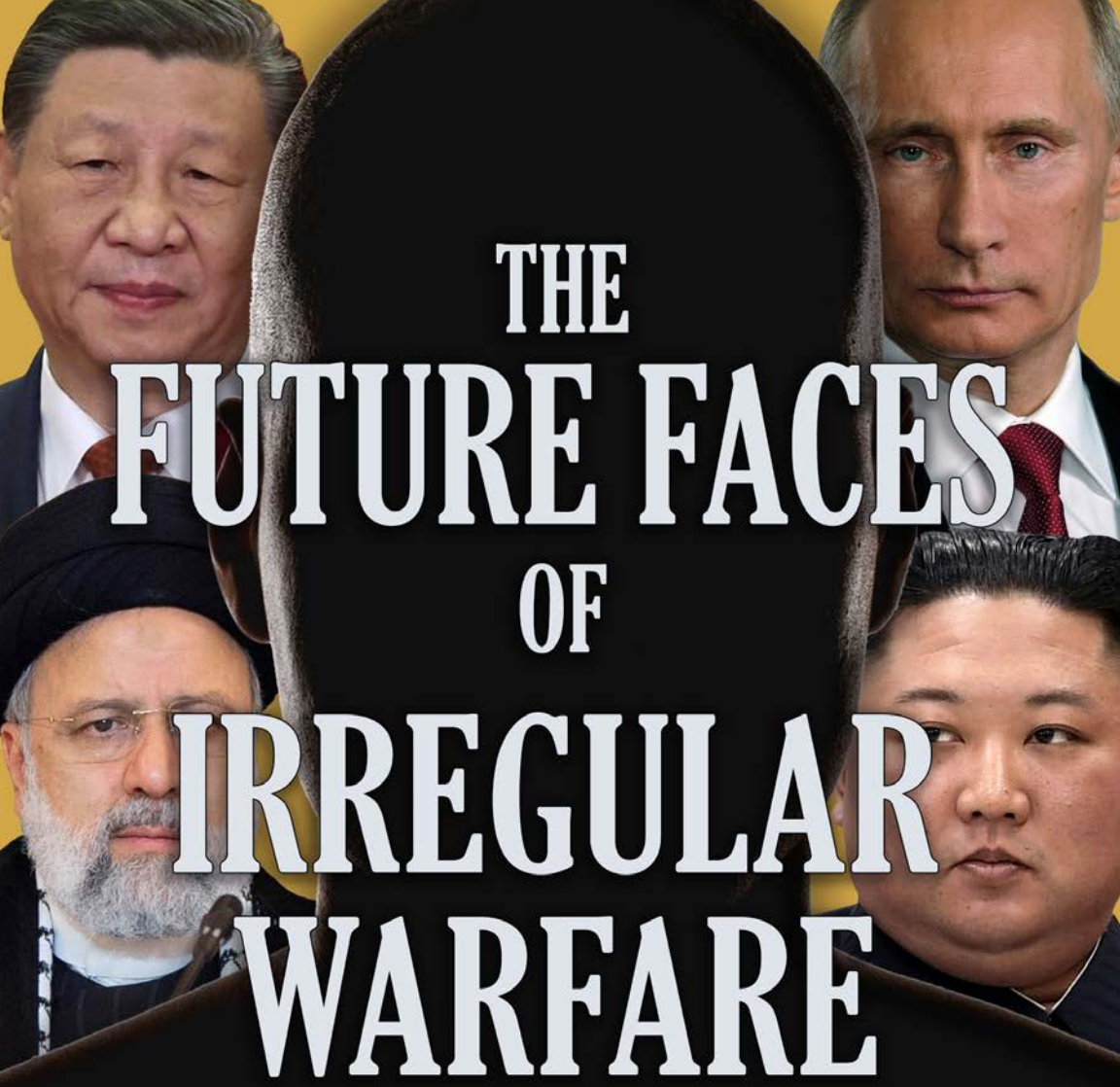

THE FUTURE FACES OF IRREGULAR WARFARE

Great Power Competition in the 21st Century

EDITORS: Varsha Koduvayur
AND James Kiras AND Richard Newton

The Future Faces of Irregular Warfare:

Great Power Competition in the 21st Century

Editors:
Varsha Koduvayur
James Kiras, PhD
Richard Newton, PhD

IRREGULAR WARFARE CENTER

Irregular Warfare Center Press

www.IrregularWarfareCenter.org

ISBN: 979-8-218-47880-3

About the Editors

Varsha Koduvayur

Ms. Varsha Koduvayur is a Senior Analyst (contractor, Valens Global) at the Irregular Warfare Center (IWC) as well as a manager at Valens Global. At the IWC, she leads research efforts on irregular warfare, strategic competition, and hybrid threats in the Indo Pacific and the Middle East. She collaborates on interagency efforts to counter hybrid threats focused on building whole-of-society resilience to gray zone activities. Additionally, she manages the publications of the IWC, serving as a peer reviewer and editor for the Center's online publications. Previously, Varsha managed the Gulf Arab states program at the Foundation for Defense of Democracies, she was a researcher in the Middle East practice at the Eurasia Group, covering the Gulf Cooperation Council countries, Libya, and Egypt, and a Junior Fellow in the Middle East program at the Carnegie Endowment for International Peace. Varsha has a BA in international relations and Arabic from Michigan State University. She has been a regular contributor to CNN Business and has had bylines in Foreign Policy, Foreign Affairs, Homeland Security Today, The National Interest, National Review, RealClearMarkets, and other outlets. Some of her selected publications include *Blind Sided: A Reconceptualization of the Role of Emerging Technologies in Shaping Information Operations in the Gray Zone* (Irregular Warfare Center); "How to Win Friends and Wage Jihad" (Foreign Affairs, with Dr. Daveed Gartenstein-Ross); and "Welcome to a Brand-New Middle East" (Foreign Policy, with David Daoud).

Professor James D. Kiras

Dr. Kiras has more than 25 years of experience within academia and defense policy. Currently he is the Dean of Academics at the School of Advanced Air & Space Studies (SAASS), the US Air Force's premier school of strategy. Dr. Kiras transformed and evolved SAASS core course offering on irregular warfare for two decades. He is a Senior Fellow of the Joint Special Operations University, Tampa, Florida and an Irregular Warfare Fellow at the U.S. Air Force Special Operations School, Hurlburt Field, Florida. In 2007 he received twin honors: AETC Civilian Educator of the Year and Air University Faculty Excellence awards. Dr. Kiras writes and lectures extensively on various aspects of irregular

warfare, including special operations, counterterrorism, and counterinsurgency. His most recent works are *Special Operations Success: Balancing Capabilities and Control (late 2024), Into the Void: Special Operations Forces After the War on Terrorism (2024)*, *Strategic Sabotage (2021)*, and *Special Operations: Out of the Shadows (2020)*. Dr. Kiras holds a bachelor's degree in history from the University of Massachusetts at Boston, a master's degree in history/international Relations from the University of Toronto, as well as a PhD from the University of Reading (UK).

Dr. Rick Newton

Rick Newton is currently serving as an irregular warfare and strategic plans officer at Special Operations Command Europe. He retired from the U.S. Air Force after a 22-year career as a combat rescue and special operations helicopter pilot, combat aviation advisor, plans officer, and educator. Between 2001 and 2023, he served on the faculty as a researcher and author at Joint Special Operations University. Rick has also served as visiting faculty at the U.S. Army School of Advanced Military Studies. He currently volunteers as the Director of the Irregular Warfare Initiative's Project Air and Space Power and as a Senior Fellow for the Homeland Defense Institute, a collaborative endeavor between U.S. Northern Command and the U.S. Air Force Academy, and as a Senior Fellow at the Global National Security Institute at the University of South Florida. He earned a Bachelor of Science degree from the USAF Academy and a master's degree from the US Army School of Advanced Military Studies. Dr Newton also holds a PhD in Defence Studies from King's College London.

Table of Contents

Foreword

LTG Michael Nagata, U.S. Army (retired)

It is a rare privilege to have the chance to provide what I pray is a useful introduction to such an important and timely work.

The contents of this compendium are a tour de force of seasoned, expert, and thoughtful contributions that anyone concerned with America's ability to effectively practice the science and art of irregular warfare (IW) would profit from. The distinguished authors and their contributions herein make an immense contribution toward an improved understanding of this kind of warfare, and both practitioners and policymakers alike would benefit from examining its contents.

As I write these words, the concept of "irregular warfare" appears once again to be a fashionable term among some in U.S. government circles. Yet, this begs the question whether it will once again become just a passing fad, or finally be treated with the sustained strategic seriousness that America's abundant national security challenges now require.

As a career special operations practitioner, officer, and leader for well over 30 years, I have seen the U.S. government's focus, prioritization, and resourcing of irregular warfare wax and wane all too frequently. Too often, I have witnessed both civilian and military leaders treat conventional forms of warfare and irregular forms of warfare as if they were competitors in a zero-sum game. This typically leads to a dysfunctional treatment as antagonistic, polar opposites that must be forced to compete for resources, people, and policy attention. That alone has plagued the United States' ability to be tactically, operationally, or strategically successful in irregular warfare.

To make matters worse, the U.S. government, including the Department of Defense (DoD), is too often quite inconsistent in how it even defines, let alone "thinks about," irregular warfare. As one example, the DoD dictionary defines irregular warfare as "[a] violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)."[1] And yet, DoD's *Irregular Warfare Annex*, published

in 2020, states: "[i]rregular warfare is a struggle among state and non-state actors to influence populations and affect legitimacy."[2]

The first definition prioritizes violent struggle; the second does not mention violence at all. Neither definition is fundamentally wrong, yet the two are nonetheless quite inconsistent. Sadly, any practitioner of irregular warfare knows all too well that this is not the only example of U.S. government inconsistency.

This type of political inconsistency can too often disable practitioners, leaders, and even those responsible for resourcing. This is despite the executive and legislative branches of the U.S. government are all working together to solve the same problems, at the same time, and in mutually supportive ways. Sadly, this is not the only problem America faces in trying to improve its skills and abilities when it comes to irregular warfare.

Another consistent problem, that all too often leads to failure, is the reluctance and even outright aversion that many U.S. government officials display when it comes to the conduct of irregular warfare activities. This reluctance creates crushing and self-inflicted difficulties on the ability of irregular warfare practitioners to be tactically, operationally, and strategically effective. This cowardice is a plague on all forms of irregular warfare, but most egregious in one particular arena: influence operations, as well as its handmaidens, information and messaging operations.

Many of those that read this compendium were once, or perhaps still are today, practitioners of irregular warfare. Accordingly, they will likely be familiar with the famous lament heard far too often by leaders and practitioners during the counterterrorism and counterinsurgency operations of the past 20 years. That lament, heard from those I served with, was, "how can it be that I have abundant authority conduct a lethal operation to outright kill this enemy and everyone with him, but I cannot send him, or the population he preys on, an e-mail or post a message to contest his poisonous ideology or degrade his influence with the same alacrity and freedom I enjoy when employing physical force?"

However, as vital and important as effective irregular warfare has been against non-state terrorist and insurgent adversaries, I believe that it will be even more important, and even more strategically consequential, against America's nation-state adversaries and competitors in the future. What some are styling as the "Digital Age of Mankind" is having the practical effect of leveling the strategic playing field amongst both nation-state and non-state actors alike in many different arenas, including that of irregular warfare.[3]

This new technological reality is enabling both state and non-state adversaries of the United States, in many places and in many cases around the world, to out-compete, out-influence, and thereby strategically prevail over, the United States...often without firing a single shot. The rapidly expanding capacity of every individual to effectively influence or alter the beliefs, values, and choices of global populations should be a wake-up-call that digital technologies have broken centuries of belief that the side with the bigger battalions will always prevail.

The world is now living in a time of radical technological change, and that change is not only continuous, it is accelerating. It is true that, in many ways, rapidly advancing technologies have enhanced the prosperity, safety, and longevity of billions of people. The convenience they provide, the global reach they allow, and the information that is now literally at almost everyone's fingertips have all been a genuine and continuing boon for peace and prosperity in many places around the world.

Yet, as has been true with every human invention since the dawn of civilization, every new technology can also be used for malign purposes. So it is with digital technologies, which are more widely available today due to their increased affordability.

It has become common to expect that while digital technologies rise in capability, power, and reach, they simultaneously also fall in relative cost. Comparing the capability-versus-cost of a microprocessor several decades ago, to a microprocessor of today, illuminates that trend vividly. As such, if there ever were a monopoly for wealthy nation-states in the wielding of increasingly powerful digital technologies (e.g., artificial intelligence, robotics, digitally secure communications, etc.), that monopoly has been forever broken. Also, like all innovations and inventions in human history, any technology, including the digital kind, that can be used for peaceful pursuits can also be harnessed as an engine of conflict and war. As we have seen, non-state actors with a even a modicum of funds can potentially reach parity, and sometimes even superiority, to the digital technology wielded by a nation-state.

This does not mean that the United States or its allies cannot prevail in competition or even war, whether of the conventional or irregular variety. Yet, it does mean that if we fail to be more adept, more agile, faster, and perhaps most importantly, more risk-tolerant in embracing these constantly evolving digital technologies, we leave ourselves open to strategic defeat by competitors and adversaries alike, that succeed where we fail.

Such a defeat should no longer to be expected to flow exclusively from a traditional battlefield disaster or setback. While the United States should certainly tend to its

readiness for kinetic combat, its traditional strength since at least the Second World War that continues to be abundantly resourced every year, the America must also be just as energetic towards ensuring readiness for irregular warfare.

The readiness investments required for irregular warfare will not be infantry battalions, aircraft carriers, or fighter-bombers. In large part, they will be how adeptly and aggressively our nation can adopt ever-more-powerful digital technologies that will allow the United States and its allies to more effectively compete in the "global marketplace of ideas." More specifically, the United State must achieve far greater effectiveness in the arena of influence operations. As any practitioner will tell you, a fundamental requirement of effective influence and messaging in the digital environment requires enormous operational and tactical flexibility, agility, and speed in getting our ideas out before, and more persuasively than, those of our competitors and adversaries. Most importantly, embracing these three key attributes—flexibility, agility, and speed—will require policymakers to accept a higher tolerance for mistakes, or even outright failures, by practitioners. Leadership micromanagement in IW is corrosive to achieving these things, and without higher risk tolerance, practitioners will not learn, and thus will not become better at what they do. Risk aversion will inevitably compel people and organizations to be unnecessarily slow, unpersuasive, uninspiring, and thus ineffective.

Finally, there is a related aspect of irregular warfare that merits examination here. It is the question of whether the United States' civilian leadership understands the importance of personal relationships when crafting plans and conducting operations in the IW arena.

If one subscribes to the idea that influence is the basic coin-of-the-realm in most aspects of irregular warfare, and our adversaries certainly and aggressively take this approach then it should be axiomatic that IW practitioners and leaders must also become skilled and adept in establishing and nourishing the personal relationships that create that vital influence. In my experience, there are typically two approaches to creating influence.

The first is what is often referred to as the "transactional approach." As the name implies, this is based on creating relationships that are based on practical transactions. Here, practitioners garner influence by providing prospective partners something they believe to be of significant value. While useful, the influence gained through transactional activities tends to be temporary; it lasts only so long as the partners or targets continue to receive that value. It also tends to be brittle and a relatively small

disappointment or unexpected shock in the relationship can often break the influence being sought.

The second is much harder to create, but far more flexible, durable, and over time can even become permanent. This is often referred to as the "generous approach" where practitioners demonstrate a willingness to provide the prospective partner something of disproportionate value that exceeds what the partner is willing or able to reciprocate and demonstrates long-term the practitioner's long-term commitment to the relationship. In such an approach, the relationship typically requires years of presence to fully develop, not mere months. This approach usually generates a sense of gratitude that opens doors to establishing deeply personal, not transactional, relationships. Such relationships are often capable of delivering much more influence than transactional relationships typically can.

In theory, the practitioner should always seek to create personal, versus transactional, relationships In practice, however, the United States is often unwilling to deploy its people for sufficient time, and with sufficient support, to make a generous approach operationally feasible. There are exceptions to this, one example being the State Department's practice of keeping its foreign service officers abroad for multiple years at a time, often having them bring their families with them when conditions allow. Unsurprisingly, these foreign service officers develop a degree of knowledge, insight, and influence in their assigned country that is far superior to anything a temporary U.S. visitor can achieve.

Yet, if the United States is to be as energetic and serious as it claims to be in applying irregular warfare approaches to its most urgent national security challenges, should it not also consider such long-term assignments for all departments and agencies, and not just the State Department? Or, is the nation satisfied with the idea that our goals can be met by continuing to confine such long-term personal relationships to State Department or U.S. Agency for International Development officials who are too often the only Americans willing to commit to years of continuous and personal relationship development?

Admittedly, there are countervailing forces the United States would have to overcome. Family separation, and possible interference with a practitioner's access to advantageous professional development opportunities (e.g., a military officer's opportunity to attend staff or war college), are very real potential obstacles, but they can be surmounted if we decide that cultivating personal relationships abroad are truly, strategically, important. Such change would certainly be culturally, and perhaps even

politically, challenging for the government to embrace, but would the potential for strategic success, against daunting global challenges, not be worth it?

In closing, whether or not the ideas I have laid out here have any actual merit, I do hope they serve as an effective intellectual appetizer for the reader, and prepares them to receive the sumptuous main course that this publication offers both practitioners and policymakers alike.

The stakes for America are incredibly high, and as Abraham Lincoln once wisely pronounced at his own time-of-crisis-and-great-change in the 1800s, "[t]he dogmas of the *quiet past, are inadequate to the stormy present."*

About the Author

LTG (Retired) Michael Nagata served for 38 years in the U.S. Army, with 34 years in U.S. Special Operations Forces. His final assignment was Director of Strategic Operational Planning at the U.S. National Counterterrorism Center. His operational and combat experiences encompassed the Asia-Pacific region, north and east Africa, the Balkans, the Middle East, and South Asia. Today he is the Strategic Advisor for CACI International, and resides with his wife Barbara in Arlington, Virginia.

Introduction

Varsha Koduvayur, James Kiras, and Richard Newton

In October 2022, Congress created the Irregular Warfare Center (IW Center) to serve as a central mechanism for developing the irregular warfare knowledge of the Department of Defense (DoD) and to advance the understanding of irregular warfare (IW) concepts, and doctrine, in collaboration with key partners and allies.[4] Two of the five tasks assigned to the Center addressed facilitating whole-of-government and whole-of-society research related to the non-military aspects of irregular conflict. More importantly, though, Congress made the point that the DoD would occupy a *supporting* (emphasis added) role when it came to interagency activities related to strategic competition short of war, a significant reorientation of emphasis that should help the department prioritize resources and direct efforts related to strategic competition.[5] This book is the IW Center's first research contribution to assist that effort and to tackle the first of DoD's responsibilities toward IW: "make permanent the mindset and capabilities necessary to succeed in its current irregular warfare mission sets."[6]

It should be expected that after two exhausting decades of counterinsurgency in South Asia and the Middle East and a global counterterrorism campaign, our nation's security establishment is aching to do something different. Something different, it should be noted, that is more in line with the "business as usual" approach and institutional preferences of its Armed Service components.[7] Readers who can recall the decade after the Vietnam War ended, 1975-1985, will remember a similar strategic reorientation. Then, the United States shifted its defensive focus to AirLand Battle, and that doctrine's near-singular emphasis on deterring war with the Soviet Union.[8] Meanwhile, in Latin America, Africa, the Middle East, the Balkans, and across Asia, "small wars," often proxy wars sponsored by the two superpowers competing for influence, sprang up like mushrooms after a spring rain.

Similarly, during the 1990s, the U.S. military invested in the Revolution in Military Affairs, a concept of warfare dominated by information systems that would, in Colin Gray's words, allow the U.S. military to do "a better job of waging Desert Storm."[9] If one can draw a line, admittedly not a straight one, connecting these two examples and the current state of strategic affairs it is reasonable to conclude that

the conventional military prefers to avoid politically-motivated irregular conflicts, often waged in far-flung, austere, and hostile environments with promises that the latest technological panacea—artificial intelligence, hypersonics, and the like—will provide easy victories. It appears that our national security establishment is there once again, shifting the paradigm it established during the past twenty years to address the burgeoning conventional threats to international security posed by China and Russia, while appearing to avoid the extremely corrosive effects of their irregular and hybrid threats in regions of strategic importance. The core conceit of Congress's guidance that DoD should support the interagency community, non-governmental organizations (NGO), and the public sector in areas related to irregular conflict is that the Pentagon need not "own" every aspect of irregular warfare. Instead, the department only needs to figure out how to appropriately collaborate, support, and cooperate with the other departments and agencies, international agencies, and the nation's allies and partners.

The study of irregular conflict, and the means to prevent, mitigate, resolve, and recover from instances of a form of warfare the DoD defines as a "struggle among state or non-state actors to influence populations and affect legitimacy,"[10] is necessarily conducted through a whole-of-government lens, with significant input from both the public and private sectors. In the modern context of strategic competition, where the West, led by the United States, seeks to counter Chinese, Russian, and Iranian economic coercion, malign influence, and political aggression, while also remaining vigilant in the face of other persistent threats,[11] the chapters in this volume offer analyses and insights to help policy makers, security professionals, and researchers appreciate the complexities of the current evolving global security environment.

While this book rightly examines the future faces of irregular conflict, like Janus, the Roman two-facing god of doors, gates, and transitions,[12] it is helpful to acknowledge the past as we focus on the future. Classic military theorists, including Sun Tzu, Thucydides, Machiavelli, du Picq, Clausewitz, Lawrence, and J.F.C. Fuller, and the more contemporary Professor Gray, all noted the overwhelming importance and unchanging permanence of the human domain, an inherently unquantifiable dimension, when considering the nature of war. After two decades of "messy" and less-than-successful counterinsurgency operations, it is completely understandable that U.S. national security priorities would choose to focus on more quantifiable defense planning scenarios such as deterring conventional war with China or Russia, where comparative numbers and capabilities of land, air, maritime, and space systems offer metrics that politicians, generals, and Chief Executive Officers (CEOs) can debate using spreadsheets and PowerPoint® charts. But in doing so, they forget Janus, who

in Roman tradition was honored first before appealing to any other god, including Mars, the god of war. As the U.S. and its partners transition to a new era of strategic deterrence that is necessarily based upon numbers and technical capabilities, rejecting or ignoring the omnipresent irregular and hybrid threats to peace and security will be a tremendous mistake.

