapter is especially valuable in helping readers make sense of the information being presented in the ongoing conflict between Israel and Hamas, particularly in light of the October 7, 2023 attack and Israel's response.

Finally, in Part IV: Conclusion, Francesca Granelli discusses "The Future of Information Operations." In this section, the author critically analyzes past information operations. Considering the fluid nature of public opinion and rapidly evolving technology, Granelli effectively argues that any information operation must be well-planned, well-structured, and have clearly defined and measurable goals.

In terms of constructive criticism, this book should have been published much earlier and could have been two to three times its current length. The material is highly digestible, provides a logical and consistent framework for understanding information operations, and is useful for both military and civilian audiences. The authors provide multiple examples of both effective and ineffective information operations spanning more than a century, leaving readers with a solid foundation for understanding the historical context and current issues surrounding official information efforts, evolving media, social media, and technology.

A potential improvement for this book (or a future volume) would be the inclusion of more contrasting perspectives, as seen in Section III, where the reader gains a clear overview of both sides involved in ongoing information operations in a specific conflict. Sections I and II focus heavily on Soviet/Russian information operations. While the material is excellent, contrasting chapters discussing allied and opposing information operations in each of these conflicts would provide greater balance and further clarify why some information operations succeed while others fail.

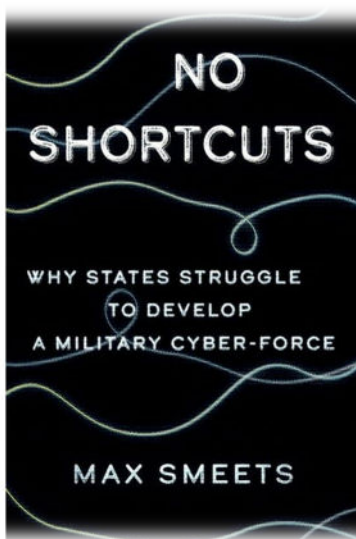
This work fills a clear gap in historiography. It is an extremely useful resource for military historians seeking to understand the development of information operations over the twentieth century, particularly those interested in Soviet/Russian information warfare strategies. Additionally, it is valuable for readers from any background who wish to comprehend the complex conflict between Israel and Hamas and the broader role of information warfare in modern geopolitical struggles.

BOOK REVIEW

No Shortcuts: Why States Struggle to Develop a Military Cyber-Force by Max Smeets

ISBN 978-0197661628, Oxford University Press, 2022, 213 pages, \$29.04

Reviewed by: **Mark Grzegorzewski**, Embry–Riddle Aeronautical University, Daytona Beach, Florida, USA



How many countries have military cyber forces today? The focus is often on the same major cyber powers, such as China, Russia, and the United States. As Max Smeets explains in the introduction to *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, at least 40 countries have established a cyber military command or similar structure. However, quantity does not equal quality, and many of these programs are severely underdeveloped and unprepared to compete with major cyber powers. So why do these states struggle?

Smeets, a senior researcher at the Center for Security Studies at ETH Zurich and director of the European Cyber Conflict Research Initiative, divides the book into three parts. The first part

(Chapters 1 and 2) discusses key concepts and provides an empirical overview of cyber-force development. The second part (Chapters 3 through 6) focuses on the internal state dynamics of cyber capability development. The final part (Chapters 7 through 9, plus the conclusion) explores how external actors can influence a state's cyber capability development.

Smeets introduces key terminology in Chapter 1 to discuss cyber operations, emphasizing the importance of defining what a "cyber weapon" is and examining the intended effects such weapons seek to achieve. By understanding these effects—disrupt, deny, degrade, destroy (D4), or espionage—readers can better grasp the purpose behind cyber operations. Smeets effectively integrates the Lockheed Martin Cyber Kill Chain methodology to show that while the effects of operations may differ, the steps involved remain consistent. The distinction lies in intent rather than process.

In Chapter 2, Smeets evaluates global cyber capabilities, noting that capturing cyber capabilities depends on how one defines a "cyber-attack." He traces the evolution of cyber policies from the early 2000s—when they were still modest—to their more comprehensive

expansion around 2010. However, Smeets notes that having a cyber strategy signifies intent, not capability. Countries differ significantly in how they structure their cyber operations, with some launching military cyber programs while others have yet to conduct observable operations to achieve cyber effects.

Chapter 3 explores the development of cyber programs, which are shaped by a state's assumptions about its threat landscape. For example, a country focused on generating spam campaigns may create a decentralized and low-maintenance program, whereas one prioritizing access to critical information may invest in a sophisticated and tightly controlled system. Smeets argues that cyber operations serve as flexible tools rather than strategic weapons due to challenges in attribution and coercion. Timing is crucial for successful cyber operations, especially when they act as supporting forces, where missteps can have severe consequences.

In Chapter 4, Smeets provides a typology to classify cyberspace actors by comparing their operational constraints with available resources. Operational constraints include factors such as the interplay between intelligence collection and military cyber operations, while resources refer to financial and organizational capacity. The most capable and threatening actors are those with minimal constraints and abundant resources, such as Russia. Smeets also presents a detailed case study of the Netherlands' cyber program, which exemplifies highly constrained and underfunded cyber programs.

Chapter 5 introduces Smeets' PETIO framework—People, Exploits, Toolsets, Infrastructure, and Organizational structure—as a method to evaluate a state's ability to develop offensive cyber capabilities. Among these, people are identified as the most critical component of cyber operations. While all elements of the framework are necessary, cyber operations cannot succeed without the right individuals in thought-intensive jobs that require human understanding and execution. Technology cannot replace this role, as cyber effects inherently target people. Exploits refer to the means by which cyber effects are delivered. While zero-day exploits are valuable, they are not a universal solution, as some organizations may have already patched specific vulnerabilities. Persistence and focus are key to long-term exploitation rather than reliance on zero days alone. Tools enable attackers to execute malware within target systems. A tradeoff exists: sophisticated toolsets make operations quieter but are costly and time-consuming to replace if detected. Infrastructure includes both access to target infrastructure for exploitation and a sandbox infrastructure for testing capabilities. To reduce costs, secondary infrastructure is often reused post-operation rather than being "burned." Lastly, organizational structure ties these elements together. While CRAMP (Capabilities, Requirements, Authorities, Mission, Permissions) is a common model for assessing cyber organizational capabilities, PETIO provides a broader framework.

Chapter 7 explores the role of experience in shaping cyber organizations. Smeets applies the concept of an experience curve, borrowed from business literature, to argue that more seasoned organizations accumulate greater resources and capabilities over time. This chapter underscores the intuitive idea that consistent practice enhances skills, making organizations more effective through shared experiences. This, in turn, leads to the

development of organizational tactics, techniques, and procedures (TTPs), which streamline the deployment of offensive capabilities.

Chapter 8 investigates unintentional cyber capability transfers, categorizing four different types. States can learn from observed cyber operations when a capability is deployed. Some may gain deep access to adversary networks, allowing them to witness operations in real-time. Public exposure of cyber tools, such as in the Shadow Brokers incident, allows other states to repurpose them. Government employees leaving for the private sector may take their expertise to contracting roles for other nations, such as former NSA employees assisting UAE cyber operations.

Chapter 9 focuses on non-state actors and their role in cyber conflicts. Smeets examines how hackers and contracting firms find and weaponize vulnerabilities for government buyers, driving up exploit prices and reducing overall cybersecurity. He argues that the zero-day market is plagued by information asymmetry, often flooded with low-quality exploits, making government partnerships with trusted sellers more effective.

Smeets concludes that most states have not crossed the barrier of entry into cyber operations due to significant internal and operational constraints. Financial and organizational limitations further restrict states' ability to conduct cyber effect operations. For these states, the fastest way to establish a military cyber force is through non-state actors ("cyber proxies"). While this approach has advantages, it also presents risks, particularly the danger of intermediaries retaining informational advantages over the state.

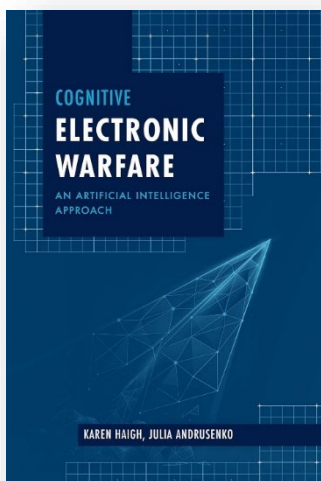
A minor critique of the book pertains to its structure. Smeets notes in the preface that portions of the material were initially presented in his cyber lectures, and two chapters were adapted from journal submissions. While each chapter stands effectively on its own, a more integrated structure could have improved the book's logical flow. Nevertheless, the book is highly recommended for those in cyber policy or strategy. It is accessible, logical, and original—essential reading for the field.

BOOK REVIEW

***Cognitive Electronic Warfare: An Artificial Intelligence Approach* by Karen Haigh and Julia Andrusenko**

ISBN 13:978-1-63081-811-1, Artech House, 2021, 239 pages, \$126.65

Reviewed by: **Sean Pascoli**, U.S. Army DEVCOM Research Laboratory, Adelphi, Maryland, USA



Cognitive Electronic Warfare: An Artificial Intelligence Approach is an essential read for the Special Operations Forces (SOF) community, as it explores opportunities to serve as a force multiplier for the Joint Force within the Electromagnetic Spectrum. Cognitive Electronic Warfare (CEW) is becoming increasingly important as modern warfare evolves with advancements in technology and artificial intelligence. CEW represents a shift from traditional electronic warfare (EW) techniques, which focus on jamming and disrupting enemy communications and radar systems, to more adaptive and intelligent methods.