The classic theorists warned that in warfare the human dimension is "as three is to one" over the physical, a notion Gray reinforces by observing the American cultural overemphasis on the technological aspects of war*fare* to the neglect of the political and social dimensions.[13] This human dimension has taken on greater importance when considering the implications of contemporary strategic competition between the United States, China, and Russia where the antagonists often choose non-lethal hybrid, or irregular, threats—coercive economic policies, malign information operations, legal gamesmanship, cyber-attacks, political bullying, and proxy/surrogate warfare, in order to avoid direct confrontation between the global powers. The authors who contributed chapters have explored these issues to offer readers a concise volume, with interesting overlapping themes, as well as guides to further study.

Each chapter offers the traditional abstract to help you decide if the content addresses the questions that piqued your interest in this book. What is unique, though, is that the authors were asked to provide study questions, similar to what one might find in graduate courses, that the authors used to guide their research. We offer them to you to help you think through the authors' arguments, prompt questions of your own, and stimulate discussion with others. In addition, each of the chapter authors provided readers with a few recommended resources should their work spur you on to additional research.

Tom Marks and David Ucko from National Defense University's College of International Security Affairs set the stage for the book with their chapter, "Defining Irregular Warfare: Legitimacy, Violence, and Politics." They discuss the challenges of reorienting policy, doctrine, and practice away from the *armed* (emphasis in original) aspects of irregular warfare, for a U.S. military that naturally gravitates towards the kinetic aspects of conflict. Sean McFate then offers a provocative treatise on what he suggests is the "Maginot Line" ethos driving U.S. defense policy. The United States, suggests McFate, is still planning for and building formations and equipment to fight and win the Second World War, albeit with 21st century technology, while failing to address the realities of modern warfare, or conflict fought through other means. Tom Searle, a Senior Fellow at Joint Special Operations University, offers an alternative to

these perspectives in his first essay, "Towards a Better Irregular Warfare Strategy: A Contrarian View." Dr Searle counters by noting that the United States has had successes in its soft power approaches to past irregular conflicts, and therefore the nation's future irregular warfare security strategy should adopt a long-term approach that does not depend upon the DoD taking all the credit and resources. These three essays should cause thoughtful reexamination among politicians and the nation's civilian and military leaders who are charged with not getting future policies, strategies, plans, and doctrine "too wrong."

The book then offers a series of essays that examine the Chinese question from a variety of angles. Tuan Pham, a retired U.S. Navy captain who has been observing and reporting on China for more than twenty years, provides his insights into Chinese economic coercion using maritime militias as a cover for the Peoples Liberation Army Navy. James Sullivan, a Coast Guard Auxiliary officer associated with the Daniel K. Inouye Asia-Pacific Center for Security Studies, provides a financial perspective on Chinese economic coercion and options the West might consider for addressing this nuanced and insidious threat to peace and stability. J. "Lumpy" Lumbaca, also from the Asia-Pacific Center, provides a chapter detailing lessons learned from Chinese irregular conflict and proposes ways the United States might become more proactive in addressing Chinese aggression short of war.

Moving halfway around the world, Swedish authors Ulrica Pettersson and Hans Ilis-Alm from the Centre for Special Operations Research at the Swedish Defence University, and Karl Salum of the Baltic Defence College in Estonia, offer their perspectives on the challenges of having a resurgent and aggressive Russia as a neighbor. Their two chapters provide unique perspectives on the Baltic and Nordic approaches to comprehensive, or whole-of-society, defensive programs from professionals living under the threat themselves. It is their hope that others might learn from and adapt what the Baltic and Nordic nations have been successfully doing to meet their nations' security needs. Keeping with the European perspective, Christopher Marsh from National Defense University's Joint Special Operations Master of Arts program provides his excellent and timely observations on the current state of Russian irregular warfare. His perspective that Russia's approach towards irregular warfare is a function of both means and ways should be of particular interest. In his comparative study of Western and Russian approaches to irregular warfare, Chris finds the latter has had a more holistic view of the subject for historical and operational reasons, comprising as it does a "special" way of war.

The remaining chapters cover a number of bespoke topics that round out the themes of irregular conflict proffered by this book. Jonathan Odom, from the George C. Marshall European Center for Security Studies, offers an accessible and insightful discussion on Russian and Chinese legal gamesmanship, or how international law might be selectively used to advantage. Jonathan's point, that Western nations must abide by the conventions of international law even when our strategic competitors do not, succinctly describes the essence of the West's conundrum: how to compete and win against an opponent that plays by a less stringent set of rules? Tom Searle graces us with another offering, this one discussing the role of terrorism and counterterrorism in the spectrum of irregular conflict. Tom notes that al Qaeda and Islamic State sponsorship of local terrorist organizations confers benefits similar to those provided by sponsoring nation-states historically. While international law and conventions address state-sponsored terrorism, the complexities of dealing with a global *movement* that chooses to operate outside the law are fairly amorphous. Thus, politicians and security practitioners are and will continue to be challenged to appropriately address the irregular threats posed by global organizations that do not easily fit into accepted definitional "boxes."

One of the more unique chapters in this volume is offered by Sam Mullins from the Asia-Pacific Center. Sam looks at the implications of climate change as a driver of irregular conflict. He suggests that how we respond to climate change, geopolitical competition driven by climate issues, water insecurity, and climate-induced migration will exacerbate irregular conflict beyond that already caused by strategic competition for influence. Christian Ramthun, Devan Shannon, and Maurice Duclos, from U.S. Special Operations Command, ask us to reconsider how the United States should employ proxies as instruments of national security policy. They recommend using business and management concepts—principal-agent theory, outsourcing, and venture capitalism—to examine U.S. doctrine for proxy warfare and that by doing so military planners and decision-makers will be better positioned to interact with their counterparts in other government departments.

The remaining chapter, offered by Rick Newton and Jennifer Walters, considers the unintended consequences of readily available low-cost, user-friendly, and highly capable aerial drone technologies. Their chapter explores the future security threats posed by malign actors' misuse of technologies intended for beneficial purposes and asks readers to consider how these developments are changing and will continue to change the character of future modern warfare.

What the authors have delivered, and the IW Center has produced, is a collection of essays the editors believe will spark discussion and debate while also leading to further research—in other words, a vital step in keeping the IW mindset alive inside and outside of DoD. We invite you to consider the diversity of opinions and variety of perspectives that constitute this first volume in the IW Center's book series.

Defining Irregular Warfare: Legitimacy, Violence, and Politics[14]

Thomas A. Marks and David H. Ucko

ABSTRACT

After two decades of concentration on non-state actors as the principal threat to national security, the United States has returned to a focus on strategic competition between state powers. The emphasis on *competition* as opposed to *conflict* reflects the renewed weaponization of statecraft below the threshold of war. The resultant ambiguity of attack, as well as of response, has in some corners brought attention to "irregular warfare," a term that originally reflected concerns with insurgency and counterinsurgency but that is now being redefined for this new strategic era. As vocabulary and concepts guide our assessment and action, this chapter frames irregular warfare in a way that subsumes the term's traditional purpose but that also allows it to be applied meaningfully to inter-state struggles. Emphasis is placed on legitimacy, violence, and politics, as it is within the elucidation of these aspects that irregular warfare finds its value. It follows that while irregular warfare is certainly a feature of strategic competition, not all strategic competition is irregular.

Introduction

After two decades of concentration on non-state actors as the principal threat to national security, the United States has been thrust into a "back to the future" moment of renewed focus on various state competitors. In one sense, we have been here before.

The Cold War featured the same primary foes—China, Russia (then the Soviet Union), North Korea, and Iran (a post-1979 latecomer)—with several others now dropped by the wayside, such as Cuba and Vietnam. The radical political forces that had succeeded in seizing power in these states had simply turned their sights towards regional and worldwide targets, thus confronting the international norms and order favored by the United States. Their approach blended kinetic and non-kinetic lines of effort to achieve their ends. It was, as Mao Tse-tung stated explicitly myriad times, "people's war" waged globally.

This, of course, is where we find ourselves again. Failure to consolidate victory in the Cold War, enabled by strategic drift and hubris, has renewed the struggle. This time, though, we are calling it great power, or simply strategic, competition. The emphasis on *competition* as opposed to conflict reflects the renewed appearance of what has been part of threat doctrine for more than a century, namely the weaponization of instruments of statecraft below the threshold of war. Though violent clashes are a given, they are normally conducted through proxies and sponsored units rather than directly between the states themselves. The resulting ambiguity of these attacks, as well as of appropriate response, has in some corners brought renewed attention to "irregular warfare," seen then as a method of competing short of another world war. Others have resuscitated what George Kennan c, at the dawn of the Cold War, as "political warfare," namely the application of war-like logic in times of peace.

In a sense, the more things change, the more they stay the same. Internally, or within states, irregular warfare is as it has been previously conceived; externally, or between them, we find ourselves grappling with a strategic approach that has long been used by our adversaries, yet which challenges us given our legacy vocabulary and structures. The terms of the trade matter, because while imperfect, they guide our understanding and our preparedness to respond.

To add clarity to an important discussion all too often mired in confusion, this chapter conceptualizes irregular warfare within a context of inter-state competition. It first grounds irregular warfare in its crucial etiology, or the reasons for its coinage, revealing in this manner the conceptual confusion that surrounded the term during the so-called War on Terror. On this basis, the chapter then explores the helpful contributions of irregular warfare in an environment of strategic competition, emphasizing throughout the term's traditional concern with questions of legitimacy, of violence, and of politics. indeed, it is the convergence of these aspects, and with the admixture of narrative and spin, that makes irregular warfare so crucial and complex.

Today, this complexity is compounded by the international development of associated conflicts. Even then, though irregular warfare is a feature of strategic competition, not all strategic competition is irregular.

A Particular Slice of Political Violence

Irregular warfare (IW) deals with a particular slice of political violence—in reality, it is "violent politics." The oft-published official graphic contrasting regular war with IW is correct as far as it goes (see Figure 1). In present American and NATO doctrinal conceptualizations, regular war takes as its focus the neutralization of the foe's military, to allow us to impose our will on its government. In IW, the focus shifts to the relationship between a state, represented by its government, and its populace. This necessarily means IW focuses upon the political relationship between those who govern and the populace, or upon the legitimacy of governance. The "violent struggle for legitimacy" that once dominated the official Department of Defense (DoD) definition of IW reflected a strategic effort to eliminate the opponent by undermining its sources of credibility, and thereby also its resolve and capabilities. Legitimacy is therefore considered the center of gravity, with the object of analysis shifting to its generation, or – put differently – how the political opportunity structure has produced and sustains the threat.[15]

In contrast, the legacy focus in professional military education (PME) is upon *the armed threat*. Center of gravity analysis, to take but the most salient illustration, takes as its object enemy forces and is minimally concerned, if at all, with the factors that drive conflict and political mobilization. Within such a paradigm, it naturally follows that defeating violent challenge is most often a matter of kinetics.

The challenge faced in integrating IW into such a matrix quickly becomes apparent. IW is not a weapon. It is a term given to a form of political violence that is unlike that which is called "regular" conflict. The latter raises armed action to a level which conflates it with war itself, the former subordinates violence to achieving a political objective. The operational art of IW is realized via multiple lines of effort (LOE), just one of which is violence.

The 2001 declaration of the Global War On Terrorism (GWOT) further muddied the waters, with all manner of political, and often even criminal, violence termed "terrorism." The rush of policymakers and academia to embrace this misdirection was well-nigh universal. Whether conflicts were those involving main force deployment, advisory, or even stand-alone partner efforts, such as in Sri Lanka, they were

terminologically characterized as "wars on terrorism." This was incorrect and unhelpful.

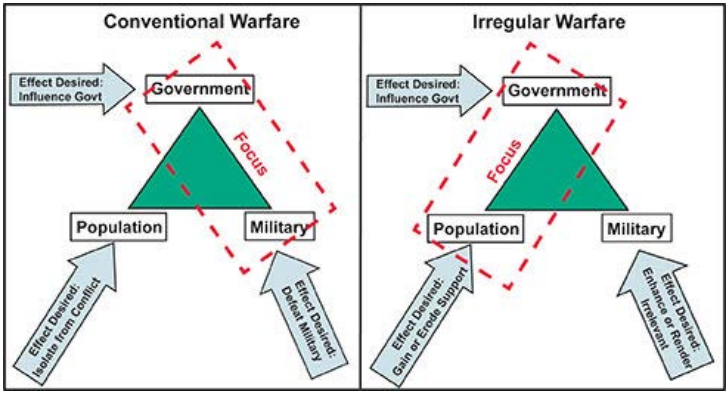

Figure 1. Conventional (Regular) versus Irregular Warfare as per U.S. doctrine

Terrorism, to be clear, as set forth both in doctrine and academia, was always considered a violent challenge to the existing order, exercised by non-state actors. There is however a categorical difference between terrorism as a "logic of action," where it is the driving force of strategy and swallows all else, and terrorism as a "method," as used by insurgents alongside other efforts.[16] When exercised as a logic of action, terrorism will alienate the very social base the political project purports to advance. This is what allows for traditional counterterrorism to focus on the perpetrators, rather than the "violent politics" at hand. With terrorism as a method, however, a narrow focus on rooting out "the terrorists," to the exclusion of finding political answers to sources of conflict, often leads to new cycles of violence that an operationally astute challenger will exploit to mobilize additional support. In both, innocents are targeted to produce political effects, especially in terms of messaging, but neither can be dealt with as a solely military mission.

From this illustration, it can immediately be discerned that responses should be driven by where a threat stands in the continuum of violent politics. The objective for insurgents, working from the ground up, is to apply their strengths against the government's weaknesses and to avoid the application of government strength against their own vulnerabilities. The goal behind such threats is to alter

the existing political distribution of power, as defined by rights, resources, privileges, and obligations. Violence necessarily starts small and grows larger, to whatever level is deemed necessary to realize the project at hand.[17] The struggle of "national liberation" in Vietnam often rose to the level of regular warfare (using attacks by battalion or higher formations as the metric). It also, during the French phase (1945-1955), could have involved nuclear war—had Paris' request for relief of Dien Bien Phu taken that course—and often did involve, during the American phase, chemical warfare.[18] The broader point is that whether the irregular actor uses full-scale conventional maneuver, terrorism, or even weapons of mass destruction, the violent line of effort is but one component of the struggle, and not necessarily even the most strategically relevant.

This would seem obvious, but in our response to irregular warfare, we often miss the strictly contingent nature of violence and instead focus overwhelmingly on this supporting action, thereby missing the structural context of the confrontation. Unsurprisingly, therefore, America's response has been most effective where the political foundation has required less urgent redress. Thus, our miscues in Iraq and Afghanistan transpired even as we did reasonably well in other conflicts, ranging from the Philippines to Colombia to Kurdish Iraq and Syria. On the whole, the more a political alternative to an existing order is able to mobilize a following, the more the scale is weighted against our armed tactical repertoire of response. "Small footprint" efforts are relatively successful because they necessarily approach the situation from its socio-economic-political basis. This is the essence of foreign internal defense (FID), assisting a partner or ally to defeat attempts to seize power in their countries.

The mention of FID forces consideration of how else IW has been (mis) understood, namely as an aggregate of its five traditional activities, where FID sits alongside counterinsurgency (COIN), counterterrorism (CT), unconventional warfare (UW), and stability operations (SO).[19] Where FID describes the efforts of an advisory government to assist another, COIN speaks to the application of military and other assets to combat rebellion within one's own country. In both FID and COIN, counterterrorism (CT) is almost by default a component. Conversely, unconventional warfare (UW) implies foreign support to a local resistance movement seeking the overthrow of an illegitimate or occupying government. Finally, in states shattered and in need of reassembly, we may engage in stability operations (SO), often characterized as "COIN with less incoming" (i.e., fewer heavier weapons being used by the residual threat actors).[20]

This grouping stems from the major irregular missions that supported the main effort in World War II. The fly in the ointment should be immediately clear. Created to

differentiate between what was normal or "regular" in armed forces tasking, and what was auxiliary or "irregular" (frequently requiring forces special in some manner), these categories cannot serve as a coherent basis for strategy, or even military deployment. The problem in the Vietnam case, for example, was that commitment of U.S. regular forces came only in 1965, after a decade of unsuccessful advisory (FID) efforts. By that time, the enemy had already recreated the template that had proved so successful against the French from 1945 to 1955, namely a synthesis of several forms of organized violence—terrorism, guerrilla, and main force—embedded in a broader strategy of political warfare (as labelled by the threat). At one end of the spectrum, the state was involved in counterinsurgency (COIN), with outside assistance (FID), at least one component of which supported minority elements of the populace in special units (UW), and was required to deal with terrorism (CT), augmented by guerrilla warfare, directed at eliminating obstacles to the revolutionary political project, especially the armed local representatives of the state (the police). At the other end of the spectrum, insurgent regular military power lay ready to inflict defeat the moment security forces dispersed to attempt protecting the populace or secure critical infrastructure (i.e., "regular warfare").[21] Of greatest irony was the presence, throughout the war, of "neutral" military observers supposedly supervising a peace agreement, thus involved in their own stability operations (SO).

Whereas these five component terms for IW activities are doctrinally useful, they do not entirely define the business at hand, which is meeting the threat challenge posed by a systemic legitimacy crisis. Violence only enables such challenges. The underlying legitimacy crisis, however, emerges from a structural inability to deal with individual grievances, hopes, fears, and aspirations. That a challenge exists does not itself make it legitimate, but individual and group action has certainly emerged from structural friction, albeit allowing for the role of chance (contingency) as opposed to deliberate design (agency). It is this structural friction which is exploited in irregular warfare to control or co-opt contested populations, be it phrased in terms of common interests, united fronts, ideological appeal, support, or credibility.

Legitimacy, in this context, is not a popularity contest, but refers instead to the perceived right to lead. This right can be secured through coercion, creating a negative form of legitimacy, but the most potent adversaries strive to combine such coercion with strategies of co-option, thereby reducing the cost of doing business and achieving more sustainable results.[22] Indeed, with legitimacy, there is strong potential for mobilization—of people, allies, support, and momentum. Without legitimacy, the effort required to consolidate a new political reality rises exponentially. In any irregular

confrontation, therefore, a key requirement is to map the system (or pathways, if one favors such terminology) that has resulted in conflict and then focus upon structural reform of the relevant drivers. Armed power provides the shield allowing such reform to occur, regardless of the precise form that protective power takes.

We occasionally perform such mapping, but our recent debacles in "Big Green" efforts, as they are often termed to emphasize the central role asserted by the conventional U.S. Army, highlight that even when the United States talks a good political game we simply do not execute. The result is that we are invariably "surprised" and then must dig ourselves out of a proverbial hole. In contrast, our cases of success stem overwhelmingly from becoming involved in conflicts where partners have been astute enough to utilize us for support, as they engaged in politically-driven responses. It is these cases which must lead in our instruction, with "Big Green" miscues used to demonstrate why we too often fail even as other, less-sophisticated militaries often succeed with our assistance.

If we summarize the instructional challenge, then, we have in our doctrine, within our own stove-piped world, already come up with a reasonably correct vocabulary and set of concepts for IW. We recognize, for instance, that legitimacy is the subject and that these conflicts are quintessentially about mobilization and influence, with violence thrown in. Yet, we muddle these understandings in professional military education by failing to focus upon armed action as but a shield for socio-economic-political empowerment.[23] We do this, because we ask tacticians to teach strategy, rather than integrating all levels of instruction (tactics, operations, and strategy). Our case studies come overwhelmingly from the colonial world (e.g., the reliance upon the French in Algeria) and do not focus upon the present world created, tangibly and intangibly, by globalization. That world, with its compression of time and space that is exacerbated and transformed by new technology, has only accelerated the political violence occurring beneath the threshold we treat as "war."

Irregular Warfare in Strategic Competition

Despite ample experience, the United States abandoned the GWOT with a curiously incomplete understanding of irregular warfare. Overly focused on the direct application of military force, concerned mostly with its own interventions in Iraq and Afghanistan, and missing the plethora of other cases and dimensions that would have completed the picture, the United States is now experiencing a renewed period of forgetting, akin to the reorientation post-Vietnam, in which widespread understanding of irregular warfare could vanish.

Ironically, while efforts to forget counterinsurgency are certainly underway, it was just as the United States embraced "great power competition" that the study of irregular warfare experienced a renewal of sorts. In 2018, long after counterinsurgency had become toxic, the U.S. *National Defense Strategy* devoted an annex to IW, the only annex in the publication, seeking to develop and institutionalize related capabilities.[24] In a similar vein, the Chairman of the Joint Chiefs of Staff made IW an "enduring special area of emphasis" in 2021, meaning (in theory) that U.S. armed forces must study, learn, and prepare for it, indefinitely. The results of either action are debatable. Still, what can explain this belated ascendance of IW after two decades of intense focus on just such missions?

The answer to this question reveals the confused nature of the discourse surrounding irregular warfare today. It is for example commonly heard that the United States military focused too heavily on counterinsurgency and counterterrorism in the post-9/11 years and that it must now learn irregular warfare instead, even though the latter doctrinally subsumes the former. The U.S. system, it would appear, is intent on sustaining irregular warfare as a helpful lens through which to understand strategic competition against state adversaries, while abandoning those parts of the enterprise that are too closely associated with past counterinsurgency failures.[25] This selectivity is puzzling, because as a past DoD *Joint Operating Concept* emphasized, "insurgency and counterinsurgency are at the core of IW."[26] It is also dangerous, in that should IW shed its grounding and etiology (that which it has always been used to describe), it can in effect be used to describe largely anything, and thus nothing.

Given the confusion at hand, it is worth asking what precisely irregular warfare means as a component of great power, or strategic, competition. We have discussed how, within its original application, IW described the effort of sub-state actors to offset their military inferiority by targeting the legitimacy of the status quo, thereby mobilizing power to eventually compete with and overthrow *l'ancien régime*. How does a comparable phenomenon unfold between rather than within societies?

Answering this question requires engaging with the definitional criteria of irregular warfare and applying these, as neatly as possible, to the vagaries of inter-state competition. Three criteria stand out. First, irregular warfare inherently describes the *mobilization of some against others*, using issues that

animate support, anger, and alienation as wedges. Irregular warfare arises because direct approaches are deemed too hazardous, and so energy is focused instead on the foundations of the status quo and creating a new world that the powers-that-be cannot resist. It follows that irregular warfare is fundamentally about politics, about "who gets what, and when," which is why it is so firmly anchored in competing visions for society. In IW, therefore, multiple lines of effort are deployed and combined to mount a comprehensive and systemic attack.

Second, *violence* is inherent to irregular warfare, in that it separates this type of confrontation from sharp-elbowed politics. The entailed violence can come and go, it can escalate and subside, but it remains a key feature of how the struggle unfolds and fundamentally alters its character. What is so often missed in analysis is that the violence in irregular warfare can rise to the level of major combat operations. For example, witness the fierce fighting between the government of Colombia and FARC insurgents (*Fuerzas Armadas Revolucionárias de Colombia*), or the government of Sri Lanka and LTTE insurgents (Liberation Tigers of Tamil Eelam), or indeed even the pitched battles of the American Civil War. Conversely, violence can also be latent, or implied, but still shape behavior and expectations. Indeed, military intensity may rise or fall, but this concerns only the correlation of forces and does not negate the nature of irregular warfare as a violent political contest. This anchoring in violence is necessary to give significance to the use of "warfare" in IW and to make this problem-set a military priority. Indeed, albeit a political phenomenon, IW is almost exclusively discussed within military contexts.

Third, the most important definitional criterion of IW is the strategic intent: *to erode or build legitimacy and influence*. The project must be understood at this strategic level, as it is this intent and focus that informs the purpose and logic of subsidiary actions taken, be they seemingly peaceful or obviously belligerent. When an insurgent group is providing medical services, or distributing aid, it is for the same strategic reasons as it engages in terrorism and violent attack: to build or erode legitimacy and forge a path to victory. When a group quietly and nonviolently mobilizes societal support, it is to assist their eventual seizure of power. The broader project, and intent, is irregular warfare.

Given these three criteria, what can be said about the role of irregular warfare within strategic competition? By hemming the conversation within the confines of IW's etiology, it is possible to answer this question more precisely. Specifically, at the international level, irregular warfare would imply a national government sponsoring terrorism and insurgency abroad, acting to subvert the societal integrity of targeted

states. It weaponizes frames and narratives to affect credibility and resolve, and it exploits societal vulnerabilities to fuel desired political change. The chief difference between irregular warfare as traditionally understood, and as applied to strategic competition, is the role of third-party states in stoking the fire. Thus, while the competition for legitimacy unfolds domestically, within an individual state, it also unfolds globally, as part of an international search for power and position. Response, in turn, must consider the sources of resilience and resistance within the targeted states, but also of the international system that is under attack.

It follows that irregular warfare informs strategic competition, but not all strategic competition is irregular warfare. Specifically, there is a key distinction to be drawn between irregular warfare—as a violent competition for legitimacy—and "political warfare," an adjacent, but distinct, term that describes the weaponization of *non-military* means to prevail strategically *without fighting*. As George Kennan put it in his famous cable of 1946, at the dawn of the Cold War, political warfare is "the logical application of Clausewitz's doctrine in *time of peace.*"[27] In practice, political warfare today includes economic pressure, disinformation, lawfare, intellectual theft, "wolf warrior diplomacy," and political infiltration, among other things. This weaponization of the "ordinary" instruments of state—trade, commerce, diplomacy, information, and the rule of law—mounts an analytical and institutional challenge to the American interagency, most of which is either not authorized, resourced, or mobilized for an effective response. Yet, unless folded into a broader IW strategy that meets the criteria set out above, political warfare is not in itself irregular warfare.[28]

This point may seem pedantic, but has important policy and strategic implications. Much as an insurgent's use of "non-violence" (propaganda, subversion, lawfare, and the like) could in theory support an IW strategy also marked by violence and armed mobilization, so could a state's use of political warfare contribute to a broader IW strategy seeking gradual global domination. The requirement for appropriate response lies in mapping the entirety of the strategy, that is, each line of effort, and querying how they fit together and what they seek to achieve. Only at that point is it possible to craft an appropriate response. On that front, the sponsorship of insurgency and terrorism abroad will call for different skillsets and authorities than responding to political warfare in isolation. Responding to both simultaneously, on the other hand, will require significant flexibility and guile. This is the challenge at hand.

Conclusion: Global Insurgency and IW in Strategic Competition

The United States is engaged in a struggle to retain its power and legitimacy. American leadership has waned since the end of the Cold War, with Russia and China, detecting a void, asserting themselves...not only as regional powerhouses, but also globally and with the intent to challenge, even surpass, the United States. Yet, unlike the great wars of the 20th century, shifts in power are today more discreet, incremental, and multifaceted in both method and effect. As demonstrated amply by the stark Russian attack on Ukraine in February 2022, the undisguised use of force is likely to generate a swift backlash and play into America's strengths. By contrast, the proper exploitation of influence, narratives, and ambiguity, such as those Russia employed during its 2014 takeover of Crimea and eastern Ukraine, sows the seeds of doubt, delays reaction, and creates the conditions for the effective use of force, should it be deemed necessary.

In a sense, the more things change, the more they stay the same. Even the late Osama bin Laden, and his al-Qaeda (AQ) organization, effectively illustrate the internationalization of irregular warfare, though the label back then was "global insurgency." As is now well known, AQ terrorist acts were, and continue to be, instrumental in the sense that they were intended to spark mass mobilization within the Muslim world. Thus, bin Laden was an insurgent using terrorism as a method, as one tactic of many, which while often dominant was still wrapped within a strategy similar to that of Che Guevara. In fact, one translation of the Arabic "al Qaeda," traditionally given as "the leaders" or "the base," could also be *foco*, as per Guevara, with the same meaning but applied to a global guerrilla revolutionary movement.[29]

What unfolded, then and now, is similar in many structural respects to what occurred during the Cold War, with both states and various political parties playing the role of AQ as sponsor and would-be leader of globally distributed struggles. The role of Moscow and the COMINTERN (Communist International) comes immediately to mind. When this view is expanded to include the relationships between the Soviet Bloc and various terrorist groups in Western society, there is a strong sense of "déjà vu all over again," although this was hardly the received wisdom of the previous two decades.

This logic is similar to that of the states now determined to overturn the existing global order. This seems a stretch only if one has been able to avoid the extensive disinformation campaign commissioned and implemented by Moscow, Beijing, Tehran, and Pyongyang. Regardless, this framework has remained consistent throughout the

three-quarters of a century since the Second World War. Irregular Warfare, then, not only unfolds domestically, within individual states, but also globally, as revisionist states amplify the contradictions of local and international norms to build influence and support.

What is required in response is a strategic construct capable of elucidating the challenges and pointing towards potential ways forward. The definition of irregular warfare must account for the simultaneous internationalization and localization of such struggles, without betraying its etiology and conceptual contribution. In previous work, we proposed the following definition:

> Irregular warfare is a coercive struggle that erodes or builds legitimacy for the purpose of political power. It blends disparate lines of effort to create an integrated attack on societies and their political institutions. It weaponizes frames and narratives to affect credibility and resolve, and it exploits societal vulnerabilities to fuel political change. As such, states engaged in, or confronted with, irregular warfare must bring all elements of power to bear under their national political leadership.[30]

This way of understanding irregular warfare respects the origins of the term, but also applies it to a new strategic environment. It retains the lessons of two decades of involvement in irregular warfare, yet allows for the internationalization of irregular struggles within a global competition for power. In seeking to capture irregular warfare, it does not demilitarize the term, but instead insists on coercion as a core component, thereby justifying its martial connotations and giving the armed forces a natural role to play. Its crucial retention of legitimacy as the center of gravity, however, also strongly implies that whatever the Department of Defense does must be in support of civilian actors and political strategies.

About the Authors

Dr. Thomas A. Marks is Distinguished Professor and MG Edward G. Lansdale Chair of Irregular Warfighting Strategy at the College of International Security Affairs

of the National Defense University, Washington, DC. He assumed his present rank and position on 1 July 2016, after 12 years as the founding chair of the War and Conflict Studies Department and professor of terrorism at CISA. He was asked to occupy these positions following the attacks of September 11th because of his extensive academic and field experience concerning irregular warfare strategy and operations.

Dr. David H. Ucko is professor of international security studies at CISA, where he also serves as chair of the War and Conflict Studies Department. Dr. Ucko's research areas include political violence, irregular warfare, counterinsurgency, and war-to-peace transitions. He is the author of *The Insurgent's Dilemma: A Struggle to Prevail* (Hurst/Oxford University Press, 2022) and four other books on irregular warfare and political reintegration. He has also published on the United Nations, North Atlantic Treaty Organization, countering violent extremism, and counterinsurgency in a range of peer-reviewed journals.

Discussion Questions:

1. Assess the implications of framing contemporary strategic competition with the legacy vocabulary and concepts of Irregular Warfare (IW), in particular as it relates to the role of violence and the "struggle for legitimacy."

2. What is the value in distinguishing between traditional and irregular warfare, or between irregular and political warfare?

3. If Irregular Warfare is about politics and legitimacy, what should be the role, authority, and capabilities of civilian government agencies for any country seeking to defend against such a challenge?

4. Consider the implications for national strategic planning created by elevating competition to the status of a security concern as opposed to a matter of policy.

Recommended Reading:

- David H. Ucko and Thomas A. Marks, *Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action*, 2nd ed. Washington DC: National Defense University Press, September 2022.
- David H. Ucko and Thomas A. Marks, "Redefining Irregular Warfare: Legitimacy, Coercion, and Power," *Modern War Institute*, October 18, 2022, https://mwi.usma.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/.

- Kevin Bilms, "What's in a Name? Reimagining Irregular Warfare Activities for Competition," *War on the Rocks*, January 15, 2021, https://warontherocks.com/2021/01/whats-in-a-name-reimagining-irregular-warfare-activities-for-competition/.
- Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism* 7, no. 4 (2018), 30-47, https://cco.ndu.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/

Irregular Competition: Contemporary Lessons Learned and Implications for the Future of Irregular Warfare

J. "Lumpy" Lumbaca

ABSTRACT

Irregular competition is defined here as "state and non-state actors proactively engaging in activities to influence populations and affect legitimacy during times of peace, competition, and conflict." America's state and non-state adversaries operate effectively with malign intent in this ambiguous space, while the United States is typically in "react" or "counter" mode. Along the same lines, America underperforms in initiating its own aggressive and proactive irregular competition activities. Derived from multiple-case study research, the author presents contemporary irregular competition lessons learned and introduces: (1) a theoretical model for how the United States and its partners may conceptualize irregular competition; and (2) practical recommendations for proactive irregular competition execution.

Defining the Problem

While irregular competition may not be the top priority for America's security enterprise today, there is nevertheless room for the United States to more effectively and efficiently implement this important tool in concert with other national security initiatives. Irregular competition is defined in this work as "state and non-state actors proactively engaging in activities to influence populations and affect legitimacy during times of peace, competition, and war." This is the author's definition but is admittedly a hybrid of others. Irregular competition, performed in a vacuum, would be unlikely to elicit a major kinetic response. It involves diplomatic, informational, military, and economic (DIME) initiatives by way of indirect approaches. Cultural, religious, legal, psychological, historical, and other factors among diverse populations must all be taken into account in this ambiguous environment, where awareness is often more important than military power.[31]

Terms such as irregular, hybrid, gray-zone, fourth-generation, new-generation, asymmetric, compound, political, and unrestricted "warfare" are often used interchangeably to describe this complex operating space. Defining the specific *thing* this chapter is about is challenging. Ask anyone in the U.S. national security enterprise if America should have some type of irregular or hybrid warfare capability, and the answer will likely be "yes." However, ask people to define precisely what that might mean, and the answers received will be inconsistent. Definitions are important and necessary, but agonizing over them may inhibit moving the discussion forward. Debating which definition is most accurate is not an objective of this paper. This is one reason why a relatively unfamiliar term – *irregular competition* – is introduced, to avoid preconceived notions and biases that may accompany the other, more commonly used, terms. Compounding the matter further, America's adversaries and partners understand the concept differently than the United States does. A common term used by everyone to describe such a complex space does not exist. Moving on to *discussing* rather than *defining*, this work focuses on the overarching *idea* of irregular competition rather than concern for any specific doctrine, dogma, definition, or preferred terminology. As Carl von Clausewitz said, "Again, unfortunately, we are dealing with jargon, which, as usual, bears only a faint resemblance to well-defined, specific concepts."[32] Those who are well-read on U.S. doctrine will immediately realize that the definitions presented throughout this study are a hybrid of many things. The reader is asked to focus on the overarching idea of Irregular Competition. As U.S. Army Colonel (Retired) Robert "Bob" Jones said about this matter, "[w]e can define our way to failure or understand our way to success."[33]

This study uses the terms "friendly" and "adversarial" irregular competition. "Friendly" can be understood simply as a characterization of activities undertaken by the United States and its friends, partners, and allies. The use of irregular competition in the "adversarial" sense is meant to characterize the activities of Russia, China, North Korea, Iran, and violent extremist organizations, also known as the "four-plus-one."[34] The way that friendly nations and adversarial nations approach irregular competition are similar at times and dissimilar at others.

Awareness of adversarial irregular competition is on the rise. It is discussed often in Congressional testimony,[35] in think-tank research,[36] and in the mainstream media. Reporting on real-time irregular competition happens around the world every day. Because of this, why is the United States not taking irregular competition more seriously, doing more to mitigate adversarial use of it, and implementing its own proactive campaign to complement ongoing strategic competition initiatives? Why is the United States less willing to employ irregular competition activities as freely as the Chinese Communist Party (CCP) or the Kremlin? The United States, unlike several of its adversaries, is much less resource-constrained, so funding is unlikely the limiting factor. Adm (Retired) Mike Rogers, former commander of U.S. Cyber Command and director of the National Security Agency (NSA), along with Hoover Fellow Dr. Jacquelyn Schneider, provided insight into this line of questioning. In summary, Rogers and Schneider stated that the United States is reluctant to aggressively engage in this space: (1) for fear of escalating situations into conflict; and (2) because of the extreme bureaucracy that is involved in the approval of such activities.[37] These reasons are likely flawed, however. The two experts explained that these types of aggressive, proactive, irregular activities—tested through simulations and real-world analyses—are less likely to escalate matters into conflict in the same way that escalation takes place with conventional or nuclear weapons.[38] Despite these reassurances, the U.S. remains hesitant to employ proactive measures in this ambiguous environment. In summary, the United States incorrectly estimates the opportunity cost to be too high and therefore remains self-constrained in its willingness to engage in effective irregular competition.

Adversarial Irregular Competition Demonstrated

While irregular competition has been employed in various forms for centuries,[39] this work is focused on the late 20th century onward. America's adversaries, enabled by emerging technologies including cyber and space capabilities, have advanced rapidly and are adept at operating in this irregular competition space. As former White House

National Security Advisor LtGen H.R. McMaster emphasized throughout his book *Battlegrounds*, malign actors synergize—like never before—disinformation, denial, disruptive technologies, coercion, and other tactics to accomplish strategic objectives below the threshold of what might elicit a military response.[40]

The following examples are provided to help paint a conceptual picture of what irregular competition often looks like. Illustrations of irregular competition originating from the CCP alone include graduated island-building, intrusive fishing fleet intimidation, and debt diplomacy exacted with other measures of economic coercion throughout the Indo-Pacific, along the Silk Road, and into Africa to influence state behavior in ways beneficial to China.[41] Other examples include economic espionage and theft of intellectual property,[42] military intimidation of Taiwan, funding research on alternative approaches to international law to rewrite history, [43] efforts to influence politics in Australia and New Zealand,[44] hostage diplomacy,[45] seizing unmanned underwater vessels,[46] internment and genocide of Uighurs in Xingjian to cleanse Chinese soil of foreign cultures,[47] co-opting small countries in Southeast Asia,[48] river patrols, casinos, and the establishment of Chinese micro-communities in the Mekong River Basin to exert influence on host nations, strong-arming the extradition of overseas critics back to China, and influencing foreign media, sports, and Hollywood organizations[49] to maintain a positive image of China.

In the case of Russia, irregular competition has become a steady state endeavor. This can be seen in the employment of the Wagner Group[50] and other non-uniformed proxies in Syria, Ukraine, Georgia, Estonia, and elsewhere, employment of the Night Wolves motorcycle gang to execute information operations and proxy conflict in Australia, Bosnia, and Ukraine,[51] election meddling in Europe and America, financing foreign political parties like the repressive Maduro regime in Venezuela,[52] energy coercion, flying close to U.S. warships in attempts to elicit an overreaction, cyber-enabled disinformation campaigns,[53] and the poisoning of critics.[54] The case of Russia's illegal invasion, and attempted genocide, in Ukraine contains acts of irregular competition occurring simultaneously with conventional military maneuvers.

Other actors like Iran sponsor terrorism globally, often through proxies. Iran also illegally transfers and sells weapons,[55] and routinely uses armed small boats to harass UK and U.S. warships.[56] North Korea utilizes irregular competition by routinely threatening other nations with nuclear devastation, which has resulted in it being designated as a state sponsor of terrorism,[57] as well as successfully assassinating individuals considered to be a political threat.[58]

From a position of weakness, non-state actors often employ components of irregular competition to gain a relative advantage over better-resourced adversaries. These initiatives include but are not limited to: disinformation campaigns to purport government illegitimacy, propaganda initiatives to incite violence, money laundering,[59] the creation of shell companies/fake non-governmental organizations (NGO) to support terrorism, the use of piracy, kidnap-for-ransom, cyber-crime, and other forms of transnational organized crime to raise funds for illicit operations,[60] sarin attacks on public transportation,[61] and online radicalization to recruit new members.[62]

Numerous other examples of irregular competition abound from countries and organizations, so the above list should be considered only a partial one. The examples provided are meant to remind the reader of the tremendous depth and breadth of this elusive operating environment.

Case Studies, Lessons Learned, and Practical Recommendations

The author conducted research on three cases of irregular competition to support this work. After an extensive case study selection process, research took place, data was collected, coded, and analyzed, and the results were interpreted. The data from this process is not included in this publication because of editorial limitations. However, the author will gladly share the complete information with anyone interested. In addition, the unabridged data will eventually be published elsewhere for the purposes of transparency, replication, and further study. For this publication, lessons learned, corresponding recommendations, and an irregular competition conceptual model derived from the analysis are provided.

Two of the cases studied focus on the "friendly" use of irregular competition. They include an examination of U.S. activities aimed at the Soviet Union in Afghanistan from 1979-1989 and U.S. activities directed toward Iran from 1979 to 2021. A third case involving CCP activities in the Philippines from 2012-2021 is used to understand the "adversarial" use of irregular competition. The lessons learned, and associated practical recommendations, are provided below.

Lesson Learned #1: All States Are Employing Irregular Competition to Some Degree

Irregular competition is common among states who are dissatisfied with some aspect of the status quo and are "determined to change aspects of the global distribution

of power and influence in their favor."[63] Those employing irregular competition prefer it as one strategic option to challenge—and ultimately change—the way global politics work without eliciting unacceptable cost and attention.[64] These activities are often implemented through gradual steps small enough to go unnoticed. In other cases, the irregular competition activities are substantial enough to be noticeable but seemingly inconsequential, so they do not cause alarm. Overall, irregular competition is an instrument that may be used to pursue geostrategic objectives while minimizing the risk of major conventional military escalation.

Practical Recommendations Emerging From Lesson Learned #1:

America's adversaries employ irregular competition regularly, and the United States should expect this to continue. As Tobias Burgers and Scott Romaniuk wrote: "China's real takeaway from the war in Ukraine is that irregular competition is best. The steep costs of Russia's invasion of Ukraine will bolster China's continued use of its effective salami-slicing and irregular tactics."[65] Irregular competition activities are cost-effective, unlikely to provoke a major military response by themselves, and are difficult to call out since they are gradual in nature and thus difficult to deter.

The U.S. approach to irregular competition should focus not only on reacting to adversarial activity but also on the American use of proactive irregular competition measures.[66] Decision-makers should consider whether they are truly in a state of "peace" and, as a result of this questionable assumption, not inclined to initiate actions that they fear America's adversaries may consider provocative."[67] As Seth Jones has written, America must engage in both defensive *and offensive* activities [emphasis added] "to advance U.S. interests and deter its adversaries from aggressive actions." This proactive approach must transcend tactical actions and embrace a comprehensive irregular competition strategy that supports overarching strategic objectives.[68] However, before doing so, America must acknowledge that proactive irregular competition involves risks. Using the Cold War as an example, it is important to remember that America would never have succeeded in undermining Soviet power and influence "without taking prudent risks that exploited its adversary's vulnerabilities."[69]

The United States must "get over its obsession" with conventional conflict.[70] This is not a "fool's dilemma" in which America must choose one or the other—traditional or irregular competition. Both are important and deserve attention. Competition and cooperation are not zero-sum. As LtGen Michael Nagata posited, America is looking for conventional struggles—struggles that we want to have rather than accepting the struggles that we are having right now, or may have in the future.[71] America would do

well to remember that it may compete through both traditional and irregular methods while simultaneously cooperating in other areas. The ability to employ irregular competition as a complement to other things the U.S. government is doing may very well result in unexpected benefits.

Lesson Learned #2: Authoritarian Regimes Seemingly Have More Options

An important debate regarding irregular competition focuses on how authoritarian regimes conduct activities using non-state actors against their democratic adversaries.[72] For example, the Philippine case study suggests that an authoritarian actor such as the CCP can mobilize portions of their populations, enterprises, and infrastructure to support irregular competition in ways that liberal democracies generally cannot. In this case alone, the CCP was able to mobilize fishing fleets, and employ ethnic Filipino-Chinese businesspeople to manipulate political and economic transactions,[73] as well as operate gambling establishments, in order to influence the Philippine population indirectly.