Karen Haigh and Julia Andrusenko provide an excellent explanation of how artificial intelligence-driven cognitive systems can enhance electronic warfare by enabling faster and more adaptive responses in fluid, rapidly developing conflicts. The book delivers just the right amount of detail, covering a wide range of subjects from machine learning to real-time decision-making and maneuvering within the dynamic RF environment. Dr. Haigh and Ms. Andrusenko bring over 40 years of experience in the AI-RF problem space, supporting government agencies such as DARPA, AFRL, and ONR, while working for industry leaders including Mercury Systems and the Johns Hopkins University Applied Physics Laboratory.

The U.S. Department of Defense has recognized the growing importance of electronic warfare in modern conflicts, leading to increased investments in research and development. The Pentagon's 2024 budget includes significant allocations for advanced EW systems to maintain a technological edge over potential adversaries. With rising global tensions and rapid technological advancements, the role of electronic warfare in safeguarding national security is more critical than ever. The U.S. military's continued investments in EW capabilities are designed to ensure it remains at the forefront of this critical domain.

One area receiving significant investment is Cognitive Electronic Warfare (CEW). The authors present a compelling case for how cognitive artificial intelligence is transforming electronic warfare capabilities, particularly as the demand for responsive and adaptive systems continues to increase. By organizing their book into six key themes—adaptive countermeasures, enhanced decision-making, spectrum dominance, resource efficiency, interference reduction, and rapid response to complex threats—the authors provide a comprehensive framework for understanding why CEW represents a crucial advancement and how it will serve as a key combat multiplier in future conflicts.

- **Adaptive Countermeasures:** Cognitive systems can learn and adapt to new signals and tactics in real time. This adaptability is critical, as modern adversaries can rapidly change their tactics or frequency patterns. CEW systems can detect these changes and adjust countermeasures on the fly, making it far more difficult for adversaries to bypass or neutralize them.
- **Enhanced Decision-Making:** CEW leverages machine learning and AI to process and analyze vast amounts of data faster than human operators. This capability enables quicker and more informed decisions in complex combat environments, where traditional EW operators may struggle to keep up with the volume and variety of incoming signals.
- **Spectrum Dominance:** As battles increasingly rely on the electromagnetic spectrum for communication, navigation, and targeting, controlling this domain becomes paramount. Cognitive electronic warfare systems can identify, classify, and respond to threats more effectively than non-cognitive systems, giving friendly forces a decisive advantage.
- **Resource Efficiency:** Cognitive systems optimize the use of electronic warfare resources by dynamically adjusting power, frequency, and bandwidth for jamming or spoofing signals, conserving energy while reducing the likelihood of detection.
- **Interference Reduction:** In coalition or joint operations, where multiple EW systems are active, cognitive EW can minimize interference with allied or friendly forces' communications and radar by intelligently managing spectrum usage.
- **Rapid Response to Complex Threats:** Advanced threats such as networked unmanned systems and next-generation missile technologies require faster and more flexible countermeasures. Cognitive electronic warfare enables high-speed, autonomous responses, particularly in time-sensitive scenarios, where decisions must be made in milliseconds.

The book also features an excellent chapter on Electronic Battlefield Management and how the Human-Machine Interface (HMI) complements electronic support by helping machines better interpret human inputs. The authors illustrate this concept using Raytheon's EW Planning Management Tool (EWPMT), a program of record since 2014, which enhances a maneuver commander's ability to plan, coordinate, and synchronize EW, spectrum management, and cyber operations. Using a playbook interface that seamlessly integrates with Hierarchical Task Network (HTN) planning, EWPMT serves as a real-world example of how theoretical concepts translate into practical applications.

Cognitive Electronic Warfare provides a strong argument for why CEW is essential for maintaining strategic superiority in the electromagnetic spectrum, where future conflicts will likely involve both traditional and unconventional forms of electronic warfare. The authors offer exceptional examples linking theory to real-world applications, equipping readers with practical tools to solve EW challenges that traditional methods cannot address. The book provides valuable insights as U.S. Special Operations Forces continue to refine electronic warfare requirements and assess their role in shaping and maneuvering the electromagnetic spectrum for the Joint Force.

This book is specifically tailored to meet the operational needs of warfighters, while also being accessible to those new to electronic warfare concepts. It clearly explains how Cognitive Electronic Warfare provides U.S. forces with a critical advantage by detecting, classifying, and analyzing signals and anomalies. These capabilities are vital in modern operational environments, where the ability to pivot rapidly in response to new intelligence can determine mission success or failure.

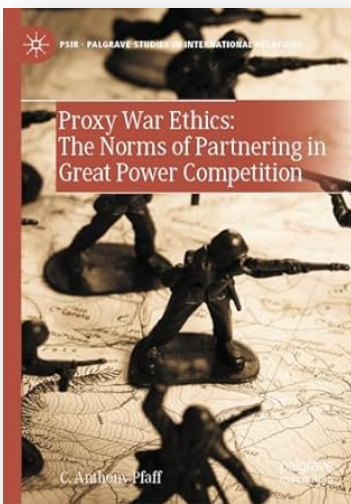
As threats continue to evolve, and as the radio-frequency (RF) spectrum becomes increasingly contested and congested, CEW provides U.S. forces with the necessary tools to dominate the operational and strategic landscape—both now and in the future.