Practical Recommendations Emerging from Lesson Learned #2:

The United States must make a more deliberate effort to understand adversaries. This includes investing in language skills at home to read and analyze competition from adversaries' perspectives, understand how adversaries talk externally and internally about competition, and develop information campaigns to provide both countervailing and alternative messages.[74] Adversaries are vulnerable to campaigns that exploit their weaknesses through the encouragement of democratic reforms, the opening of relatively closed financial markets, and reducing their control over information.[75]

A potential method of interfering with CCP progress might be to disaggregate China's local-level activities, and target specific aspects of those instruments to mitigate their effectiveness.[76] For example, targeting the CCP's military instrument of power through irregular competition would likely not involve engaging military assets directly, but instead would seek new and creative ways to diminish these capabilities. This could include deploying emerging technologies to confuse or interfere with People's Liberation Army Navy (PLAN) maritime reconnaissance aircraft GPS[77] in the

South China Sea, or identifying malign maritime activity observed through persistent unmanned aerial systems.[78]

The CCP case in the Philippines suggests that it may be beneficial for the United States and its partners to seek marginal gains through irregular competition while confronting the CCP. Just as the impact of the CCP's strategy stems from the cumulative effect of carefully coordinated actions, tailored American (or Philippine, or other partners') irregular competition directed toward the CCP could aim to tip the balance in small steps. The most viable approach may be to seek marginal gains targeting "accessible vulnerabilities."[79] Shutting down, or providing alternative messaging to that propagated by, Confucius Institutes are examples of such action.

This approach may have the greatest impact if it can target specific elements central to China's local irregular competition campaigns. The intent would be to "frustrate, undermine, and deny" the individual Chinese instruments being combined to subvert local governance.[80]

In addition, the U.S. and its partners should more deliberately and publicly highlight irresponsible, illegal, or destabilizing adversarial activities. This would admittedly be difficult since such activities are often gradual and uneasily noticed. "That means establishing diplomatic norms as well as naming, shaming, and sanctioning bad actors."[81] After doing so, America and its partners and allies should consider the economic consequences for such malign irregular competition activities.

Lesson Learned #3: Interagency Cooperation is Critical

The benefits of American internal interagency cooperation, as well as Congressional support, are substantial and increase the effectiveness of irregular competition activities. The importance of cooperation between policymakers and those planning and executing irregular competition to achieve common objectives cannot be overstated. This point was made most clearly in the Afghanistan and Iran case studies in which a whole-of-government involvement took place at various times over the years.

Practical Recommendations Emerging From Lesson Learned #3:

Holistic approaches to proactive American irregular competition will require involvement and buy-in from those outside of the traditional security sector, such as

the U.S. Agency for International Development (USAID), the State Department, the Treasury Department, or even the Department of Commerce. "The idea of incorporating non-military activities into the U.S. government's operational definition of national security predates 9/11."[82] The Australian government, for example, determined that its national security strategies and policies were too narrowly drawn toward conventional military threats. This focus did not protect against emerging non-traditional threats.[83] In the United States, a refocus should recognize the role of irregular competition in areas such as economic prosperity, diplomacy, national welfare, climate security, energy, infrastructure, education, industry, and the general nature of American society.[84]

In support of this line of effort, as with any traditional conflict or competition, one should know the intended outcomes before setting off on the endeavor. America has often stepped hastily into conflicts, usually with good intentions, without having a clear idea of what success in them would look like. The importance of determining strategic objectives, and communicating those goals to all involved, is critical to success. Furthermore, those goals must be realistic. Professor Donald Stoker from the Dwight D. Eisenhower School of the National Defense University wrote that American leaders no longer know how to think about conflicts, particularly those fought for limited aims. America often gets involved in conflict without understanding what a "victory" might mean.[85] America's involvement in Afghanistan, its longest war to date, provides an excellent example of what can go wrong when clear, realistic objectives are not stated and understood from the beginning. "Moving the goalposts," or changing the parameters of the game as it is in progress, rarely results in success. Irregular competition is no different from any other type of conflict or competition in this regard. It is critical for America's leadership to clearly understand and articulate intended objectives and outcomes from the start.

Lesson Learned #4: Irregular Competition Coalitions and Alliances Are Necessary

The importance of coalitions or alliances, sometimes with and among unlikely actors, is not unusual in irregular competition. Furthermore, forming a coalition or alliance increases the effectiveness of irregular competition activities. This was evidenced in all three case studies, whether irregular competition was friendly or adversarial in nature. In no case did the state using irregular competition go it alone. As described in the case studies, the United States partnered with Pakistan to manipulate activities and people in Afghanistan against the Soviets, it partnered with Saudi Arabia and Israel to counter Iran, and China partnered with Cambodia to influence the Association of

Southeast Asian Nations (ASEAN). Although they may be fleeting and conditional, foreign alliances and partnerships are common in irregular competition.

Practical Recommendations Emerging From Lesson Learned #4:

The United States must seek expanded international collaboration on responses to adversarial irregular competition and devise proactive friendly irregular competition activities. The United States must include irregular competition in its bilateral and multilateral security dialogues and agreements. Security professionals know well that one state cannot "go it alone" when it comes to achieving most strategic objectives. While partnerships and alliances must be developed, reinforced, and maintained, they must also be updated to account for the evolving technological innovations that shape the contemporary global security operating environment. Just as those relationships must account for space, cyber, social media, and other technological innovations, they must also account for the friendly and adversarial use of irregular competition. Using the current U.S.-Philippine defense pact as an example, the CCP, "has been able to reshape security conditions in the region in ways that actively skirt the Mutual Defense Treaty and undermine the ability of the alliance to respond."[86] This includes using malign irregular competition tactics like deploying maritime militias, and cyber operations that occur below the threshold of traditional military action. Instead of fostering new alliance mechanisms to counter these irregular competition tactics, bilateral discourse has too often centered on military hardware, which "at best paper[s] over the policy and institutional deficiencies."[87] The United States should therefore consider developing an interagency/international network focused on irregular competition and hold scenario discussions with key allies and partners to better understand their concerns, responses, and needs.[88] Furthermore, along the lines of irregular competition coalition building, the United States should consider economic incentives for partners demonstrating proactive irregular competition activities (which much be carefully defined).

Additionally, capacity building for the Philippines and other partners and allies should be one of the highest priorities for America's, "ability to pursue common security and economic goals with like-minded nations is the cornerstone of our success and at the root of our strategy."[89] America's underlying approach in supporting the Philippines, however, need not be aimed at matching competitor capabilities directly.[90] As Assistant Secretary of Defense for Indo-Pacific Security Affairs Ely Ratner has noted, America's strategy will include the development of more combat-capable credibility,

but also building "asymmetric advantages for U.S. partners" and enabling "the most capable of U.S. partners in the region."[91]

Moreover, the United States should prioritize educating partners, allies, its government employees, members of Congress, and other relevant stakeholders on irregular competition. It is only possible to act on friendly or adversarial irregular competition if one understands it. This involves providing "self-help" tools to implement friendly irregular competition, as well as tools to deter and defend against adversarial irregular competition. Understanding the issue is a prerequisite for successful irregular competition efforts.[92]

Lesson Learned #5: Irregular Competition Has Limitations

Irregular competition is not a silver bullet. Across the case studies analyzed, it is reasonable to assume that the actors employing irregular competition were not completely satisfied with the results. Furthermore, irregular competition can have impacts larger, or different, than what anyone may have expected at the outset. In Afghanistan, for example, irregular competition was successful in supporting the ultimate defeat of the Soviet Union, but also likely contributed to a continuation of regional instability, which America would certainly not have chosen. The American use of irregular competition against Iran has at least maintained the status quo in the Middle East, with no major conventional wars with Iran. At the same time, however, there has been no substantial limitation of Iran's ability to negatively influence regional populations or affect governmental legitimacy. In the Philippines, the Chinese use of irregular competition has resulted in marginal political and economic gains for the CCP, such as Manila ultimately choosing not to push the results of the UN tribunal against China. However, it simultaneously caused a several instances of backlash among the Filipino population. Irregular competition thus has limits, but it is nevertheless used by all actors in concert with other instruments of statecraft. Because of this reality, the researcher proposes that it be used or countered with maximum effectiveness, which this study hopes to support.

Practical Recommendations Emerging From Lesson Learned #5:

The United States must acknowledge that there are limitations to what irregular competition can achieve. This applies to both the friendly and adversarial use of

irregular competition. Policymakers, strategists, practitioners, and academics alike must be aware of this. China in the Philippines, for example, has had limited success in its use of coercive gradualism. In some instances, irregular competition has backfired on the CCP, such as with the aggressive nationalist reaction among Filipinos in the face of Chinese encroachment. For America, nearly 70 years of irregular competition directed toward Iran has resulted in limited diplomatic, economic, and strategic military accomplishments. Despite limitations, what is not possible to observe in this research, or anywhere else, is what the outcome would have been in the case of China/Philippines, U.S./Iran, U.S./Afghanistan, or anywhere else, had irregular competition not been implemented. Irregular competition, like any other tool used by state and non-state actors, should be exercised in concert with traditional Diplomacy, Information, Military, and Economic (DIME) instruments and elements of power[93] to achieve desired objectives. While irregular competition is only one among many tools, its effective use should be maximized nevertheless.

Theoretical Implications

Informed by the results above, the author proposes a conceptual model for irregular competition thinking, planning, and policymaking to help offset shortcomings and improve effectiveness in friendly irregular competition. Implementing conceptual change is far less demanding and costly in political, military, monetary, and ethical terms than continuing a traditional, generally military, tactical-operational-level crisis management approach to contemporary global security.[94]

Before discussing the model, however, the author proposes that irregular competition should be understood as one of two components to strategic competition. The other component is traditional competition. Traditional competition is predominantly government-focused activity, while irregular competition is more population-focused. Note that U.S. national security strategy documents do not include this bifurcated construct of irregular competition and traditional competition. This construct is a contribution of this study. Since this work emphasizes irregular competition, not traditional competition, little is discussed here about the latter.

Figure 1 graphically represents the idea of traditional competition and irregular competition as components of strategic competition, specifically focusing on the irregular competition side of the graphic. It is important to keep in mind that Figure 1 cannot adequately capture the overlap between irregular and traditional competition.

Additionally, collaboration and cooperation across the government, and among partners and allies, cannot be overstated. The lines between irregular and traditional competition are therefore not clear, but instead blurred and cross-cutting; activities can and should occur on both sides of the paradigm in concert, at the same time, and are not mutually exclusive.

Figure 1. Conceptualizing Irregular Competition as a Component of Strategic Competition

As depicted in Figure 1, the DIME instruments of power in irregular competition manifest differently than in traditional competition. For example, the diplomatic instrument of power is manifested in irregular competition as political warfare. In his book *On Political War*—which remains a seminal work on the subject—Paul Smith describes political warfare as the use of "political means to compel an opponent to do one's will, based on hostile intent."[95] It is a calculated interaction between an actor and a target audience, including a competitor's government, military, and general population, which uses various techniques to coerce certain actions, thereby gaining a relative advantage over an opponent.[96] Furthermore, political warfare's coercive nature leads to the weakening or destroying of an opponent's political or social will and forces a course of action favorable to an actor's interest. For the purposes of this work, however, George Kennan's definition of political warfare below will be used. Kennan,

an American diplomat and key figure in the development of U.S. Cold War policy, often referred to as the "father of containment," introduced and defined "political warfare" in 1948 as he provided guidance to a newly founded CIA:

> Political warfare is the logical application of Clausewitz's doctrine in time of peace. In the broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures, and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare, and even encouragement of underground resistance in hostile states.[97]

The informational instrument of power is manifested in irregular competition as propaganda and psychological operations. In *On Political War*, propaganda is driven by national objectives, has many aspects, and involves some degree of hostile and coercive political purpose. Psychological operations, on the other hand, are driven by strategic and tactical military objectives, and may be intended for both hostile military and civilian populations. Whether propaganda or psychological operations are discharged, the primary vehicle is the use of "words, images, and ideas," which, when combined, may enable information and disinformation campaigns to alter a target audience's opinions.[98] It involves heartening friends and disheartening enemies, and gaining help for one's cause while inducing the abandonment of the enemies'.[99] Propaganda and psychological operations involve both information and disinformation, and are likely cyber-enabled today.

The military instrument of power is manifested in irregular competition as irregular warfare (IW), where the security sector of both state and non-state actors attempts to influence populations and affect legitimacy. The U.S. Department of Defense's (DoD) 2020 *Summary of the Irregular Warfare Annex*[100] makes clear that IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities. According to the U.S. military, IW includes five primary activities: unconventional warfare (enabling resistance movements), foreign internal defense (supporting another country's security programs), counter-terrorism, stability operations, and counterinsurgency. Beyond what is formally written into military doctrine, IW might also encompass such things as support to political warfare (defined earlier), counter-unconventional warfare (countering an adversary's will and capability

to defens against a resistance movement), proxy warfare, military information support operations (also known as psychological operations), cyberspace operations, countering threat networks, countering threat finance, civil-military operations, and security cooperation. As evidenced above, the military's IW construct is quite expansive. It is worth noting that the DoD is currently reevaluating its definitions and understanding of IW as the current construct is considered by many to be confusing and inadequate.

The economic instrument of power is manifested in irregular competition as pressure, persuasion, coercion, and subversion. Once again, adapting Paul Smith's[101] writing to the subject of irregular competition, activities undertaken in the economic space are intended to inflict necessary economic damage to force political change. Conduct here will differ according to whether the actor is authoritative or democratic since standards, laws, norms, and the ability to mobilize an actor's resources differ. Economic activities in irregular competition support furthering political goals without direct confrontation. With the interconnectedness of global economies, economic activity executed as part of any irregular competition strategy must be calculated and integrated with all other instruments of power to achieve political objectives but not provoke direct conflict.

A closing note on the conceptual model is necessary at this point. The reader is reminded that this model was derived inductively from empirical research. The author worked back and forth between data collected and themes emerging from the data in the case studies until a comprehensive theoretical structure was established.[102] This essentially meant working the data "from the ground up," noticing patterns that emerged, and eventually finding that some part of the data suggested a useful concept.[103] This useful concept is the theoretical model presented in Figure 1.

Additional Considerations

Three additional considerations should be included in any discussion of irregular competition strategy. First, the question of who in the U.S. government should lead irregular competition efforts or ultimately be responsible for their success or failure must be addressed. There currently exists no single government office or institution responsible for such efforts. The DoD spends an increasing amount of time and effort on irregular warfare, but IW is only the *military's* contribution to a larger irregular competition effort. Considering whole-of-government requirements, the National Security Council (NSC) could take the lead rather than DoD. A 2019 Center for

Strategic and International Studies (CSIS) report suggested that NSC leadership could be put in motion by issuing an irregular competition Presidential Decision Directive (PDD). The PDD would outline dynamic campaign approaches, identify supporting executive branch elements, and designate an NSC senior director.[104] According to the CSIS study, this director, along with a supporting intelligence-operations task force and senior interagency coordination mechanisms, would be responsible for coordinating and perhaps leading irregular competition efforts. However, this proposal may not be the best solution. In short, once the NSC is in charge, other government agencies and offices that have nothing to do with national security, such as NGOs or academic institutions, but have important roles in a whole-of-government approach to irregular competition, may be put off by the idea of being directed by, or associated with, the U.S. government's security apparatus. Furthermore, one might look to the history of NSC-68,[105] an initiative that pioneered whole-of-government irregular competition-like efforts following the Second World War, to look for appropriate lessons. Drafting authority alone for NSC-68 was taken away from the NSC primarily because of infighting within the military bureaucracy and shifted to the State Department, which had "the clearest understanding of the sweeping and radical character of the work which they were undertaking."[106] The DoD was hampered by divisions of authority between the Secretary of Defense and the Joint Chiefs of Staff, in addition to conflict regarding the military's budget.[107] With this in mind, along with an acknowledgment of the current organization of the U.S. government, it is worth asking whether significant reorganization, or even an entirely new office, would be required to implement an effective irregular competition approach.

A second area requiring further analysis involves relevant metrics. It is difficult to quantitatively measure success or failure in the largely qualitative world of irregular competition. As discussed earlier, it is important to set clear objectives before initiating any irregular competition campaign. Indeed, this is true for any national security initiative. This is a critical component of irregular competition because, without metrics for success, the actor implementing it cannot objectively calculate whether they have succeeded, failed, or are making progress. Measurement tools are critical to providing decision-makers with quantitative and qualitative assessments and recommendations. A study conducted by Larson, Eaton, Nichiporuk, and Szayna[108] proposed that any analysis of irregular environments should start with a generic and broad understanding of the conflict and then engage in successively more-focused and more-detailed analyses of selective topics. The point is to develop an understanding and then uncover key drivers behind such phenomena as an orientation toward principal protagonists in the

conflict, mobilization, recruitment, and choice of political bargaining or violence. Such a framework may illuminate areas where additional detailed analysis could matter and areas where it probably would not matter. Following that, a more intensive analysis of each stakeholder in the irregular competition scenario is recommended. The third step, dynamic analysis, aims to make sense of the data and insights collected in the previous steps. Such a tool may be useful in augmenting, but not replacing, traditional analytic methods to accent irregular features at the strategic and operational levels that are important determinants of irregular competition outcomes.[109] Measurement frameworks such as these would also facilitate continuous evaluation of any proposed irregular competition campaign. Important to remember is that more than one set of metrics may be required for different irregular competition environments. While a general set of metrics would be helpful, more nuanced metrics for each geopolitical situation may be necessary. Without such metrics, one might get involved in a protracted irregular competition struggle blind to its overall progress. In summary, the importance of metrics in irregular competition cannot be understated.

A third area of consideration involves education. How should America educate and inform its citizens, as well as foreign partners and allies, of the importance and intricacies of irregular competition? As authors Stringer and Urban state, a historic misalignment of efforts has led to irregular competition campaigning failure.[110] This is partly due to an overreliance on military power, which can rarely address the underlying political, cultural, and economic drivers of conflict. In a context where each of these pillars provide critical resources to advancing an irregular competition campaign, each relevant stakeholder should have access to irregular competition education.[111] Education efforts domestically and abroad on this topic will likely involve different approaches. Similarly, educating government employees and educating civilians, for example, may require different methodologies. Before America and its partners can embrace irregular competition, there is a logical prerequisite for education to understand what it is and why it is important.

Conclusion

> *Conflict now involves entire populations, as well as large number of indigenous national civilian agencies, other national civilian organizations, international organizations, nongovernmental organizations, private*

> *voluntary organizations, and subnational indigenous actors involved in dealing politically, economically, socially, morally, criminally, and/or militarily with ambiguous and complex threats to national and global security and well-being... At the same time, an almost unheard-of unity of effort is required to coordinate the multilateral, multidimensional, and multi-organizational paradigm necessary for success on either or all sides of a contemporary conflict.*[112]
>
> *-Max Manwaring*

Few people agree on the finer points surrounding irregular competition, and this single work cannot rectify that. Irregular competition is a sensitive subject, but the United States, its partners, and its adversaries are all involved in one way or another. To paraphrase a quote from Trotsky, "you may not be interested in irregular competition, but irregular competition is interested in you."[113] This is a people-centric struggle, in which cognitive awareness and emotional intelligence are often more important than military might. Any irregular competition strategy must be flexible enough to transform with technological innovations. Adversaries are plugged in and hyper-networked. This expanding physical and virtual operating space makes working by, with, and through like-minded partners more important than ever since the threat space is exponentially larger than any one actor can manage. As American Gen Richard Clarke noted, we must look to the multinational community, "leverage exporters of security, and pull them in with shared interests."[114]

At any given time, irregular competition – or whatever term one uses to describe this space – is high or low on the priority list for U.S. national security leaders, policymakers, and practitioners. Strategic competition with China is the main priority at the moment, but irregular competition should be understood as a component of this larger contest. It is not something that happens or doesn't happen in place of strategic competition. After all, influencing populations and affecting legitimacy, the goals of irregular competition, remain important no matter what the larger objectives are. The United States spends millions of dollars annually on activities related to irregular competition. One can imagine the spending that goes into the State Department's Global Engagement Center (GEC) activities, the Defense Department's irregular warfare initiatives, the

Department of Energy's counterterrorism and counterproliferation endeavors, and the Treasury Department's counter-threat-financing programs, to name but a few organizations engaged on some aspect of irregular competition. These programs, and many more across the U.S. government, play a role in influencing populations and affecting legitimacy. This occurs despite whatever temporary state of peace, competition, or conflict is playing out in any given space and time. Regardless of where irregular competition sits on any individual leader, organization, agency, or administration's list of priorities, it cannot be denied that irregular competition is taking place. America's irregular competition strategy should therefore be as effective and efficient as possible.

About the Author

Dr. "Lumpy" Lumbaca is a Professor of Counter-Terrorism, Irregular Competition, and Special Operations at the Department of Defense's Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI APCSS) in Honolulu, Hawaii. He is a retired U.S. Army Special Forces officer and can be followed on X @LumpyAsia.

Discussion Questions:

1. What are the implications for the use of irregular competition as the potential for traditional, state-on-state conflict intensifies?
2. Why does America continue to force a distinction between employing traditional or irregular competition, rather than a balance of both?
3. Is the United States capable of reorganizing itself for whole-of-government irregular competition activities?
4. Will the United States be able to shift from simply reacting to adversarial irregular competition, to employing its own proactive irregular competition activities instead?

Recommended Reading:

- Fridman, O. (2018). *Russian Hybrid Warfare: Resurgence and Politicisation.* London: C. Hurst & Co. Publishers Ltd.
- Kilcullen, D. (2020). *The Dragons and the Snakes*. New York, NY: Oxford University Press.
- Manwaring, M. G. (2010). *Gangs, pseudo-militaries, and other modern mercenaries: New dynamics in uncomfortable wars*. Pp. 164. University of Oklahoma Press.
- Smith, P. A. (1989). *On Political War.* Washington, DC: National Defense University Press.

Towards a Better Irregular Warfare Strategy: A Contrarian View

Thomas Searle

ABSTRACT

Many academics and pundits are in a state of near panic over the imagined incompetence of the United States in irregular warfare (IW) and the IW brilliance attributed to competitors such as Russia, Iran, terrorists, and the People's Republic of China. The hysteria is entirely overblown since the United States has long enjoyed remarkable success in IW while its adversaries have stumbled and struggled to keep up. However, past performance does not guarantee future success and the United States needs to continuously improve its IW performance to stay ahead of its competitors.

This chapter recommends three approaches to build and sustain more successful IW campaigns. First, IW campaigns should focus on U.S. values since IW campaigns are typically long and very hard to sustain through frequent personnel turnover unless they are broadly supportive of one or more values widely held by American officials and citizens. Second, IW campaigns must start from a clear-eyed understanding of how our foreign partners differ from the United States and the chapter suggests a few characteristics common to many foreign partners. Third, the United States should avoid overbearing, hierarchical command and control structures in favor of looser, collaborative approaches based on the reverse-poker concept.

Introduction

Let's start with some myth busting. In recent years there has been a vast outpouring of complaints about the poor U.S. performance in what might be called irregular warfare (IW). Inspired, perhaps, by frustration over the challenges the United States faced in Iraq, particularly from 2006-2008 and in 2014, accusatory academics claim the country has lost every war it has fought since World War II due to its incompetence in IW. According to these critics, the United States possesses overwhelming conventional military power and yet continuously loses in war, conflict, and competition because it always fails in everything except large-scale conventional combat operations, i.e., in IW. Even in conflicts involving large-scale conventional combat operations, such as the 2003 invasion of Iraq, it inevitably transforms into irregular conflict, and the United States inevitably loses. Sean McFate is perhaps the most visible advocate for this view through his popular book *The New Rules of War*,[115] but Harlan K. Ullman's *Anatomy of Failure*[116] makes many of the same claims, and even careful scholars like Thomas A. Marks and David H. Ucko get caught up in the hysteria in their otherwise excellent *Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action*[117], where they find some imagined "crisis" in U.S. irregular warfare.

This failure narrative has been accompanied by a parallel narrative of IW success by America's enemies, particularly Russia, the People's Republic of China (PRC), Iran, and international terrorist organizations. A prominent example of this school of thought would be Seth G. Jones in his popular book *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare.*[118] According to the enemy success narrative, Russia's "hybrid warfare"[119] using the Gerasimov (or Primakov) Doctrine[120] and "little green men"[121] has been highly successful in accomplishing Vladimir Putin's goals while avoiding large-scale conventional combat, i.e., by engaging in IW. The PRC's Belt and Road Initiative[122] and its island building campaign in the South China Sea[123] are likewise presented as enormous wins in its competition with the United States in the IW space below the threshold of armed conflict. This enemy success narrative also claims that Iran has taken control of Lebanon, Syria, Iraq, and Yemen through the brilliance of the Iraqi Revolutionary Guard Quds Force[124] and without resorting to any conventional combat operations, proving both the effectiveness of Iranian IW and the failure of U.S. IW. Furthermore, the enemy success narrative claims the Global War on Terrorism catastrophically failed by increasing, rather than decreasing, the terrorist threat and expanding the power and reach of Al Qaeda while also creating and growing Daesh (also known as the Islamic State in Iraq and Syria or ISIS)[125], and all the while consuming

enormous resources and distracting the United States from the more serious threats posed by Russia and the PRC.[126]

Nevertheless, while the narrative of universal U.S. failure in irregular warfare efforts could not be further from the truth, the parallel narrative of enemy triumph is similarly off the mark.

The Long History of U.S. Success and Enemy Failure in IW

Those who claim the United States has consistently failed in IW since World War II forget that the country won the Cold War without defeating Soviet nuclear or conventional forces. In fact, the Soviets successfully deterred a U.S. nuclear attack, and also successfully deterred a conventional invasion, but still could not prevent the destruction of the USSR through unfriendly methods below the threshold of direct armed conflict, i.e., through IW. The multiple rounds of NATO enlargement since the collapse of the Soviet Union constitute another, spectacular IW success. There were 16 NATO countries in 1990. Since then 16 more countries have joined NATO.[127] Some readers will question whether NATO enlargement constitutes IW success by the U.S. and its allies, but Vladimir Putin certainly views it as aggression below the level of armed conflict, i.e., as IW[128], and we would regard a comparable expansion of Russian, Chinese, or Iranian military alliances as IW successes by those nations, so we must accept NATO expansion as an IW success.

The defeat of the Soviet Union and NATO enlargement are part of a larger pattern of U.S success in IW. For other examples we can look to the so called Color Revolutions that toppled the governments of Yugoslavia (2000), Georgia (2003), Ukraine (2004), Kyrgyzstan (2005), Moldova (2009), Armenia (2018), and Bolivia (2019), drove Syrian forces out of Lebanon (2005), and caused major civil disturbances that threatened to bring down many other regimes.[129] While the U.S. government does not take credit for the Color Revolutions, Russia, the PRC, and many other foes of the United States blame the country for them.[130] It is certainly the case that individuals and organizations funded by the U.S. government assisted some Color Revolutions[131], that Color Revolutions were based on democratic principles long advocated by the U.S. government, and that the United States did nothing to prevent or defeat these Color Revolutions. All of this makes it fair to consider the Color Revolutions as examples of U.S. IW success. The same could be said for the Arab Spring revolutions of 2011 that brought down the governments of Egypt, Libya, Tunisia, and Yemen, and forced governmental reforms in Bahrain, Jordan, Kuwait, Lebanon, Morocco, and Oman,[132] since these followed the Color Revolution

model of civilian-led pro-democracy protests encouraged, but not entirely directed, by the U.S. government.

In addition to population-centric IW successes like the collapse of the USSR, the enlargement of NATO, and Color Revolutions that brought down repressive governments, the United States has also enjoyed significant success in IW efforts that are not population-centric. These include strategic sabotage efforts such as the Stuxnet cyber weapon that sabotaged the Iranian nuclear program.[133] While Stuxnet is the most famous of these strategic sabotage efforts, it is hard to imagine that it was wholly unique. Instead, we must assume that Stuxnet was the visible tip of a much larger iceberg of clandestine and covert activities, both cyber and non-cyber, that the United States is executing against its adversaries. Since the effectiveness of these covert and clandestine IW efforts are hard to evaluate in an unclassified setting, we will not discuss them further in this essay, but they should still be kept in mind.

Additional examples of non-population centric U.S. success in IW would be the financial coercion described in Juan Carlos Zarate's terrific book, *Treasury's War: The Unleashing of a New Era of Financial Warfare*,[134] the extraordinary economic sanctions imposed on Iran[135] and on Russia, since Putin's full-scale invasion in early 2022,[136] and the targeted killing of Iranian Quds Force commander Qasem Soleimani, which significantly degraded Iranian IW efforts in the Middle East.[137]

In assessing U.S. competence in IW, it is also worthwhile to ask how American competence is viewed by foes, particularly Russia and the PRC. In the Russian case, the so-called Gerasimov Doctrine (named after General Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces) is not a plan to defeat the United States without resorting to armed conflict. Instead, it is General Gerasimov's attempt to explain modern war, as conducted by the United States, and why American methods (i.e., IW) have been so successful, in the hope that Russia can learn to imitate and counter what the United States has accomplished so effectively.[138]

As for the PRC, Xi Jinping is terrified of becoming the victim of a U.S.-sponsored Color Revolution, as the USSR was, and for years he has regularly complained to American officials, foreign leaders, his followers in the Chinese Communis Party (CCP), and anyone else who would listen about the global threat posed by such Revolutions.[139] More recently, the PRC has criticized U.S. actions as "salami slicing" (i.e., IW) tactics and insisted that these tactics will not work.[140] Of course, these complaints announce the PRC's fear that U.S. IW might work, and the difficulty in finding a countermeasure to "salami slicing" that is more effective than public complaints.

In addition to these historic IW successes by the U.S. government, and the fear they incite in the leaders of Russia and the PRC, current IW campaigns against leading foes are going remarkably well. Let's consider the status of U.S. IW against Iran, Russia, the PRC, and terrorism, respectively.

In early 2023, Iran was wracked by long-running protests that the Iranian regime blames on the United States.[141] Certainly, the U.S. government welcomed and encouraged these Iranian protesters even if it did not provide any overt direction, or material support, to them. The protests put severe strain on the government of the Islamic Republic of Iran[142] and the costs of suppressing the protests were vastly more than what it cost the United States to encourage them. The protests also isolated the country, as European nations sanctioned elements within the Iranian government for its heavy-handed crackdown, and Tehran retaliated by sanctioning European politicians and entities.[143] As such, the anti-government protests in Iran must be considered an IW success for the United States, even if they failed to force the removal, or even the substantial reform, of the current government.

Similarly, U.S. and NATO support to Ukraine in its ongoing war against Russia can be considered irregular warfare. For their part, the Russians insist they are in a war against the United States in Ukraine and the country and its armed forces are merely the surrogates, proxies, or pawns of Washington.[144] As such, the continuing success of the Ukrainian armed forces and the spectacular failure of the Russian armed forces must be considered an enormous strategic IW success for the United States. The fighting in Ukraine has dramatically weakened Russia across all elements of national power. Diplomatically, Russia is isolated as never before in its history, with the UN voting 143 to 5 to condemn the Kremlin's attempt to annex parts of Ukraine.[145] Militarily, Russia has lost hundreds of combat aircraft, thousands of tanks and other fighting vehicles,[146] and hundreds of thousands of troops, while its reputation for combat effectiveness has been shattered.[147] Economically, sanctions, the direct costs of the war, and other financial disruptions resulting from the war will cost about $100 Billion (6% of its annual GDP) in the first year of the conflict compared to what the economy would have been if Russia had not invaded Ukraine.[148] A further $330 Billion in Russian assets have been frozen in response to the invasion and may never be returned.[149] On the whole, then, Russia's ongoing catastrophe in Ukraine is already a spectacular IW success for the United States and the level of success increases every day as Moscow's squanders vast resources for minimal gains.

Whatever IW campaigns the United States is currently waging against the PRC are producing much less visible and dramatic results than the protests in Iran or the war in Ukraine. However, the last few years have seen some good news on the PRC front as well. For example, the counter-PRC groupings known as The Quad[150]—consisting of Australia, India, the UK, and the USA—and AUKUS—consisting of Australia, the UK, and the USA[151]—have been energized by the threat from the PRC. Likewise, the states bordering the South China Sea—Vietnam, Malaysia, Indonesia, and the Philippines—have hardened their attitudes against the PRC in response to predatory PRC behavior in the region.[152] Europe is also taking a tougher line with the PRC[153] and its Belt and Road Initiative has lost much of its luster in many places and is thus producing lower than expected returns.[154] Furthermore, while recently imposed U.S. economic sanctions on the PRC are nothing compared to those in place on Iran (for years) and on Russia (since Feb. 2022), they do target key technologies and are specifically designed to counter threats to American security.[155]

U.S. success against transnational terrorists has been, perhaps, even more impressive than its other IW successes (for details, see the chapter on Counter Terrorism in this volume). After the spectacular terrorist success on 11 September 2001 (9/11) the United States has successfully prevented anything remotely comparable. The United States has also demonstrated the ability to destroy terrorist sanctuaries at will in Afghanistan in 2001, in Iraq from 2007-2008, and in the ISIS Physical Caliphate from 2014-2017. In each case the United States killed tens-of-thousands of enemy fighters and sent the scattered remnants fleeing to wherever they could hide. Terrorism, like the poor, will always be with us, but whether the goal of U.S. IW against transnational terrorist organizations was to protect the homeland from attack or to punish enemies, that goal has been, to a very large degree, achieved.

Having disposed of the myth of consistent IW failure by the United States let's turn, briefly, to the equally untenable myth of routine enemy success. Other chapters in this volume cover the IW efforts of Iran, Russia, the PRC, and terrorist organizations in detail, but a brief review will demonstrate that their performance has not been overly impressive. Iranians like to brag that they run four Arab countries—Syria, Yemen, Iraq, and Lebanon—but the picture is less rosy for them than they it might appear.[156] Iranian (and Russian) assistance has certainly kept the Assad regime in power in Damascus, but the ongoing civil war has left Syria a shattered nation with a per capita GDP that ranks 198th in the

world, according to the 2023 CIA World Fact Book,[157] indicating that the country will be a drain on Tehran's resources, rather than an asset, for the foreseeable future. Yemen, ranking 202nd in per capita GDP, is in even worse shape than Syria, though it consumes vastly fewer Iranian resources.[158] Iran's influence in Iraq[159] and Lebanon[160] is challenged by popular protests in both countries.[161] It is hard to escape the conclusion that Iran's IW efforts have brought it little benefit at high cost, and that the grim future of the regime will not be markedly improved by some future IW success against the United States.[162] On 7 October 2023, Hamas, an Iranian proxy, launched a spectacular terrorist attack on Israel. The attack and ensuing war have been an enormous tragedy for Israel, and the Palestinians, but not a success for Iran since Hamas has been bitterly disappointed by the support it received from Iran and other Iranian proxies, demonstrating the weakness of Iran's so called "axis of resistance."[163]

Russia's catastrophic failure in IW is plain for all to see. While outsiders were lauding Putin's supposed brilliance in IW,[164] he recognized that in Ukraine—the most important target of his efforts—his campaign failed. As Putin acknowledges, he launched his full-scale invasion of Ukraine in 2022 because his IW campaign was doomed and he was left with "no other choice" than a major conventional war to avoid complete strategic failure in Ukraine.[165] Fortunately for the United States, by replacing an inexpensive failed IW campaign with a disastrously expensive failed conventional warfare campaign, Putin has put his entire regime in jeopardy.[166]

The PRC's IW efforts are making zero progress in resolving the Taiwan issue in Beijing's favor and seem to be having the opposite effect as the local population becomes increasingly hostile to the Chinese Communist Party.[167] As for international terrorists, twenty years of unprecedented efforts and the deaths of tens of thousands of Al Qaeda and Daesh fighters has produced only one noteworthy achievement, the return of the Taliban to Kabul, and even that merely restored the status quo from 2001.

As demonstrated by this brief assessment of the facts, any narrative claiming routine IW brilliance and success by the enemies of the United States is pure mythology.

Exploding the myths of U.S. incompetence, and enemy brilliance, in IW does not mean that every effort undertaken by the United States has been a success, nor that its enemies always fail. On the contrary, IW efforts by the United States often result in failure. For example, the IW effort against the Castro regime that led to the landing of Cuban exiles at the Bay of Pigs in 1961 was an embarrassing failure.[168] By the same token, the fall of Saigon to Vietnamese communist forces in 1975, and the reconquest of Kabul by the Taliban in 2021, must be considered IW failures for the United States. More

troublingly, to date, Russia has successfully prevented a Color Revolution in Venezuela, suggesting that the enemies of U.S. policy might be getting better at countering its IW techniques.[169] However, the impressive list of U.S. successes in IW certainly shatters the myth that the United States consistently fails in its IW campaigns and the equally impressive list of enemy failures in IW shatters the myth that its enemies are IW geniuses who need to be copied wholesale.

Building a New Strategic Approach to IW

Can we build a new strategic approach to IW that is not based on a dishonest assessment of the past and the present? If we are not failing catastrophically, and if our enemies are not succeeding spectacularly, can we find the motivation to improve our performance or are we doomed to lapse into complacency until our enemies eventually get their act together and defeat us? In short, are the members of the Chicken Little "sky is falling" caucus wrong about the facts, but right about the need to misrepresent the facts in order to generate needed change? We shall see.

The proposals that follow are an attempt to build a new strategic approach to IW based on the historical record rather than on panic and hyperbole. These recommendations are based on three principles: focusing on our values to pursue consistent goals, understanding our partners to get the best out of them and avoid disappointment, the reverse poker technique for international and interagency cooperation.

Consistent Goals Based on Enduring U.S. Values

IW success typically requires consistent support over the long term. Gerasimov may wonder that "a perfectly thriving state can, in a matter of months and even days" be overthrown by a Color Revolution.[170] But we all know the "perfectly thriving" states that fell to Color Revolutions were failing their populations in the usual ways (denial of human rights, denial of political representation, denial of economic opportunities, etc.) and that years of painstaking efforts to promote democracy, support civil society, advocate for human rights, etc. helped build the pre-revolutionary conditions in those countries.

The great disadvantage of the United States in a long-term activity like IW is that the U.S. system is highly decentralized. At the federal level, power is divided between the executive and legislative branches, and the overwhelming majority of U.S. information power and economic power is in private hands and not under direct government

control, thus making it extraordinarily challenging to develop a fully integrated whole-of-society approach with the institutional raw material available. This synchronization challenge is compounded by frequent turnover of government personnel, along with frequent elections, bringing frequent changes in policy. However, American values, such as democracy promotion, are widely held by U.S. citizens in and out of government and across both parties. As a result, an IW campaign closely tied to American values is relatively easy to sustain since U.S. officials and private citizens are inclined to support such campaigns naturally, even without central direction to do so. Fortunately, such American values *are* broadly popular, giving the United States an enormous soft power advantage over its adversaries. After all, the Shiite fundamentalism underpinning the Islamic Republic of Iran has little appeal to non-Shiites; the extreme Russian nationalism underpinning Putin's regime has little appeal to non-Russians; and the Chinese nationalism underpinning Xi's PRC has little appeal to non-Chinese. Since U.S. values are often critical to its IW success, let's take a brief look at some key ones and how they differ from those adversaries have to offer.

The extraordinary success of the Color Revolutions and NATO enlargement have left U.S. enemies bewildered. Vladimir Putin had a ring-side seat for three decades of NATO enlargement, but he still cannot comprehend it. In Putin's mind, NATO enlargement is driven by an expansionist United States imposing its will on eastern Europe. At the Munich Security Conference back in 2007, he insisted that NATO enlargement "is not connected in any way with the democratic choices of individual states" and is instead more proof that the United States "overstepped its national borders in every way."[171] Contrary to his claim, NATO enlargement is entirely driven by the democratic choices of the states who join, and is in no way the result of coercive pressure from the United States. For example, democratic Finland and Sweden preferred to remain outside NATO until Putin's invasion of Ukraine demonstrated that the Russian threat was great enough that it required an immediate change to the highly successful and generations-long "nonalignment" policies of both countries.[172]

To Putin, a state choosing to join NATO means choosing to surrender independence and accept U.S. domination.[173] However, the nations that have joined NATO, their true goals were clearly listed by Lord Ismay, the first Secretary General of NATO, more than 70 years ago: "to keep the Soviet Union [Russia] out" of their countries, and "the Americans in" their countries.[174] The questions Putin should be asking are: why do so many of Russia's neighbors want the Russians out of their countries? And, why do so many of those same countries feel the opposite way about Americans? The short answer is "soft power," the ability to attract or repel other countries without the use of force.[175]

The United States possesses positive soft power through American values such as democracy (from the Greek *demos* meaning "people" and *kracia* meaning "power") and its close cousin, self-determination. Putin and Xi Jinping were brought up in the Leninist tradition that true democracy (or "people power") is impossible to realize because the people do not understand their best interests and are always being led (i.e., manipulated) by someone. Lenin used this view to justify an elite vanguard party to force the people to act in their best interests, since the people will neither recognize nor pursue their best interests without this guidance.[176] Xi Jinping, and the Chinese Communist Party (CCP) he leads, still embrace this Leninist tradition. Putin, without the advantages of an elite party apparatus, sees himself as a unique genius capable of leading the Russians to their best interests[177] and believes all other nations are being led by some elite and not following the true will of their people.

Putin and Xi also reject the notion of self-determination, i.e., the idea that a group of people should be able to make political choices for themselves. Instead, the smaller and weaker must bow to the superior power of larger and stronger. As Thucydides said more than 2,400 years ago "the strong do what they can and the weak suffer what they must."[178] When Putin denies the independence of Ukraine and says there are only a few truly sovereign nations in the world (he has identified Russia, China, and India as among these) he is rephrasing Thucydides and stating his preference as a fact.[179] By the same token, when PRC Foreign Minister Yang Jiechi lost patience at the 2010 ASEAN (Association of South East Asian Nations) Conference and said, "China is a big country and you are small countries, and that is a fact,"[180] he was rejecting self-determination for all in favor of the PRC as a regional hegemon dominating its smaller neighbors.

The Islamic Republic of Iran is similarly focused on regional hegemony rather than self-determination. It might prefer to control foreign states through the democratic support of local populations, but instead it must rely on armed proxies (Hezbollah[181] in Lebanon, the Houthis[182] in Yemen, Shiite militias in Iraq[183], and both the unpopular Assad regime and Shiite militias[184] in Syria).

Unsurprisingly, U.S. values of democracy, self-determination, and independence, even for small nations, are much more widely popular than Iran's, Putin's, and Xi's belief in autocratic leadership and regional hegemony by large nations. As a result, the United States enjoys positive soft power and continually attracts novel partners such as Finland and Sweden, even without bribes or threats, whereas Iran, Russia, and the PRC tend to repel both potential and current partners. Instead, Iran, Russia, and the PRC must rely on bribes and threats and even these often fail as demonstrated in the inability

of these countries to achieve their goals in Iraq (the removal of U.S. forces), Ukraine (the permanent rejection of NATO and EU membership), and Taiwan (reunification with the PRC) despite the coercive pressure they have employed.

American values are not just critical to winning over potential partners, but also a direct threat to the enemies of the United States. The CCP even published a handy list of the values they fear the most, and hence provide a guide to some of the values the United States should promote most actively through IW. In April 2013, the CCP published "Document No. 9," titled "Communiqué on the Current State of the Ideological Sphere."[185] Document No 9 listed seven dangerous values that are banned from the PRC because of the threat they pose: (1) western constitutional democracy; (2) the notion of human rights and other "universal values" all people deserve; (3) civil society not controlled by the government; (4) market economies independent of government control; (5) freedom of the press; (6) honest assessment of the CCP's past mistakes; and (7) questioning whether the PRC is in fact a socialist country. These are excellent suggestions for what the United States should be promoting inside and outside the PRC in its IW campaign. After adjusting the last two items to read "honest assessment of Russia's past mistakes" and "questioning whether a Putin-led Russia will ever be a great nation" they also provide a good guide to IW campaigning against Moscow. Adjusting the last two values to read "honest assessment of the Islamic Republic of Iran's mistakes" and "questioning whether the Islamic Republic is in fact Islamic" equally makes them a good guide for IW campaigning against Tehran.