BOOK REVIEW

***Proxy War Ethics: The Norms of Partnering in Great Power Competition* by C. Anthony Pfaff**

ISBN: 978-3-031-50457-0, Palgrave MacMillan: Cham, Switzerland, 2024, 244 pages, \$95.42

Reviewed by: **LTC Joshua Lehman**, United States Military Academy at West Point, West Point, New York, USA



“Ethical decision-making does not have to be risk-free; it just has to be prudent.” This might be the central governing principle that Anthony Pfaff advances in his moral analysis *Proxy War Ethics: The Norms of Partnering in Great Power Competition*. Pfaff’s burden is to show that the principles of the Just War Tradition are applicable to 21st-century proxy warfare.

The argument is made in six chapters. Grounding his ethical paradigm in the Just War Tradition, Pfaff considers the principles of Jus Ad Bellum and Jus In Bello as they apply to proxy war. In the first chapter, he clarifies the central notion of a proxy relationship by contrasting it with allies and partners. To do this, he employs four relational concepts: power asymmetry, interest alignment, benefits, and control.

Pfaff contends that a sponsor-proxy relationship is a principal-agent relationship wherein contingent interests can and do diverge, benefits are transactional and indirect, and principals control agents through withholding resources. Understanding the nature of the relationship allows him to shed light on the moral hazards inherent to both sponsor and proxy and to subsequently develop a set of ethics for operating with unique risks. It is important to note that Pfaff does not see all principal-agent relationships as sponsor-proxy relations. He excludes those actors that work within the same constitutional framework, e.g., private military contractors, and he excludes robots as non-moral entities.

The second and third chapters provide a historical case study analysis to identify ethical conditions and moral hazards involved in proxy war. Pfaff treats case studies from the Peloponnesian War through recent civil wars in South America. These case studies show the central ethical problems of proxy war: divergence of interests between sponsor and proxy makes the relationship unstable, perhaps even incoherent—the sponsor’s commitment to the proxy is uncertain; controlling the proxy is not only operationally difficult, but lethal support to the proxy might end up in the hands of actors the sponsor

does not intend to support; moreover, a proxy might violate norms or rights, raising questions of sponsor responsibility; introducing sponsorship risks prolonging a war or even starting one that might not have otherwise begun; non-vital interests may become amplified, possibly leading to a quagmire; and postbellum questions of sponsor withdrawal emerge.

To address these problems, Pfaff examines seven *Jus Ad Bellum* principles applied to proxy wars in his fourth chapter. The main concerns for the sponsor are: Is the proxy's cause just? Will supporting a proxy initiate a war that would have otherwise not come about? Will supporting the proxy prolong a war? Pfaff categorizes all proxy wars as a form of intervention and relies on Michael Walzer's norms for guidance. However, he uses Walzer's doctrine to render the justness of the proxy irrelevant, arguing that this approach results in endless escalation. Therefore, the sponsor ought to support only a just proxy.

Regarding proportionality, Pfaff's sponsor must ask how sponsorship will affect proxy proportionality calculations. The principle of legitimate authority poses a problem for proxies that may not be state actors. Here, Pfaff relies again on Walzer in locating authority in the ability of a political community or group to gain the assent of its people and effectively govern, though Pfaff is willing to extend legitimate authority to non-state international organizations like Hezbollah, so long as they meet a set of criteria showing the assent of the people and the necessity of the assent. The Just War principle of public declaration creates a thorny problem for clandestine or low-visibility military assistance. Pfaff responds that proxy relationships should be public, but that secrecy is permissible when "human rights and human well-being are concerned." Nonetheless, Pfaff calls for some form of oversight.

Proxy war challenges the right intention because the dual intentions—of proxy and sponsor—can and often diverge. Pfaff responds that the right intention is achieved when both proxy and sponsor have just causes; they need not align perfectly. The last resort in proxy war becomes a matter of sponsors' understanding of the proportionality calculus of the proxy. The sponsor has alternatives; the proxy may not, but sponsors should understand what moral hazards increase by offering the proxy a war option. Finally, sponsors "should intervene with proxy success in mind." This wards off the moral hazard of abandonment.

In chapter five, Pfaff turns to five *Jus In Bello* considerations. First among these concerns is interest divergence and the threat of sponsor betrayal. In other words, once a sponsor's war aim has been achieved, it is possible that the sponsor will reduce costs by exiting the war—a move that can be understood as a betrayal to the proxy. Sponsors must recognize the moral hazards involved in exiting the war. Regarding proportionality, Pfaff is concerned that sponsors alter calculations of the cost of violence. Moreover, they increase the threat of escalation as counter-sponsors respond tit for tat. Pfaff calls for just sponsors to develop plans for "escalation dominance." Such a plan commits the sponsor to the success of the proxy force, a commitment that, as readers of Walzer will recall, is prohibited in the interest of the sovereignty of the supported political community.