Understanding Our Partners

Sun Tzu famously said that to succeed in battle, i.e., in conventional warfare, you must understand yourself and understand the enemy, but in IW it is also vital to understand partners and neutrals, because they are routinely key to long-term success. By the same token, if the United States does not understand its partners, it will routinely miss opportunities and make unrealistic demands on partners leading to disappointment and failure. For example, the United States counts on NATO to help counter the threat from Russia. Poland and Portugal are both members of NATO, but there are historic and geographic reasons why Warsaw feels the threat from Russia more acutely than Lisbon does. In fact, from a U.S. point of view, Poland is likely to overstate the Russian threat, whereas Portugal is likely to understate it. Thus, friction between the United States and Poland over Russia is likely to center around Polish complaints that Washington is doing too little and doing it too slowly, whereas friction between the United States and

Portugal over Russia is likely to center around Portuguese complaints that Washington is asking it to do too much, too fast.

The lesson is that the United States must listen carefully to the unique point of view of each partner and neutral and take these perspectives into account in developing and sustaining long-term IW campaigns. When we consider state, sub-state, and transnational actors, the number of potentially important partners and neutrals becomes enormous, and much too large to consider in detail in this chapter. Certain patterns, however, are common enough that they need to be identified and addressed here. Specifically, we will note five recuring features of U.S. relations with partners: (1) partners are unlikely to be "more Catholic than the Pope;" (2) partners are needy; (3) partners are imperfect; (4) the United States is rich and powerful; and (5) the United States is far away.

Partners are Unlikely to be "more Catholic than the Pope:"

If the United States is committed to opposing Russia, the PRC, Iran, or someone else, then its partners will usually oppose them as well, but are likely to take a slightly softer line. There is little for them to gain by taking a harder line than the United States on American-led policy, and they would incur significant risk by taking a harder line since the target will naturally focus its retaliation on those taking the hardest line. On the other hand, there is much to be gained by taking a somewhat softer line since it shows independence from the United States and the target may even provide valuable rewards to those taking a softer line, such as when Saddam's regime in Iraq bribed French companies to help evade economic sanctions.[186] When U.S. officials understand this dynamic they will expect consistent complaints from partners that Washington is too antagonistic, and assertions that the partner's softer approach is superior. Sometimes the partners sincerely believe they have a better approach, but usually they are merely taking the U.S. line and softening it a little, for reasons unrelated to the specifics of the policy.

Partners are Needy:

If a group or nation can achieve all its goals without U.S. assistance, then it does not need to partner closely and it probably will not do so. On the other hand, if a group or nation is in desperate need of assistance, then it is much more likely to partner closely with the United States. This basic point should be obvious, but anyone who has worked with U.S. partners has heard American officials complain that their phones are blowing up with endless requests for assistance from the neediest partners, and they never get calls from the partners who are doing well, as if this were surprising and not an inherent feature of international relations.

Partner neediness is particularly apparent when the danger to the partner is acute, and the danger to the United States is less apparent. For example, Ukraine has faced an extreme threat from Russia since 2014, but the United States has felt that threat much less acutely and has thus consistently provided less support to the government of Ukraine than they would like.[187] This gap in threat assessment is often mirrored by a gap in the level of sacrifice by the United States and its partners as evidenced by quips like the claim that Washington will "fight Russia to the last Ukrainian."[188] This gap in threat assessment and sacrifice often becomes unreasonably acrimonious on both sides. For example, Afghans complained of "abandonment" by the United States in 2021, rather than thanking the country for the 20 years of support between 2001 and 2021. At the same time, U.S. citizens complain that the Afghans were unwilling to fight the Taliban, although vastly more Afghans than Americans died fighting the Taliban. These frictions and gaps are built into the system and should never come as surprises to U.S. citizens or officials. Indeed, all parties should approach such negotiations with humility, since there will always be more than enough blame to go around after failures, like Afghanistan in 2021, just like there will always be more than enough praise to go around after successes, like the 2014 Maiden Revolution in Ukraine.

Partners are Imperfect:

As one would expect, partners typically have all the same problems the United States does, such as challenges in inter-ministerial coordination, competing priorities, limited government coordination with the private sector, legal systems that fail to keep up with technological change, inexperienced personnel in critical positions, etc.) U.S. partners often face additional challenges the United States does not, such as unstable currencies and immature or fragile institutions. Furthermore, partners have their own approval and budgeting processes, timelines, and election cycles, and these typically do not mirror those of the United States. It requires careful study for a U.S. official to learn both their own system and the partner's system well enough to resolve conflicts between the two. Any U.S. official who has developed the sort of mastery of both systems that would allow for true synchronization is likely due to rotate out soon.

The challenge of corruption requires special attention. U.S. officials frequently decry corruption in small, poor countries, such as Afghanistan or Bosnia, while conveniently forgetting the number of American governors who spend their retirement in prison, and the corruption challenges of rich and powerful allies. For example, the unofficial slogan of French President Jacques Chirac's 2002 re-election campaign was, "vote for the crook [the incumbent Chirac], not the fascist [the challenger, Marine Le Pen]."[189] It is

also important to remember that the personal relationships that are so critical to getting things done both inside the U.S. government, and between the American government and its foreign partners, can look like corruption, or at least favoritism, from the outside.

Furthermore, structural challenges are often present, such as bureaucratic regulations that are so complex that they require someone to break the rules in order to get anything done. For example, if one regulation requires "permit A" before a person can apply for "license B," but another regulation requires "license B" before a person can apply for "permit A," then no one will ever get either unless some official breaks the rules. The official will only break the rules for friends, or in return for bribes, and thus the system requires corruption to operate. Another common problem is low official salaries for bureaucrats, sometimes due to rapid inflation that is not matched by adequate raises. When salaries are inappropriately low, officials are virtually required to supplement their incomes with bribes. Corruption has dozens of other nuances that are too numerous to list here, but the important point is that corruption is a systemic problem that is likely to demand cultural change within a society and its institutions, as well as significant regulatory reform, and both will be opposed by the people who benefit from the current system. Attempts to fight corruption, and the myriad other challenges facing U.S. partners, are doomed without patience and clear understanding of these challenges.

The United States is Rich and Powerful:

The United States has been the richest country in the world for a century, and has been the most militarily powerful country in the world for at least the last 30 years, since the dissolution of the Soviet Union. Everyone knows this. Those who oppose the United States believe they are proving their extraordinary courage by opposing such a powerful nation and will claim those who support American policy are cowards who do so out of fear. Those who oppose the United States will also claim that by opposing them. they are proving that they have noble, non-financial motives since a nation as rich as the United States will presumably help friends financially and hurt enemies in equal measure. They will also claim that those who support U.S. policy are corrupt and greedy and abandoning their principles in pursuit of a big payday from the rich Americans. These are inescapable features of U.S.-partner relations in much of the world and American officials need to keep in mind the fact that their partners are being criticized as cowards and sell-outs and that those who oppose Washington's policies are loudly proclaiming their courage and nobility of purpose. U.S. opponents will also claim that the country is too powerful (hegemonic), present in too many places, and that the freedom and independence of every state requires, first and foremost, opposition to the United States. Again, these

consistent themes in adversary narratives need to be understood and anticipated by U.S. officials.

The U.S. is Far Away:

For U.S.-partner relations, at least those outside the Western Hemisphere, geography is a double-edged sword. To everyone in their regions, U.S. competitors like Russia, the PRC, and Iran, will consistently emphasize the fact that the United States is far away and that the Americans can, and almost certainly will, eventually leave, whereas they have been involved in their regions for millennia because they can never leave. Russia, the PRC, and Iran will also say the geographic facts mean that, sooner or later, everyone in their region must come to some sort of accommodation with them. So, the logic runs, regional neighbors should quit stalling, give Russia, the PRC, and Iran what they want, and send the Americans home. Of course, this contradicts the idea of the United States as a global hegemon described above. Russia, the PRC, and Iran conveniently ignore the contractions in their narratives, but U.S. officials should never hesitate to emphasize them.

While the vast distance between the United States and many of its partners is exploited by Russia, the PRC, and Iran to discredit American commitments and staying power, that same distance also has advantages. First, the centuries of interaction between Russia, the PRC, and Iran and their neighbors have often been fraught with conflict. The historic hostility between Russians and Poles, Chinese and Koreans, Persians and Arabs, etc. make Russia, the PRC, and Iran unappealing partners to many of their neighbors, and those hostilities are compounded, not mitigated, by the permanence of geographic proximity. The United States, by contrast, is very far away, as Saudi King Ibn Saud famously said, and that distance makes the U.S. presence inherently less permanent and overbearing than domination by a stronger regional neighbor. For smaller nations, the United States thus provides the best available counterweight to hostile local hegemons like Russia, the PRC, and Iran.

Reverse Poker and Limited Command and Control

Until official IW doctrine is published, readers seeking doctrine-like tips on the mechanics of planning the military portions of irregular warfare campaigns should turn to David H. Ucko and Thomas A. Marks' *Crafting Strategy for Irregular Warfare*.[190] Since non-military tools are typically the key to success in long-term IW campaigns, we will instead discuss the "reverse poker" technique for integrating interagency, international, multinational, and commercial capabilities. Reverse poker builds on President Harry

Truman's observation that, "it is amazing how much you can accomplish if you do not care who gets the credit."[191]

In a normal game of poker, the players conceal their cards from the other players at the table, and each player tries to build the best possible hand, with incentives to misrepresent them to other players. In reverse poker, the players turn their cards around, show them to the other players at the table, and share them openly so that each player can build a much better hand than would have been possible independently. In IW, the figurative cards may be of many types—information, authorities, assets, relationships, etc.—and there are many figurative card tables—embassies, remote locations, any sort of meeting or interaction, etc.—and the parties probably will not share all of their cards with every other player, but the default in poker is to bluff and compete, whereas the default in reverse poker is to inform and assist.

As might be imagined, reverse poker tends to produce better hands for everyone at the table and since the strategic competitors—Russia, the PRC, Iran, VEOs, etc.—are not at the table, better hands for all interagency, international, and commercial partners improve the odds of success for the United States and its partners at the expense of competitors. Of course, there are valid reasons not to share everything with everyone, but concern over who gets the credit should not be one of them since there will be more than enough credit to go around when the United States and its partners succeed, and more than enough blame for everyone when they fail.

Reverse poker relies on weak command and control relationships. An overbearing command structure would simply take all the cards from all the players and redistribute them as the leader sees fit. Such a "unity of command" approach is often useful in large scale combat operations, but in IW, where there is no single authority over all of the interagency, international, commercial, and non-governmental partners involved, such centralization is not practical and efforts to impose it will merely inspire resentment, evasion, and sabotage. Instead of through a single, all-powerful commander imposing his will, Color Revolutions have succeeded through informal and emergent cooperation and collaboration.[192] These IW successes can be replicated, but not with overbearing command and control.

Conclusion

The United States has enjoyed significant success in IW but faces major challenges from the PRC, Russia, Iran, and transnational terrorists. Future success will require the United States to sustain long-term IW campaigns. Sustaining such campaigns typically

requires a close connection between objectives and enduring U.S. values. International partners are usually vital to U.S. success in IW, so American officials need to develop an extremely sophisticated understanding of partners' fears, cultures, and goals in order to get the best possible long-term cooperation from each of them while also, when necessary, facilitating reform of partner institutions. All of this is facilitated by the "reverse poker" approach to interagency, international, and private sector cooperation.

About the Author

Dr. Thomas Searle is a retired U.S. Army Special Forces officer and noted scholar of special operations, including an influential theory of how they work. In uniform, he served in many joint special operations task forces in Afghanistan, Colombia, Iraq, the Philippines, and elsewhere. He has written classified histories of counterterrorism operations and organizations. As a civilian war planner at U.S. Special Operations Command, Dr. Searle worked to address global terrorist threats in an era of strategic competition. He helped develop and refine the U.S. Global Campaign Plan to Counter Violent Extremist Organizations and synchronize its implementation around the globe. Dr. Searle is currently a Professor of Interdisciplinary Studies in the Center for Adaptive and Innovative Statecraft at the Joint Special Operations University.

Discussion Questions:

1. This chapter considers NATO enlargement and Color Revolutions to be irregular warfare successes by the United States and its partners because similar achievements by competitors would have been viewed as IW successes by them. Do you agree or disagree with this argument? Why? If Color Revolutions and NATO enlargement are not IW, then what are they?

2. This chapter suggests some reasons why Russia, Iran, and the PRC have enjoyed limited success in irregular warfare. What are they? In your opinion, what else might be holding them back? Can you think of IW advantages adversaries enjoy over the United States? How should the United States mitigate those adversary advantages?

3. This chapter advocates a reverse-poker approach. What does this mean? What benefits does it offer? What are the obstacles to adopting a reverse-poker approach? Have you ever tried something similar? How did it work? Can you think of one of your previous experiences, or a historical case, where the reverse-poker approach might have been helpful? For example, could it have been helpful prior to the 9/11 terrorist attacks?

4. This chapter makes some very specific general claims about U.S. partners. What are some of those claims? From your experience, do those claims ring true? Are there additional common features of U.S. partners that this chapter did not include?

Recommended Reading:

In the century since World War I, the idea of regular, or conventional, warfare has been remarkably consistent: soldiers in uniform, tanks, cannons, rockets, combat aircraft, warships and submarines, etc.—all serving recognized nation-states in operations where both sides recognize that they are at war, even if formal declarations of war have not been exchanged. However, the image of irregular warfare has evolved over time from a focus on communist rebels during the Cold War, to terrorists and Islamic insurgents after 9/11, to problematic acts of competition below the level of direct, large scale, combat operations in the current era of strategic competition. These suggested readings track this evolution in IW.

- Bernard B. Fall, "The Theory and Practice of Insurgency and Counterinsurgency", *Naval War College Review,* 3 April, 1965. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=7049&context=nwc-review
- This was a lecture given by Bernard Fall in December 1964, just as the United States was rapidly expanding its troop presence in Vietnam. It reminds us that Western incompetence in IW was already a cliché by 1964, and describes how communist rebels, inspired and assisted by state sponsors in Moscow and Beijing, employed terrorism and guerrilla warfare to advance the cause of global communist revolution. While their sponsors in Moscow eventually collapsed, and their sponsors in Beijing abandoned them, communist rebels still accomplished things in Asia, Africa, and

Latin America during the Cold War that put to shame anything terrorists and U.S. competitors have achieved since the end of the Cold War.

- Michael G. Mullen, Chairman, Joint Chiefs of Staff, *Irregular Warfare: Countering Irregular Threats Joint Operating Concept Version 2.0* (Washington, D.C.: Department of Defense, 17 May 2010). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510
- This represented the official understanding of IW in the U.S. military during the post-9/11 era, when counterterrorism and counterinsurgency against Islamic extremists like al-Qaeda and the Taliban were the main IW challenge.
- Mark A. Milley, Chairman, Joint Chiefs of Staff, *Joint Concept for Competing* (Washington, D.C.: Department of Defense, 10 February 2023). https://s3.documentcloud.org/documents/23698400/20230213-joint-concept-for-competing-signed.pdf

In the current era of strategic competition, the main purpose of IW is to create, sustain, and expand advantage in strategic competition short of direct, large scale combat operations against U.S. competitors. The current definition of irregular warfare should probably be: the military contribution to strategic competition (or competitive statecraft). This document is the official statement of how the U.S. military will contribute to strategic competition in the future and hence the official, unclassified IW bible for the American military in the years to come. Note that the people who wrote and approved the 2023 concept had been active during the era of previous IW concepts and, for better or worse, that experience influenced the 2023 Concept.

There are a growing number of online resources for tracking the continuing evolution of IW thinking. Good places to start are the Irregular Warfare Initiative https://mwi.usma.edu/irregular-warfare-initiative/ and the Irregular Warfare Center https://irregularwarfarecenter.org/

Cheap Toys and Deadly Results: The Rise of Guerrilla Air Forces

Richard D. Newton and Jennifer N. Walters

ABSTRACT

Commercial, off-the-shelf drones, cameras, and communications have dramatically changed the character of modern warfare. Malign nonstate actors have adopted benign technologies to shift the air power paradigm. Now, small states and rogue actors are able to intimidate and coerce their opponents using tools and techniques previously only available to the air forces of rich, developed nations. This chapter explores the implications of future security threats posed by the employment of low-cost, user-friendly, and highly-capable aerial drone technologies by malign nonstate actors. It asks readers to consider how the diffusion of these high-tech capabilities (e.g., artificial intelligence, 3-D printing, miniaturization, remote-controlled air, land, and maritime systems, multi-spectral sensors, and encrypted communications, etc.) is changing and will continue to change the character of modern irregular warfare.

Introduction

Drones have a perception problem. In large part, this perception emanates from the debate over targeted killing programs using medium-altitude long-endurance drones.[193] The rapid proliferation of inexpensive, commercially available, and easy-to-use personal drones means that even ordinary citizens with a few hundred dollars and a modicum of technical skill can now capture high-resolution photographs and videos. They can also carry small cargo loads over long distances to places previously inaccessible to the general public.[194] Today, there are more than nine million drones operating in the United States. Roughly one in 10 Americans own a personal RC (remote- or radio-controlled) vehicle for recreational purposes. Maritime drones that operate on the water, or below the surface, are not as readily available as aerial drones, so while this chapter acknowledges them, the preponderance of malign drone use is focused on unmanned *aerial* vehicles.

In 2019, the U.S. Federal Aviation Administration (FAA) reported more than one million registered drones. Remotely controlled quadcopters and model airplanes were intended as tools for good: to help farmers selectively target areas needing fertilizer; to provide 24/7 surveillance of wildlife preserves to prevent illegal hunting; to monitor wildfires to more effectively direct fire crews; and to quickly and more accurately search large tracts of inhospitable terrain for lost or missing persons. They were, indeed, also designed for recreational purposes; hobbyists use their drones for purposes that range from amateur photography to quadcopter racing. Unfortunately, bad actors have misused them to invade personal privacy, create life-threatening dangers to commercial air traffic, smuggle drugs, transport weapons, and intimidate neighborhoods.[195] Among the unintended consequences of the democratization of any technology is the contortion of that new capability for ignoble aims. Drones are no exception. Criminals, terrorists, insurgents, paramilitaries, militias, rogue nation-states, etc. have discovered innovative ways to use recreational drones to coerce, intimidate, and circumvent the law. Increasingly capable and readily available commercial drone technology paired with sophisticated communications systems and 3-D printing, exacerbated by the involvement of malign actors, has created "guerrilla air forces." Small aviation teams such as ISIS's "Unmanned Aircraft of the Mujahideen" have used drones in hit and run tactics to ambush, harass, and embarrass conventional police and military units. These attacks undermine the government's ability to provide stability and security, and serve to intimidate civilian populations. These activities echo how guerrillas on land have confounded conventional militaries and security forces for centuries.

To clarify, the law of unintended consequences describes the notion that any action taken by individuals, governments, or organizations nearly always have multiple results, many that are unanticipated and sometimes undesirable. In this way, those consequences are also unintended. In a 2011 TED Talk, historian Edward Tenner pointed out that human technological capabilities have been increasing geometrically over time, but our ability to predict the implications of those increased capabilities has failed to keep up.[196] In the case of unmanned vehicles—whether air, maritime, or terrestrial—an exquisite technology intended for peaceful and commercial use has also been deployed in problematic applications. What the inventors, engineers, and entrepreneurs failed to foresee, however, were the ways that enterprising bad actors might employ these creations in novel ways underpinned by malevolent intent.

Background

Unmanned aerial vehicles (UAV) are not new. One of the earliest recorded uses of UAVs was in 1849 when Austria sent 200 hot-air balloons packed with explosives over Venice during a siege. This early ancestor of contemporary drone technology evinced how a new air power technology can produce unexpected applications. More than 175 years later, Hamas continues to use incendiary balloons in terror attacks against Israel.[197] For airmen thinking about unmanned technology, the Austrian balloon experiment underscored the need for guidance and control of weaponized aerial vehicles.

Nearly a century after Austria's rudimentary drones, the British developed and flew the first truly unmanned guided aircraft in 1916, the Ruston Proctor Aerial Target. The British intended to use this kamikaze drone to ram German Zeppelins that were bombing England. The Ruston Proctor drones were controlled by radio using a technique developed by Archibald Low. Like the Austrian balloon bombs, the technology at the time was too immature to support the desired strategic goal, namely stopping German bombers, and the project was scrapped. Still, designers and engineers kept working to improve the technology. In 1918, American inventors Peter Cooper Hewitt and Elmer Sperry successfully demonstrated an unmanned Curtiss airplane stabilized by gyroscopes and controlled by radio. The war ended before the Hewitt-Sperry craft could be fielded.[198]

Between the two world wars, British engineers tested a number of radio-controlled unmanned aircraft in 1935. One of them, the De Havilland DH-82B Queen Bee, was an inexpensive target drone based on the Tiger Moth training airplane. Over 400 were built and flown by the Royal Air Force and Fleet Air Arm (Navy). It is thought that the

term "drone," which also refers to males in a honeybee colony, was inspired by the Queen Bee.[199]

During this period, the U.S. Navy and U.S. Army also experimented with controlling unmanned aircraft from a second aircraft primarily as targets for anti-aircraft gunners. Later, during the Second World War, the U.S. Army Air Force and U.S. Navy modified four-engine bombers to serve as flying bombs to attack hardened German submarine pens and launch sites for V-1 cruise missiles. This effort was code named "Project Aphrodite." A volunteer pilot and flight engineer would take the explosive-loaded bomber off, stabilize it at 2,000 feet, and then engage the autopilot. They would then transfer control of the drone to a mothership that would then fly the drone to its final target via remote control. The pilot and flight engineer would then arm the explosives, and bail out. Of the 14 missions attempted, none were successful, and the project was cancelled in January 1945.[200] The Germans, on the other hand, did develop and field a mildly successful drone, the *Mistel*. They paired a fighter with an explosive-laden, unmanned Ju-88 medium bomber. The fighter pilot flew the joined pair to the target, released the drone, and flew the fighter back to base. The trajectory towards autonomous flight arced aggressively through the following decades.

This curve of progress continued during the Cold War era, which saw advancements in engine and electronics technology. These critical technologies led to mature UAVs for photographic and signals reconnaissance, electronic warfare, leaflet dropping, and target practice, in addition to serving as cruise missiles. These unmanned systems made it possible to collect intelligence and spread information in areas defended by equally-advanced air defense systems. The post-war electronics revolution allowed miniaturization and commercialization of radio components such that RC cars and airplanes became available to the general public. As hobbyists, tinkerers, and inventors experimented and played with these inexpensive and readily available "toys," they naturally increased the pace of improvements and expanded the capabilities—chiefly range, endurance, and payloads.

From the early 1980s through the first decade of the 2000s, military drone capabilities advanced at a rapid pace, spurred by government investments and the desire to both increase aviation capabilities and reduce the burden of a human crews in the cockpit i.e., life support systems, the risk of shoot-down and capture, and the natural limits of endurance. In 2005, the FAA issued its first civilian airworthiness certificate for a drone to the General Atomics corporation.[201] The first drone pilot certificate, though, was not issued until 2016. By 2023, in order to grow drone expertise and professionalism

in the United States, the FAA registered over 100 universities, colleges, and technical schools in its Collegiate Training Initiative to prepare and certify American students for careers in unmanned aerial systems.[202]

On the commercial front, multinational business giants such as Amazon, Google, and UPS have been investing in the research, prototyping commercial technologies, and working with the FAA to develop safety protocols to enable small package deliveries by aerial drones. On the ground, Amazon, Google, and General Motors have received permits to allow fully autonomous, driverless ground vehicles.[203] And taking a different and transformative step in RC logistics, in 2020, Rwanda partnered with Zipline® to become the first nation in the world to use drones to deliver critical medicines and blood supplies to 19 remote hospitals and clinics.[204] Similar programs are saving lives in Australia and Latin America, throughout Asia and the Indo-Pacific region, and across Africa. As positive as these trends have been, though, it should be expected that malign actors would take note and twist the spirit of innovation to attain unintended malicious capabilities from these burgeoning drone technologies.

Even the simple presence of a UAV or an unmanned ground vehicle (UGV) exerts a powerful influence: a defender cannot ignore the risk the drone poses. In 2016, the Iranian backed terrorist group Hezbollah used a commercial UAV to drop two small bombs onto Syrian rebels, the first reported use of hobby drones to carry weapons. This trend persisted. In 2017, Hezbollah acknowledged its use of drones after striking Islamic State (IS) positions with bombs dropped from a commercial UAV.[205] In 2017, the first incident of an unmanned maritime vehicle was recorded when Houthi rebels in Yemen attacked a Royal Saudi Navy frigate with an explosive-laden remotely-controlled small boat,[206] with a similar feat repeated by the Ukrainians in 2022 when they modified a number of jet skis with Starlink antennas and infrared electro-optical devices to attack Russian ships in Sevastopol.[207] According to New America's 2020 database, there are two dozen nonstate groups from Japan, to Mexico, across to Africa, and up through the Middle East and Ukraine, that have used or are using unmanned aerial systems for: target reconnaissance and designation; resupply; surveillance; reconnaissance; and various forms of information operations.[208] On the global stage, the myriad applications of drones are growing more lethal, complex, and credible each and every day.

Adversity Leads to Innovation

Brent Goldfarb & David A. Kirsch's research into the history of innovation revealed a compelling insight: the rate of major technological innovations reached a

zenith during the Great Depression. Their insight suggests that calamity forces people out of their comfort zones and requires them to accept and adapt to change.[209] War, the ultimate calamity, intensifies the pace of change. While the exigencies of war have led to the rise of commercial airline transportation, modern antibiotics, and personal computing, to name a few well-intended examples, malign actors always find unexpected and unintended ways to repurpose technologies for malintent. The risk of nefarious technology exploitation is not only present but, in a more interconnected world, imposes more outsized consequences.

Seven years ago, in 2016, T.X. Hammes warned that the convergence of artificial intelligence, increased computing power, improved communications, multispectral sensing, and additive manufacturing (3D printing) was increasing the capabilities available to small, agile, and politically-motivated groups. The implications for future conflict presaged a world in which, "small, smart, and cheap weapons based on land or sea or in the air [could] dominate combat."[210] The implications for irregular warfare, he predicted, were significant because the mindset and strategic calculus of the malign actors able to develop and employ drones were so notably different, if not diametrically opposed to, that of nation-states. Hammes noted nonstate actors rarely possess the bases, population centers, or critical infrastructure a nation-state must protect, leaving them more agile and unconstrained. Most importantly, nonstate actors do not play by the same rules of warfare as do nation-states. The scale and scope of commitments, equities, and capabilities of nonstate actors versus nation-states render fundamentally different applications of technology, especially when that technology is accessible.

When one studies the history of warfare, a cyclical relationship between tactics and technological advancements emerges. More specifically, a new technology leads to counter-tactics and countermeasures, which then continually spur further development. Melvin Kranzberg has observed that technology is the process of manipulating the material world for human purposes.[211] When new, advanced systems change the battlefield equilibrium, and give one side an asymmetric technological advantage, then humans typically adapt tactics and procedures to address and counter these novel technologies, thus restoring equilibrium to the system. Similarly, when tactics stagnate, technology reacts to disrupt this stalemate. The stirrup, the chariot, the English longbow, gunpowder, the internal combustion engine, aircraft, and radios are just some examples of technologies that changed how humans fought but were also overcome by adapting tactics that led to even newer technologies.[212] Maj Gen Sir Anthony Trythall noted: "All military technological developments will in time be countered, and so on ad infinitum. Asymmetry leads to opportunities and symmetry leads to stalemate."[213] Therefore,

it is unsurprising that the contour of conflict often aligns to the spiral of this tactics-technology epicycle.

In early 2023, Ukrainian special operators speaking at a conference on special air warfare in the United States invited Western companies to come to their war-torn homeland to test their unmanned systems in combat conditions. Just as the Soviets used the crucible of the Vietnam War to test their weapons against U.S. systems, the Ukrainians highlighted the real-world opportunities Russia's invasion continues to provide to the West to advance the tactics-technology cycle. "This is the 'right time,' one Ukrainian military official said, 'to find weaknesses [in the Russian systems] and to determine solutions and how to deal with Russian [electronic warfare] systems. Because, in the future, you will have the same problem.'"[214]

The presenters also reported that the Russian direction-finding technology used to locate and attack their drone operators has been countered by placing the antennas for the control panels far from the drone operator, but even that tactic does not completely work. The Ukrainians further described how Russian electronic jamming limited their ability to control their small drones to a single frequency band, the same one used by the global positioning system for aviation, maritime, and terrestrial transportation systems safety. However, the limits of Russian aggression are not clear and even this band could potentially suffer targeted attacks, resulting in widespread communications degradation. In the laboratory of this current war, one can easily imagine how this constantly shifting balance of advantage can spur tactical and technical innovations and change.

From a malign nonstate actor's perspective, the engagement becomes challenging when the tactics-technology cycle favors the defense, specifically when the nation-state becomes more adept at detecting, denying, disrupting, and defeating the technologies malign actors use. Even under adverse conditions however, malign actors have shown they can effectively use commercial air, land, and maritime drone technologies to change the character of conflict by complicating the state's ability to defend its citizens and protect critical infrastructure.

How Do Malign Actor Drones Change the Character of Conflict?

Since 1914, air power has provided armies with an asymmetric advantage in the third dimension. The original mission for air forces focused on reconnaissance and surveillance to complement the scouting functions of horse cavalry. Later, air power

carved out its own niche—deep reconnaissance and surveillance where horses could not go—across vast oceans, over treacherous mountain ranges, and across the vagaries of jungles. As air forces and aircraft technologies evolved, they added air attack, long range artillery spotting, battle damage assessment, air transport, air mobility, communications, liaison, and medical evacuation to the capabilities air power offered. For approximately a century, developing this nascent range of capabilities demanded substantial investments to sustain air power advantages. Development, manufacturing, production, education, training, basing, logistics, and maintenance all required a level of sustained economic investment in air power beyond the reach of most nations. Therefore, control of the air has largely been the province of the rich and developed nations.

Beginning in Somalia in 1920, when Great Britain's Royal Air Force (RAF) used eight De Havilland DH-9A biplanes to find, attack, and defeat the Dervishes, rich and developed nations began to prefer air power as a cheaper way to control irregulars with fewer friendly casualties than costly ground operations.[215] 1998 marked the point where an insurgent group could credibly claim to possess an "air force." That year, the Liberation Tigers of Tamil Eelam (LTTE), a Sri Lankan insurgent group bent on establishing an independent state for Hindu Tamils, acquired a Robinson R-44 helicopter and a few microlight aircraft. This was the first recorded case of an insurgent group using aircraft in its attempt to overthrow a government. While the tactical outcomes from the 11 raids conducted by LTTE's Sky Tigers between 2006 and 2009 were relatively underwhelming, the propaganda coups and resourcing changes stemming from them were significant. More importantly, a precedent had been irrevocably set: air power was no longer the sole domain of the nation-state.

In 2004, Iran provided the Lebanese terrorist group, Hezbollah, with eight small Mirsad-1 UAVs equipped with cameras and a radar, along with operator and maintenance training.[216] Hezbollah initially used these drones for reconnaissance, but by 2006 they were using their drones for artillery spotting and dropping small bombs. As with the Sky Tigers in Sri Lanka, the individual tactical effects Hezbollah achieved were relatively minor, but many consequences emerged that influenced the state of the conflict. Drones were at the center of Palestinian propaganda campaigns, compelled changes to Israel's defensive programs, motivated new investments, and forced a reimagining of how attacks against the country might materialize.[217] This case depicts how guerrillas exploiting the air domain were largely ignored by developed nations who remained focused on medium-altitude, long-endurance drones that were closer in technology to the high-end systems typical in modern air forces.[218]

While Western governments were dismissing the irregulars' use of small, commercial drones as negligible threats, other irregular forces were taking close note and studying this disruptive practice. In 2018, an anti-government faction in Venezuela flew two explosive-laden, GPS-guided DJI M600 drones over a parade in Caracas attended by the country's president, Nicolás Maduro.[219] While no one was killed, the incident caused international outrage across the political spectrum, and gave credence to previously discounted warnings from academics, government officials, and drone scholars who had cautioned that commercial, easy-to-use, and relatively inexpensive drones could take the tactics-technology cycle into a new, and unforeseen, iteration of political violence and irregular warfare.

In December 2018 and January 2019, the presence of small commercial drones, in these instances flown by hobbyists, shut down flight operations at London's two busiest airports. Heathrow, an airport that supports over 1,200 flights per day, shut down for an hour, while Gatwick, which supports more than 800 flights per day, remained closed for 32 hours.[220] While there was no obvious nefarious intent during these two incidents, the reaction by British authorities illustrates the danger that small unregulated and unidentified commercial drones pose to infrastructure and civilian routines.[221] In 2019, Houthi rebels in Yemen launched a swarm of small, Iranian-provided, drones and cruise missiles against oil processing facilities at Khurais and Abqaiq, some 500 miles inside Saudi Arabian territory. The Saudi air defense system, one of the most sophisticated in the world, was useless against these low flying and slow-moving UAVs, which had been launched from three different locations but synchronized to simultaneously arrive on target from three different trajectories.[222] This attack suspended half of Saudi oil production for a number of weeks and caused ripple effects throughout the global economy.

Government agencies, security forces, and political leaders can no longer ignore the implications of commercial technologies that enable this form of air power. Cheap, accessible drones empower small nations and nonstate actors to exploit the 3rd dimension and achieve outsized effects with otherwise small, and often merely symbolic, actions. For millennia irregulars have used ambushes, hit-and-run attacks, harassment, and symbolic gestures to force emotional overreactions, spread malign information, and create various psychological effects. T.E. Lawrence noted in *Seven Pillars of Wisdom* that guerrillas did not achieve decisive effects when facing national armies, but rather, they were, "an influence, an idea, a thing intangible, invulnerable, without front or back, drifting about like a gas." Modern, commercially-available, easy-to-use, increasingly-capable, and relatively-inexpensive drone technology has underscored Lawrence's characterization by

giving irregulars the ability to now use, "the smallest [air] force in the quickest time at the farthest place" to surprise their opponents, from the air, with little to no danger to the guerrillas.[223]

The Asymmetric Advantage Granted by Air Power Has Changed

The Islamic State of Iraq and Syria (ISIS) has proven to be one of the more creative and innovative groups when it comes to the use of commercial drone technologies. Because they faced opponents wielding overwhelming military power and boasting extreme resource overmatch, they approached their strategic situation using a logic discounted by conventional Western planners. This same logic, however, would have been familiar to Lawrence. ISIS needed to reconnoiter, develop, and strike targets that would cause significant psychological, but not necessarily military, impact. Their use of divergent thinking—unconventional, non-linear, and non-Western—led them to solutions that induced panic among civilian populations and drove up the cost of counter-drone operations. From this vantage point, they were highly successful in attaining their strategic goals. By executing drones strikes unpredictably, ISIS embodied the small guerrilla force tipping the scales of power towards themselves and away from a militarily superior opponent.

Between 2016 and 2017, ISIS identified and exploited a flaw in American air superiority over Syria. In 2018, they launched a swarm of homemade drones against Russian bases in Khmeimim and Tartus in Syria. In addition, ISIS experimented with RC cars as small, mobile improvised explosive devices. They also sought commercial crop-dusting drones to deliver low-grade nuclear materials.[224] While this drone program, like ISIS itself, has been severely degraded and somewhat controlled, the implications for the future remain significant. Other nonstate actors, disadvantaged small states, and proxy groups inspired by the ISIS's achievements are learning from their example how to develop their own, indigenous versions of drone warfare.[225]

While the Islamic State's innovative use of commercial drone technology was remarkable, a more important consideration was how their strategic thinking evolved to change the character of irregular warfare. Tactically, ISIS developed and deployed low-cost unmanned, aerial, systems to challenge American and Russian technological superiority in Syria. Between 2015 and 2017, ISIS quadcopter drones carried out 60-100 attacks against coalition forces each month. In 2016, Gen Raymond Thomas, then the commander of US Special Operations Command, opined that the most daunting

problem U.S. special operations forces (SOF) faced was, "an adaptive enemy who, for a time, enjoyed tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones." This characterization attests to the tactical effectiveness of the Islamic State's drone program.[226] General Thomas's observation also reinforced the shift in the tactics-technology cycle, showing how an underestimated opponent frustrated coalition air superiority and became the first enemy combatant to attack American troops from the air since April 1953.[227] For the first time in more than half a century, American troops, rear areas, and transit routes were now vulnerable to enemy aircraft dropping bombs on their heads, while the operators of those remotely piloted enemy aircraft faced little to no combat risk.

It was at the strategic level, though, that ISIS demonstrated how their drone program created what has been called a "poor man's air force"[228] that could influence politicians and cause fear among targeted populations and military units. The potential psychological effects wrought by drones are highly attractive for nonstate actors seeking to publicize their exploits. ISIS used high-resolution cameras such as Go-Pros® to record their operations and then turned those videos into propaganda to demonstrate the accuracy of their bombing, the inability of their adversaries to defend against them, to highlight their drone operations, and to advertise to like-minded state and nonstate actors. ISIS overtly demonstrated their unexpected technical prowess, but also brandished their tactical reach and power. Ultimately, they used drone footage to tell a story that Americans no longer controlled the air, offering a how-to guide for other creative and determined antagonists to threaten coalition forces by infiltrating sovereign airspace. In 2020, al-Shabaab militants from Somalia used a small fixed-wing drone to reconnoiter and coordinate its devastating attack of the joint U.S.-Kenyan air base at Manda Bay. Al-Shabaab later released the video to demonstrate and publicize their achievement.[229]

Another challenge posed by small commercial drones is their ability to provide real-time overhead surveillance, reconnaissance, and targeting data. Consumer drones and modern camera systems allow hobbyists to stitch multiple still photographs together to create super-wide fields of view, following a dozen moving targets simultaneously, and incorporating night vision technologies into guerrilla air forces' airborne ISR capabilities. In 2011, the Libyan Transitional National Council forces used a small Aeryon Scout quadcopter, fitted with both conventional and thermal-imagery cameras, to observe enemy positions and avoid attacks as they marched from Misrata to Tripoli.[230] In July 2022, the Islamic State affiliate in West Africa used a quadcopter drone with a camera to discover and avoid a planned ambush in northeastern Nigeria.[231]

Modern air defenders now face similar algebraic challenges to those Lawrence had said were facing the Turks during the First World War: specifically, trying to defend 140,000 square miles against extremely mobile guerrillas who could strike from anywhere, yet were nearly impossible to find and thus impossible to bring to battle.[232] The number of counter-UAV (C-UAV) air defense systems needed to protect valuable potential targets has hugely raised the costs imposed by small weaponized drones. Adding to these costs is the infrastructure needed to train operators and maintenance personnel for such systems. One must also consider the complexity of the command and control (C2) network that manages a C-UAV system alongside the conventional air defense system. To illustrate the expense to defend against such threats, the Raytheon Coyote interceptor is an expendable drone that is advertised as a low-cost counter to weaponized commercial drones. The Block 1 version costs approximately $15,000 per warhead, or about 10 times the cost of a high-quality commercial drone. Other proposed upgrades increase the system's capabilities and effectiveness but at increasing cost, including additional procurement, training, manpower, and sustainment. Similarly, the Russian Pantsir S-1 surface-to-air missile and gun system has proven to be a highly effective at defending against low-altitude drones.[233] The $14 million price tag for each Pantsir system further illustrates the cost dilemma posed by the weaponization of commercial drones. As Audrey Kurth Cronin noted in her examination of the implications of technology dispersal, even the most sophisticated counter-technologies have limited utility when facing irregular enemies using available technologies in unconventional ways.[234]

In a 2022 study considering the impact of drones on the character of modern warfare, five Italian researchers examined the tactics-technology cycle, what they called "hider-finder competition" regarding air defenses. After looking at three conventional conflicts where the use of drones was extensive, they concluded that the future of warfare would become more difficult, demanding, and expensive.[235] As expected, the stronger and richer, rather than the weaker and poorer, sides usually prevailed in the drone-counter drone competition. What they did not look at, however, was the impact of guerrilla, or "poor man's," air forces during these irregular conflicts. In those instances, the stronger and richer adversary typically holds the military advantage, but like the Ottoman Turks Lawrence and the Arabs faced during the First World War, defending against irregulars who could be everywhere, yet nowhere, becomes draining and difficult to sustain. In this case, irregulars posed more of a psychological than physical threat and had no need for extensive logistics, research, development, and training infrastructures. Guerrilla air forces require their opponents to defend the depth, length, and breadth of their territory against an enemy that retains the initiative, now in three dimensions. Such initiatives

become much more expensive. Drones enable irregulars to add an enormous premium to the price tag of defense.

What Next?

According to the U.S. Department of State's Bureau of Counterterrorism, Iran continues to provide drones, training, and funding to both the Houthis and Hezbollah.[236] Future off-the-shelf drones will be able to carry heavier loads, fly farther, loiter longer, maintain contact at greater distances from the operator, and communicate reliably using secure links. Air defenses have proven effective against drones. Electronic warfare efforts have also proven effective at detecting, disrupting, and defeating the connection between the controlling operators and the drones. Thus, the cycle continues.

The threat and sophistication of drone attacks and surveillance will continue to evolve. Among more recent developments in this domain is the deployment of drone swarming capabilities. While drone swarms have been a source of popular entertainment for almost a decade, the weaponization of such swarms is novel. For example, pairing armed air and maritime swarms simultaneously to attack a target is a cutting-edge application.[237] For commercial light shows, micro-UAVs equipped with LEDs, a GPS sensor, and a communications module–all controlled by a central computer on the ground—have become the "new fireworks" according to *Fortune* magazine. In 2018, Intel Corporation set a world record for the largest drone swarm performance during the Winter Olympics.[238]

The January 2018 attack by a swarm of 13 aerial drones against Russian bases in Syria, however threatening, was relatively ineffective. While each drone carried up to 10 one-pound bombs. Pantsir S-1 surface-to-air missiles shot down seven of the drones and electronic warfare systems allowed the Russians to hack into the drones' controls and recover the other six.[239] Four years later, in October 2022, the Ukrainians attacked the Russian Black Sea Fleet in Crimea using a swarm of 16 mixed-capability drones, nine aerial and seven maritime drones. The combination swarm hit a frigate and a minesweeper, inflicting only minor damage, but the psychological and morale implications were huge. The drones were able to penetrate Sevastopol's harbor defenses, thus shattering the Russians' sense of security. Naval analysts noted that while the attack did not have the same impact as previous Ukrainian sinkings of Russian ships in the Black Sea, it did suggest a new era of naval warfare. What was previously a theoretical threat to modern naval warships had become reality.[240]

As drone swarming technology becomes more readily available to less sophisticated users, countering drone swarms will present significantly more intractable defensive challenges. Despite robust air defense systems, some armed drones will inevitably get through. Ukraine estimates that it has been able to shoot down or disrupt between 60 and 80 percent of the Russian drone swarms it has faced. Even with that level of success, however, the drones have destroyed almost a third of Ukraine's electrical power stations, and killed hundreds of civilians.[241] So far, the ability to swarm multiple drones has proven to be a more difficult technological feat, but as the tactics-technology cycle spins, that will soon no longer be true.

In June 2022, a Puerto Rican company, Red Cat Holdings, announced its subsidiary, Teal Drones, would offer its Golden Eagle in a four-drone swarm system to commercial customers. The tablet-sized controller displays up to four video feeds at a time, gives a 360° field of view, and is intentionally intuitive and easy to use.[242] The Teal Drones' web site advertises the system with encrypted communications between the drones and the controller, night-vision capabilities, and the ability to simultaneously control both air and ground-based drones. The Chinese demonstrated military-grade drone swarming technology in 2022, and Russia, India, Turkey, and Israel are all working assiduously to develop their own drone swarming technologies. It is not hard to imagine this technology transitioning to hobby drones, and from there quickly reaching state and nonstate actors. In their hands, able and willing to weaponize these swarms for nefarious aims, this technology can metastasize into terror.

The question becomes, then, how to counter drone swarms? Electronic jamming, lasers, cyber-attacks, and counter-swarms are all being tested. The U.S. Navy tested a LOCUST (low-cost UAV swarming technology) system that was able to control a swarm of 50 Coyote C-UAV drones. Its purpose is to counter an enemy swarm with a friendly one. The U.S. Air Force Research Laboratory developed and tested a high-powered radio frequency weapon that overwhelms the drones' circuits, thereby causing the swarm to lose control and crash. Laser weapons can overheat drone circuits. Traditional jamming systems have proven effective against less-sophisticated commercial drones, but malign actors are already adapting communications encryption to protect their drones from jamming.