Another plan demanded by an ethical approach to proxy war is the control of lethal support to prevent the diffusion of arms to unintended recipients. Finally, Pfaff addresses the problem of dirty hands, arguing that it is permissible to support morally compromised

proxies so long as “proxy failure represents greater injustice than dirty hands represent.” Of all the claims in the book, this probably is the most debatable. It seems to invite a realist calculation that the Just War Tradition rejects. There is no true Doctrine of Double Effect that one can rely on to account for unintended human rights-violating proxy actions. Proxies are morally responsible agents, not weapon systems. Rather, it seems that the arguments against utilitarianism are appropriate here: we should not be willing to accept an evil in order to achieve a greater good—or, in this case, a lesser evil.

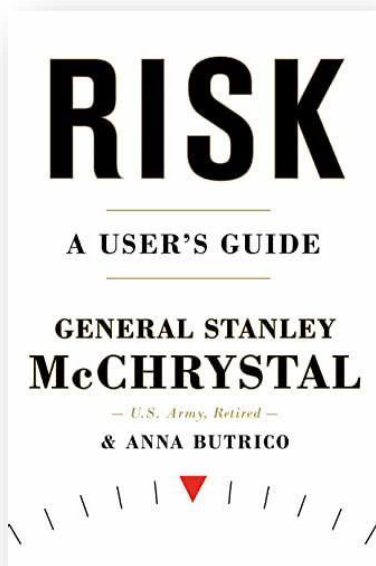
Pfaff’s final chapter revisits the opening account of the geopolitical situation of the 21st century and shows that today is a continuation of the history recounted in earlier chapters—the world is ripe for proxy warfare; it is happening now and will likely happen in the future. The author’s clear presentation of the Just War principles applied to the situation of proxy warfare is a testament not only to the book’s analytic rigor but also to the enduring value of the Just War Tradition. Scholars at the graduate level and higher working in the Just War Tradition will benefit the most from this book, though mid-to-senior-grade security professionals studying and practicing international relations, ethics, and policymaking will also find it profitable. If there is any form of warfare that lends itself to the realist vision of warfare, it is proxy war, with its assumption of realist geopolitics. Pfaff shows that a Just War ethicist need not eschew proxy war; he should simply be prudent about it.

BOOK REVIEW

***Risk: A User's Guide* by Stanley A. McChrystal and Anne Butrico**

ISBN 9780593192207, Penguin Books, 2021, 343 pages, \$17.49 hardcover

Reviewed by: **Ibrahim Kocaman**, Embry–Riddle Aeronautical University, Daytona Beach, Florida, USA



Operating under uncertainty has perhaps never been as challenging as it is in today's global landscape. Whether you lead a governmental agency, a military unit, a business, or are just an ordinary citizen, the environment you need to navigate is characterized by a myriad of risks. These arise from the intricate mix of political and economic uncertainties, rapid—often disruptive—technological changes, ramifications of the AI revolution, and unconventional challenges like climate change, among others. If you are struggling to manage the risks you face, General Stanley McChrystal and co-author Anna Butrico's book *Risk: A User's Guide* offers a beacon of hope. Speaking from experience, McChrystal proposes embracing risk intelligently, and rather than preoccupying yourself with things beyond your control—like the risk itself—focus on what you can control and how you can develop immunity

against risk by empowering yourself and your organization. This main argument is predicated upon McChrystal's proposition that "we are, most often, the architects of our fate." Ultimately, McChrystal aims to emphasize the agency we have in developing our responses that collectively build our immunity against risk.

The book's central argument is that "at its core, effective risk management is about leadership and how capable leaders are in fostering resilience within their organizations." While this is not the first book that puts the spotlight on leadership, it makes a noteworthy contribution to our understanding of decision-making in an unpredictable environment. On the contrary, McChrystal starts by acknowledging that risks will always be there. Breaking down risks into several categories (i.e., communication risk, narrative risk, and structural risk), he highlights the host of challenges all types of organizations—government, military, and business—face in navigating the uncertainties of our world. His nuanced conceptualization of risk pertains to both external threats and internal vulnerabilities.

The book is organized into three major parts spanning seventeen chapters, along with a prologue and an epilogue. In part one, the authors prepare the reader for their central thesis by

conceptualizing risk as “the probability of something unwanted happening, and the potential consequences if it did.” They illustrate this with the example of the Sword of Damocles, where the sword hanging over the king’s throne represents the risk, and the combination of its probability of falling and the calamity it would create if it did constitute the actual risk. The authors also offer their blueprint for addressing risk, which entails an approach that acknowledges risk as an inescapable reality, albeit something that is still manageable by building resilience at both individual and organizational levels. McChrystal calls this blueprint a “Risk Immune System.” He proposes four functions essential to an effective Risk Immune System: Detect, Assess, Respond, and Learn.

In part two, the chapters are organized around risk control factors, as the book intentionally focuses on what one can control in responding to risks. McChrystal identifies ten dimensions of control that need to be monitored and adjusted to build his proposed Risk Immune System:

1. **Communication:** How we exchange information
2. **Narrative:** How we present who we are and what we do
3. **Structure:** How we design our organization
4. **Technology:** How we apply equipment, resources, and know-how
5. **Diversity:** How we leverage the host of abilities and perspectives we can tap into
6. **Bias:** How our assumptions about the world impact us
7. **Action:** How we overcome inertia/resistance in implementing our response
8. **Timing:** How the timing of our action affects its effectiveness
9. **Adaptability:** How we respond to changes in the risks and environments
10. **Leadership:** How we direct and inspire the Risk Immune System (pp. 11-12).

After identifying these dimensions of control, in part three, McChrystal offers 11 practical solutions, combinations of which could be tailored to an organization's needs to build a relevant toolbox for enhancing resilience to risk. These solutions include assumptions check, risk review, risk alignment check, gap analysis, snap assessment, communications check, tabletop exercise, war gaming, red teaming, pre-mortem, and after-action review.

The book is well-organized and structured, and at times it reads like a textbook from a course syllabus on management. That said, the book balances theoretical concepts, statistics, and leadership principles with real-life examples. It strikes a fair balance between conceptual arguments and practical applications, blending in case stories, vignettes, and historical accounts—such as Pearl Harbor, the 9/11 attacks, and the COVID-19 pandemic—along with contemporary cases from the business world, including Apple, Google, and Boeing. It also frequently draws on McChrystal’s recollections from his lengthy military career and personal history. This delicate balance and exceptional storytelling make the book appealing to a broader audience, including military personnel, educators, executive leaders, and entrepreneurs.

While mostly well-received within the community, the book has garnered some criticism, such as in *National Review* and from Air Force Brigadier General Chad Manske. Both critiques argued that McChrystal lacked credibility due to his failures in Afghanistan. Judging McChrystal's competence in risk management solely based on his relatively brief tenure (just over a year) as commander of the International Security Assistance Force (ISAF) overlooks his much longer military career.

Yet, the book and McChrystal's proposed blueprint for a Risk Immune System (RIS) are not free from their drawbacks. To start with, while it presents many useful analogies, McChrystal's RIS framework reflects an oversimplification of the complex and multifaceted dimensions of risk that organizations across various sectors encounter. Second, thanks to his colorful military career, the book heavily relies on military analogies in developing and defending its central thesis. This leads to an overemphasis on organizational structures akin to the military, which might come at the expense of individual agency—something the book conversely aims to advocate for. Finally, the book and the proposed RIS framework focus exclusively on internal risk factors within individuals and organizations, largely neglecting external risks such as political, economic, societal, and cultural variables, all of which have undeniable effects on the level and gravity of risk. While one may argue that such an exclusive focus aligns with the basic premise of the book—focusing on what you can control—it could still offer insights into how the effects of external factors could be mitigated.

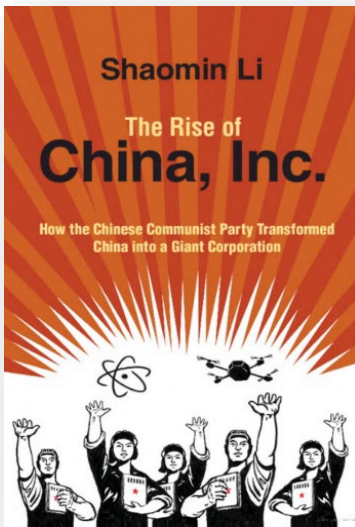
All in all, McChrystal and Butrico's book offers useful insights and provides readers with a risk management framework that could be applied to a diverse range of organizational settings, including all levels of government, the military, and industry. McChrystal's call for a focus on people and what they can control—rather than fixating on the inherent characteristics of risk that are well beyond our control—constitutes a significant contribution to the risk management literature and has clear policy implications. His nuanced conceptualization of risk and emphasis on leadership as essential to developing an organizational response to risk should also be noted. These valuable insights make this book a guiding light for readers seeking to navigate the complexities of today's world. The book also serves as a valuable resource for leaders whose mandates entail protecting their organizations from the dire consequences of unpredictable and inescapable risks.

BOOK REVIEW

***The Rise of China Inc.* by Shaomin Li**

ISBN 978-1-316-51387-3, Cambridge University Press, January 2022, 346 pages, \$41.99 paperback

Reviewed by: **Ian Murphy**, SECURIFENSE, INC., Hendersonville, North Carolina, USA



Operating under uncertainty has perhaps never been as challenging as it is in today's global landscape. Whether you lead a governmental agency, a military unit, or a business, or are just an ordinary citizen, the environment you must navigate is characterized by a myriad of risks. These arise from the intricate mix of political and economic uncertainties, rapid—often disruptive—technological changes, the ramifications of the AI revolution, and unconventional challenges like climate change, among others.

If you are struggling to manage the risks you face, General Stanley McChrystal and co-author Anna Butrico's book *Risk: A User's Guide* offers a beacon of hope. Speaking from experience, McChrystal proposes embracing risk intelligently. Rather than preoccupying yourself with things beyond your control—like the risk itself—he

advocates focusing on what you can control and how you can develop immunity against risk by empowering yourself and your organization. This main argument is predicated on McChrystal's assertion that "we are, most often, the architects of our fate." Ultimately, McChrystal emphasizes the agency we have in developing responses that collectively build our immunity against risk.

The book's central argument is that "at its core, effective risk management is about leadership and how capable leaders are in fostering resilience within their organizations." While this is not the first book to spotlight leadership, it makes a noteworthy contribution to our understanding of decision-making in unpredictable environments. Unlike many discussions that frame risk as an external problem to be eliminated, McChrystal acknowledges that risks will always exist. Breaking risks down into several categories (e.g., communication risk, narrative risk, and structural risk), he highlights the host of challenges that all types of organizations—government, military, and business—face in navigating uncertainty. His nuanced conceptualization of risk pertains to both external threats and internal vulnerabilities.

The book is organized into three major parts spanning seventeen chapters, along with a prologue and an epilogue.

In Part One, the authors introduce their central thesis by conceptualizing risk as “the probability of something unwanted happening and the potential consequences if it does.” They illustrate this with the example of the Sword of Damocles, where the sword hanging over the king’s throne represents the risk, and the combination of its probability of falling and the calamity it would cause if it did constitutes the actual risk. The authors also offer their blueprint for addressing risk, emphasizing that while risk is an inescapable reality, it is still manageable through building resilience at both individual and organizational levels. McChrystal calls this blueprint a “Risk Immune System” (RIS) and outlines four essential functions for its effectiveness: Detect, Assess, Respond, and Learn.

In Part Two, the chapters focus on risk control factors, as the book intentionally emphasizes what one can control when responding to risks. McChrystal identifies ten dimensions of control that must be monitored and adjusted to build a robust Risk Immune System:

1. Communication – How we exchange information
2. Narrative – How we present who we are and what we do
3. Structure – How we design our organization
4. Technology – How we apply equipment, resources, and know-how
5. Diversity – How we leverage various abilities and perspectives
6. Bias – How our assumptions about the world impact us
7. Action – How we overcome inertia or resistance in implementing our response
8. Timing – How the timing of our actions affects effectiveness
9. Adaptability – How we respond to changes in risks and environments
10. Leadership – How we direct and inspire the Risk Immune System

In Part Three, McChrystal presents 11 practical solutions, combinations of which can be tailored to an organization's specific needs to build a risk resilience toolbox. These solutions include: assumptions check, risk review, risk alignment check, gap analysis, snap assessment, communications check, tabletop exercise, war gaming, red teaming, pre-mortem, and after-action review.

The book is well-organized and structured, and at times reads like a management textbook. However, it effectively balances theoretical concepts, statistics, and leadership principles with real-life examples. It strikes a fair balance between conceptual arguments and practical applications, blending case studies, historical accounts, and contemporary business examples. The authors draw on lessons from Pearl Harbor, the 9/11 attacks, and the COVID-19 pandemic, as well as corporate case studies from Apple, Google, and Boeing. McChrystal frequently reflects on his lengthy military career, enriching the discussion with firsthand insights. This delicate balance and compelling storytelling make

the book appealing to a broad audience, including military personnel, educators, executive leaders, and entrepreneurs.

While generally well-received, the book has drawn some criticism. For example, National Review and Air Force Brigadier General Chad Manske questioned McChrystal's credibility due to his failures in Afghanistan. However, judging McChrystal's competence in risk management solely based on his relatively brief tenure (just over a year) as commander of the International Security Assistance Force (ISAF) overlooks his much longer military career.

That said, the book and McChrystal's Risk Immune System (RIS) framework are not without their drawbacks. First, while it presents many useful analogies, McChrystal's RIS framework oversimplifies the complex and multifaceted dimensions of risk that organizations face. Second, thanks to his military background, the book heavily relies on military analogies, leading to an overemphasis on rigid organizational structures, which might undermine the very individual agency the book seeks to promote. Finally, the RIS framework focuses almost exclusively on internal risk factors—neglecting external risks such as political, economic, societal, and cultural factors, all of which significantly impact risk management. While one may argue that this focus on internal factors aligns with the book's central premise—focusing on what you can control—it would still be beneficial to explore how external factors can be mitigated.

All in all, *Risk: A User's Guide* offers valuable insights and provides readers with a risk management framework applicable to government, military, and industry settings. McChrystal's call to focus on people and what they can control, rather than fixating on the inherent unpredictability of risk, constitutes a significant contribution to risk management literature and carries clear policy implications. His nuanced conceptualization of risk and emphasis on leadership as key to developing an organizational response to risk further enhance the book's impact.

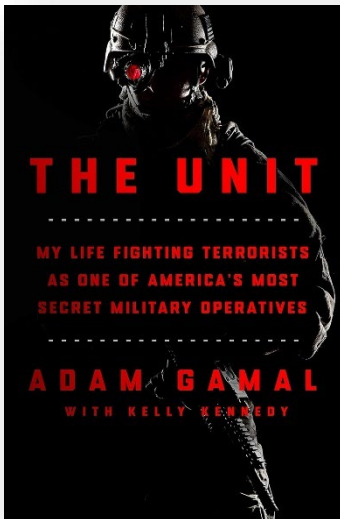
For leaders seeking to navigate today's complex world, this book serves as a practical guide. It is also a valuable resource for professionals whose responsibilities include protecting their organizations from the dire consequences of unpredictable risks.

BOOK REVIEW

***The Unit: My Life Fighting Terrorists as One of America's Most Secret Military Operatives* by Adam Gamal**

ISBN: 978-1250278173, St. Martin's Press, 2024, 304 pages, \$15.13, hardcover

Reviewed by: **James Stejskal**, Historian, Alexandria, Virginia, USA



When I first read about *The Unit: My Life Fighting Terrorists as One of America's Most Secret Military Operatives* online, I was concerned about the secrets the book might reveal—specifically, that it might disclose too much about what I know to be one of the best-kept secrets in the United States military or, for that matter, the U.S. government.

The Unit—I will call it that as well and for good reason—the missions it has, the people who carry them out, and how it goes about its work have been classified for many years. Rightly so.

There has been much conjecture, and many assertions made about this military organization by journalists, podcasters, and armchair strategists who claim they know what's what. Most of those contentions have fallen well short of reality—thankfully. Because “The Unit” is a vital resource that plays a key role in protecting our nation.

So it was with some trepidation that I contacted the co-author, Kelly Kennedy, to ask whether the book had gone through the Defense Department's required pre-publication review process. I was relieved when she told me that the author had insisted on following proper clearance procedures with the DoD and *The Unit* to ensure no security breach would occur. Somewhat placated, I ordered the book to see what “Adam Gamal” (a pseudonym) had to say.

First off, it's good. It's a well-constructed narrative that moves along quickly and draws the reader in.

Second, it's not about *The Unit*. I can say that. The author touches on aspects of his duties but nothing that would paint a picture for an adversary. I'll get into that later.

Third, what it *is* about is a personal story. Adam Gamal tells us an immigrant's tale—a journey from Egypt to the United States. A story of family and his “becoming” American. The author begins by taking us back to his birthplace of Alexandria on the shores of the Mediterranean. He describes his parents as key to an upbringing that gave him the tools to

succeed—first by being a strong couple, neither dominating the other, then by ensuring he overcame his childhood asthma. How they conditioned him to beat it, giving him the stamina to pass *The Unit's* physically and mentally grueling assessment and selection program, is a tribute to both their and the author's determination. His self-taught father insisted he get a good education and, above all, be tolerant of others in the melting pot that Alexandria was at that time. Muslims, Christians, and Jews got along in those days—not too long ago.

There was one other thing he learned: to avoid the Muslim Brotherhood—the extremists who would eventually alter the status quo as the “hateful” influence of Salafists seeped into Egypt. It was because of his education, family, and friends that he turned away from extremists and their teachings. But perhaps the event that affected him most of all was the visit of Jimmy Carter to Egypt after Anwar Sadat signed a peace treaty with Israel. Gamal persevered and ended up studying in the United States and working wherever he could.

If there was one event that steered his course into the Army, it was the 1993 bombing of the World Trade Center in New York. He joined as an immigrant, without a security clearance. He would have to work his way up. Why did he join? It was his way of paying his debt to his adopted country in advance and a way to counter the extremists he scorned. From there, he recounts some of his “adventures.”

There are snippets of his military life—going through basic training, and deployments with the conventional (aka “green,” aka “big”) Army—before he takes the jump into the “black” world. He describes dealing with the anti-Arab resentment of soldiers who had served in Operation DESERT STORM, people who only saw that he was brown and different from them. But he persevered. He applied his life lessons and climbed the ladder, but it was his “alien” origins that became an asset and changed his life's course. His culture and language brought him to the attention of *The Unit*, which needed men and women like him.

In the book, Gamal alludes to his service with the “secret squirrel” side of the military. It was the kind of job that, when someone says, “Thank you for your service,” you know they haven't the faintest idea what “your service” actually was. In Adam Gamal's case, it meant living and working in places with little comfort, great danger, and often no top cover from the Air Force.

And quite often, it was dangerous beyond measure—literally. You are usually living on your own amid what might be a peaceful place one second and the worst place on Earth the next.

The author knows what that kind of service is about, and it shows in his writing (ably assisted by Ms. Kennedy). But he does not shout it out. He quietly emphasizes that the work is done by men and women—committed professionals who have chosen a path that lies in the shadows and is rarely acknowledged. His book commemorates those like him who have chosen that route to repay a nation that gave them the opportunity and the freedom to choose.

Suffice it to say, the book will not show or tell you much about the men and women of that *Unit* or even what it does—other than that it does its job very well. What you will learn is that there are people, many of them immigrants, willing to do what is necessary to protect our country and its way of life. It is a story well worth reading—one that demonstrates that while so many Americans stay home safe and uncommitted, there are others who risk it all to do it on their behalf.

This book will interest anyone who wants to understand why cultural diversity and the ability to work in foreign environments are crucial for the U.S. to achieve its goals around the world.