Conclusion

Using history as a guide, one outcome appears all but certain: the tactics-technology cycle will continue to spiral. T.X. Hammes's warning about the sinister implications

of combining increasingly capable and available technologies with malicious actors was accurate but not notably prescient. In fact, it should have been expected. Alfred Nobel created dynamite as a safe alternative for construction and mining, while IBM created the first smart phone to give people mobile access to their email and telephone. Anarchists, revolutionaries, terrorists, and criminals adapted these and other benign technologies—robotics, 3-D printing, cameras and sensor technologies, smart phones, and computers—for nefarious purposes. This pattern has existed for as long as humans have been manipulating technology in an attempt to shape and control their shared environments.

In the case of drones, governments, security practitioners, and policymakers must think like their adversaries. They must fully delve into divergent ways of thinking to consider how innocent technologies might be used, alone or in combination, to intimidate, coerce, and attack. Only then do they have a reasonable chance of getting out in front of malign actors who are unconstrained by bureaucratic processes that can slow revolutionary, evolutionary, and opportunistic innovation. Developed nations must contend with the constraints of fiscal year funding, research and development systems, logistics and training infrastructures, legal frameworks, and ethics considerations. This is a reality that will not change. The global security environment, from the American perspective, peers wearily at the sources of great power competition with an increasingly myopic focus. Undoubtedly, these threats demand the tools to competitively overmatch and credibly deter potential adversaries. However, balancing such a complex set of threats is essential. A lack of attention on the widespread and powerful employment of drones in irregular warfare will not ebb to the rising tide of strategic power competition and conflict. If national leaders remain fixated on the large, high-tech, and costly weapon systems needed to deter the likes of China and Russia, rather than the pervasive threats posed by low-cost and easily adaptable technologies being fielded by guerrilla air forces, then we—the U.S. and our partners and allies—risk being overwhelmed or priced out of the fight by enemies who shop at Amazon, Best Buy, or Walmart.

About the Authors

Richard Newton is a retired USAF Air Commando and combat rescue helicopter pilot. He volunteers as an editor for, and occasional contributor to, the *Air Commando Journal*, Irregular Warfare Initiative, and Irregular Warfare Center, while also researching and writing about air power, irregular warfare, and special air warfare in conflicts short of war. He is a graduate of the USAF Academy, holds masters from the U.S. Army School of Advanced Military Studies, and earned a PhD from King's College London.

Jennifer Walters is an active-duty Air Force pilot. Most recently, Jennifer served as the lead speechwriter to the Chairman of the Joint Chiefs of Staff in Washington, DC. As a KC-10A instructor pilot, she led aircrew on air refueling, humanitarian, and contingency operations across the globe. She is a distinguished graduate of the United States Air Force Academy and holds a Master of Philosophy and PhD in policy analysis from the RAND Graduate School. She serves as the executive director of the Irregular Warfare Initiative.

Discussion Questions:

1. What are the possible future security implications of low-cost, user-friendly, highly-capable, and relatively-inexpensive aerial drone technologies for modern contemporary warfare?

2. How should nation-states threatened by rebels' use of drone technologies address the proliferation of highly capable commercial, off-the-shelf systems?

3. Has the diffusion of high-tech capabilities (artificial intelligence, 3-D printing, remote-controlled air, land, and maritime systems, multi-spectral sensors, and encrypted communications, etc.) put conventional military and security forces "on their back foot,"—and if so, in what way(s)?

4. Propose four to five (two to three near-term and two to three mid-term) opportunities—political, diplomatic, legal, economic, informational, cyber, and/or legal—to degrade, disrupt, or deny the ability of malign nonstate actors to acquire, develop, and employ air, land, and maritime drone technologies.

5. What should policymakers, security practitioners, and other governmental planners do to mitigate and manage the threats posed by surveillance and armed drones flown by malicious actors?

Recommended Reading:

- David Hambling, *Swarm Troopers: How Small Drones Will Conquer the World*, (Venice, FL: Archangel Ink, 2015)
- Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, (New York: Oxford University Press, 2019)
- Michael J. Boyle, *The Drone Age: How Drone Technology Will Change War and Peace*, (New York: Oxford University Press, 2020).

Legal Gamesmanship: How China and Russia Use International Law in Geopolitical Competition

Jonathan G. Odom

ABSTRACT

An array of concepts, such as "legal instrumentalism," "lawfare," and "legal warfare," have developed to describe how nation-states use law, particularly international law, in their relations with one another. But increased competition between nations in contemporary international relations has shown that these existing concepts are imprecise, antiquated, or underinclusive. As an alternative, this chapter offers the preferable alternative concept of "legal gamesmanship" to capture how nation-states use international law in contemporary international relations through all instruments of national power (i.e., beyond just militaries) and across the full continuum of competition (i.e., beyond just armed conflict). More specifically, legal gamesmanship can be defined as "conduct by a nation-state, or otherwise attributable to a nation-state, which leverages or exploits the structural, normative, or instrumental functions of

international law in order to achieve that nation-state's objectives within a competitive environment." This chapter defines the concept of legal gamesmanship and explains its constituent elements. It also applies this definition and describes real-world examples of China and Russia employing legal gamesmanship in their respective competition with the United States and other nation-states. Nation-states must be able to recognize situations when legal gamesmanship is being employed against them, and they must consider lawful, appropriate, and effective ways to counter such actions.

Introduction

A fundamental and recurring challenge in international relations is the imperfection of words that humans choose when discussing the behavior of states (i.e., nation-states). These problematic word choices can arise in the rhetoric of political officials, as they either seek to justify the decisions and actions of the states they represent or criticize those made by others. These word choices can also occur in the discourse of academic scholars, as they observe and analyze the official decisions and actions of states and attempt to discern patterns and derive concepts from them. Some words, through overuse in political and academic discourse, run the risk of becoming worthless. This was the warning issued over 75 years ago by the British author George Orwell. Known best for his political novels *Animal Farm* and *1984*, Orwell also penned an insightful essay titled *Politics and the English Language*. Published in 1946, Orwell's commentary on linguistics observed that certain words are "political words" having "several different meanings which cannot be reconciled with one another," with the result being that such words risk becoming "meaningless."[243]

One example of problematic word choice in contemporary international relations involves the various uses of the word "warfare" within terminological phrases to describe theoretical concepts. In general, a traditional dictionary definition of warfare is, "armed conflict between two massed enemies," while a doctrinal explanation is, "[t]he mechanism, method, or modality of armed conflict against any enemy."[244] However, government officials and academic scholars tend to use the word "warfare" in a broader sense. Consider the following noteworthy instances of such usage. In 1948, U.S. diplomat George Kennan famously defined political warfare as, "the employment of all the means at a nation's command, short of war, to achieve its national objectives."[245] As early as 2001, official doctrine of the U.S. Department of Defense (DoD) defined irregular warfare as, "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population."[246] More recently, DoD strategic guidance

has notably dropped the modifier "violent."[247] Beginning in 2003, the People's Liberation Army (PLA) directed Chinese forces to, "conduct public opinion warfare, psychological warfare, and legal warfare" in what have come to be known colloquially as "the three warfares."[248] In 2013, Russian General Valery Gerasimov observed a, "change in the character of warfare" to include, "the use of political, diplomatic, economic and other nonmilitary measures in combination with the use of military forces," which Russian military commentators have labelled "new generation warfare."[249] These uses of "warfare"—accompanied by modifiers like political, diplomatic, legal, psychological, public opinion, or irregular—are questionable, given that many of them involve scenarios short of armed conflict.

This proliferation of "warfare" labels in the contemporary discourse of international relations can be problematic on multiple levels. From a legal perspective, nation-states have deliberately moved away from categorizing hostile activities as "war" in terms of international law. After World War I, states collectively renounced "war" as "an instrument of national policy in their relations with one another."[250] After World War II, states declared that they were "determined to save succeeding generations from the scourge of war."[251] Rather than speak further in the status terminology of "war," however, they focused more generally on the nature of state competition by agreeing to, "refrain in their international relations from the threat or use of force" against other states.[252] Likewise, many of these same states agreed to apply the international legal rules of warfare to, "all cases of declared war or of any other armed conflict" between states, "even if the state of war is not recognized by one of them."[253]

Additionally, the overuse of "warfare" in contemporary discourse can be confusing or distracting to various audiences, particularly those with limited or no military background. In the appropriately titled book, *How Everything Became War and the Military Became Everything*, law professor and former Pentagon official Rosa Brooks observed:

> Today, we're coming again to one of history's crossroads. As the familiar distinctions between `wartime' and `peacetime,' `armed conflict' and `crime,' `foreign affairs' and `domestic' issues, and the `military' and `civilian' domains lose all clarity, the elaborate legal and institutional architecture designed to constrain state power and protect individual rights is growing increasingly unstable, both globally and in the United States. There's nothing natural or inevitable about any of our familiar categories or distinctions. They are products of human

> minds, conceived as a means of organizing ourselves and channeling violence and coercion at a particular moment in history. We created the categories we use, and if they're no longer serving the purpose we want them to serve, we can change them.[254]

Similarly, the U.S. National Security Strategy (NSS) of 2017 recognized that war has perhaps become an antiquated term to describe political relations among major powers and should be replaced with the more appropriate concept of competition:

> The United States must prepare for this type of competition. China, Russia, and other state and nonstate actors recognize that the United States often views the world in binary terms, with states being either 'at peace' or 'at war,' when it is actually an arena of continuous competition. Our adversaries will not fight us on our terms. We will raise our competitive game to meet that challenge, to protect American interests, and to advance our values. Our diplomatic, intelligence, military, and economic agencies have not kept pace with the changes in the character of competition. America's military must be prepared to operate across a full spectrum of conflict, across multiple domains at once. To meet these challenges we must also upgrade our political and economic instruments to operate across these environments.[255]

Clearly, "competition" has become a preferred description of relations between major powers for the foreseeable future, given that the preceding NSS used the word only four times, while the current NSS uses it 45 times.[256] Consequently, the official doctrine of the U.S. military has shifted from a binary categorization of peace and war, to a more nuanced "competition continuum," in which there is, "enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict."[257]

If the concept of warfare has becomes antiquated to describe relations between states and—in the words of Professor Brooks—is, "no longer serving the purpose we want them to serve," then collective thinking about how nation-states use international law in their relations among one another should also evolve. The purpose of this chapter is to do just that: to shift the reader's thinking about the role of international law in relations between states to a concept, which was first proposed and is further refined in this chapter as "legal gamesmanship."[258]

First, this chapter will review several existing law-related concepts and examine shortcomings in those concepts. Second, this chapter will derive lessons learned from how other competitors in non-geopolitical contexts use rules to their advantage. Third, this chapter will define legal gamesmanship and explain its constituent elements. Fourth, this chapter will apply this definition and identify real-world examples of the People's Republic of China and the Russian Federation employing legal gamesmanship in their respective competition with the United States and other nation-states. Through this discussion, the reader will be empowered to recognize situations when nation-states employ legal gamesmanship, and consider appropriate and effective ways to counter such actions.

Existing Law-Related Concepts

Before discussing the concept of legal gamesmanship, we should first acknowledge several existing law-related concepts and thereafter reflect upon some of the inherent limitations and shortcomings of those concepts. These existing concepts include legal instrumentalism, lawfare, and legal warfare.

The first existing concept to consider is *legal instrumentalism*. This legal concept is foundational in nature to the idea of law itself. As law professor Brian Tamanaha concisely describes, "[a]n instrumental view of law means that law—encompassing legal rules, legal institutions, and legal processes—is consciously viewed by people and groups as a *tool* or *means*, with which to achieve *ends*."[259] This legal concept finds its origins in 19th century discourse on law, primarily domestic law. For example, English philosopher and jurist Jeremy Bentham described how legislators enact laws for, "coercive or penal motives," in order to shape the behavior of their governed population.[260] Over a century later, American political scientist Robert Keohane opined that international law can be viewed through either an "instrumentalist optic" or a "normative optic."[261] Yet the focus of Keohane's use of the "instrumentalist" label was not on legal instrumentalism, but rather on his instrumentalist theory of international relations—that is, explaining why and the extent to which nation-states conform their behavior to international law. Nonetheless, legal scholars have recognized that legal instrumentalism in the international law context is similar to that in the domestic law context. As American legal scholar Timothy Meyer observed, "[i]n legal practice, instrumentalism has been associated with an approach to international law that treats it as a means to achieve ends, rather than as embodying certain ends in itself."[262]

The second existing law-related concept to consider is *lawfare*. In the fall of 2001, soon after al Qaeda's terrorist attacks on 9/11, American military lawyer and legal scholar Charles Dunlap opened a speech at Harvard's Kennedy School of Government by asking the question, "[i]s lawfare turning warfare into unfair?"[263] Thereafter, he defined lawfare as, "a method of warfare where law is used a means of realizing a military objective." Eventually, he refined the definition of lawfare to be, "the strategy of using—or misusing—law as a substitute for traditional means to achieve an operational objective."[264] Over the subsequent two decades, Dunlap, along with a host of legal scholars and commentators, have spoken and written much about this concept of lawfare. They have applied it to real-world situations to analyze how state and non-state actors have employed "law as a weapon of war," including terrorist groups like al Qaeda, state-sponsors of terrorism like Afghanistan's Taliban regime, regional powers like Iraq and Yugoslavia, and eventually major powers like Russia and China.[265]

The third existing law-related concept to consider is *legal warfare*. It is similar to the academic concept of lawfare, but was adopted and developed officially by a nation-state, the People's Republic of China (PRC). The seed for this concept might have been planted in a 1996 speech by Jiang Zemin, then-PRC President and General Secretary of the Chinese Communist Party, to a Beijing meeting of Chinese international lawyers. He urged: "Our leaders and cadres, especially those of high rank, ought to take note of international law and enhance their skill in applying it...We must be adept at using international law as 'a weapon' to defend the interests of our state and maintain national pride."[266] Three years later, in the seminal book *Unrestricted Warfare*, two senior Chinese military officers described a variety of means that, "seem unrelated to war" but which, "will ultimately become the favored minions of this new type of war."[267] These means included trade warfare, financial warfare, new terror warfare, ecological warfare, psychological warfare, media warfare, network warfare, technological warfare, fabrication warfare, resources warfare, economic aid warfare, cultural warfare, and lastly but most notably for our purposes, "international law warfare."[268] Several years later, the Chinese government directed the political works of the PLA to include what it labelled as "legal warfare," without publicly defining what that concept would entail.[269] Thereafter, Chinese military scholars have developed this concept through a series of book-length treatments, including an analysis of 100 uses of legal warfare in world history.[270] There does not appear to be a unified Chinese definition of legal warfare, however, yet many of them refer to, "the use of law in warfare," "us[ing] law as the combat weapon," and, "us[ing] the law as its main method of struggle."[271]

Each of these three existing law-related concepts might have some value in framing and understanding the behavior of nation-states in their relations with other states, but they also have some inherent limitations or shortcomings. Specifically, legal instrumentalism is relatively general or universal in nature, but it does not necessarily frame the decisions and actions of nation-states in the special context of competition with other states, or what such a competitive environment might include. Furthermore, the root word in legal instrumentalism creates a false implication that nation-states can use international law only via the instrumental function of law, but nation-states can also use international law via the structural and normative functions of law. Additionally, both lawfare and legal warfare describe how states use law as a "weapon" even in situations when the actor-agent of the state is not the military, the actions are not hostile in nature, and the involved states are neither in nor near the status of armed conflict. Moreover, while the concept of lawfare might have originally been intended to be a neutral term to describe any state's use of the law (i.e., either "us" or "them"), it has gradually morphed into a pejorative characterization of something that only "the other side" (i.e., "them") does. Due to these limitations and shortcomings of existing law-related concepts, we must therefore consider whether there might be a more appropriate concept to frame the relationship of law to the behavior of nation-states in the broad range of interstate competition.

Competition and Gamesmanship

Competition is a reality of relations between nation-states.[272] Official U.S. military doctrine states: "Competition is a fundamental aspect of international relations. As states and non-state actors seek to protect and advance their own interests, they continually compete for diplomatic, economic, and strategic advantage."[273] As mentioned previously, this same doctrine publication shifted from a binary, mutually-exclusive world of peace and war, in which nation-states are either in cooperation or conflict with one another, to a more nuanced, trinary continuum of cooperation, competition, and conflict. The second element of this continuum, "competition below armed conflict," is described as follows:

> Situations in which joint forces take actions outside of armed conflict against a strategic actor in pursuit of policy objectives. These actions are typically nonviolent and conducted under greater legal or policy constraints than in armed conflict but can include violent action by the joint force or sponsorship of surrogates or proxies....Competition below armed conflict may include diplomatic

> and economic activities; political subversion; intelligence and counterintelligence activities; operations in cyberspace; and the information environment, military engagement activities, and other nonviolent activities to achieve mutually incompatible objectives, while seeking to avoid armed conflict. Within competition below armed conflict, joint force actions may include security cooperation activities, military information support activities, freedom of navigation exercises, and other nonviolent military engagement activities.[274]

In this nuanced environment, each state will, "apply the instruments of national power," in order to achieve their respective national objectives.[275] This can include the employment of diplomatic power, informational power, military power, and economic power—either standing-alone or in combination.

While U.S. military doctrine has been refined to include a trinary continuum of cooperation, competition, and conflict, the discussion of international law within the same doctrine remains binary. For example, a call-out box citing the U.S. Department of Defense *Law of War Manual*, includes only the legal definitions of international armed conflict, non-international armed conflict, mixed armed conflict, and internal armed conflict.[276] Further, it makes only two other references to law, including: (1) the "legal and institutional advantages of the peace/war binary model;" and (2) the way in which geopolitical rival states "employ a mixture of instruments of national power... in a manner calculated not to trigger our legal or institutional thresholds for armed conflict."[277] Beyond that, the refined U.S. military doctrine makes no reference to the role of law in the competition continuum, particularly none in the "competition below armed conflict" portion. Therefore, the role of law, particularly international law, is ripe for consideration and exploration within the geopolitical competition of nation-states.

Given the reality that the condition or status of armed conflict can still sometimes exist between nation-states, existing law-related concepts like lawfare and legal warfare might continue to be appropriate for describing and analyzing the decisions and actions of states involved in such conflicts. But, given another reality where international relations no longer involve only peace and war between states, should there not be a more precise law-related concept than lawfare and legal warfare for describing and analyzing the decisions and actions of states in the third portion of the continuum?

Where might we find lessons about the role of law in competition among nation-states? One option would be to examine real-world case studies derived from world

history. For example, U.S. military doctrine cites historical examples of the competitive relations between the United States and the Soviet Union during World War II and the "Great Game" of political and diplomatic confrontation between the British and Russian Empires in the nineteenth century.[278]

Alternatively, we could also look to other analogous situations—scenarios that also involve competition, albeit with different types of actors but similar types of actions. For that, we need look no further than the competition arising in organized sports and athletics. Such athletic competition arises more frequently, sometimes on a near daily basis, than nation-state conflict. It occurs openly and transparently, often visible on our television sets from a variety of camera angles and repeated through slow-motion replays. Yet the root agents, human beings, are the same in both international relations and athletic competition. Most notably, athletic competitions are governed by codified rules known to all competitors, implemented by governing bodies, and applied instantaneously by refereeing officials. For all these reasons, athletic competition can help us understand not just the roles of rules in competition but also how competitors can manipulate the rules in such competition.

Perhaps the best athletic competition for reflecting on this reality is the sport of football (also known as soccer in the United States), given its universal popularity around the world. Football has been described romantically as "the beautiful game."[279] Yet fans of this sport witness the recurrence of questionable behavior by players in the midst of competition, which are not necessarily beautiful. Consider these recurring examples:

- An offensive player for one team is dribbling the ball towards the opposing team's goal. This player enters what is known as the penalty area. A defensive player from the opposing team slides on the pitch towards the offensive player in an attempt to prevent the offensive player from taking a shot on goal. Physical contact between the two players occurs. The offensive player falls on the ground immediately, and then makes verbal sounds, facial expressions, and body language consistent with someone who is injured. The referee blows their whistle, calls a foul against the defending team, and awards a penalty kick for the offensive team. A player chosen by the offensive team takes the penalty kick and scores a goal, in a higher-percentage opportunity than scoring goals in the normal course of the game.
- An offensive player is dribbling the ball near the halfway line of the field of play. This player finds an opening in the formation of the defensive team

and accelerates their running to dribble through that opening. Due to the location of defensive players, the offensive player is likely to have a one-on-one scoring opportunity versus the defending team's goalkeeper. The closest defending player is able to close the distance with the offensive player from behind, slides on the ground into the offensive player, and intentionally trips the offensive player. The referee blows their whistle, calls a foul against the defending team, and presents a yellow card (caution) to the defending player. But the defending team has avoided the risk of a high-percentage scoring opportunity.

- In a match between two teams, one team has a one-goal lead against the other team in the final minutes of play. For every restart of play (e.g., throw-in after an out-of-bounds situation, free kick after a foul), the leading team's players do not outright delay the restart, but they also do not demonstrate a sense of urgency either. Additionally, the leading team's goalkeeper falls to the ground whenever he gathers the ball from a shot on goal by the trailing team—no matter whether the inertia of the shot forced the goalkeeper to fall. Each of these actions by the leading team consumes valuable seconds of time on the game clock, thereby preventing the trailing team from having additional opportunities to score a goal and tie the game.

What do all three situations have in common? In short, they involve agent-actors of an organization using the rules applicable to their competition in an intentional manner during a competitive event against the efforts of a rival organization in order to achieve an advantage. In none of these situations are the players actually cheating—that is, totally disregarding the applicable rules of the game. But in none of these situations are the players merely competing—that is, purely using their athletic skills in a manner superior to the opposing players. Instead, in each of the situations, the players are engaged in "gamesmanship," what has been previously described as "the art of winning without actually cheating."[280] In short, these athletic competitors are gaming the rules of the game.

Legal Gamesmanship

Athletes are not the only agents who game the rules in relation to others. So, too, do the official representatives of nation-states in their relations with other states. Given that the foundation has been laid about the analogous situation of gamesmanship in athletic competition, now would be the appropriate time to define and outline the concept of

legal gamesmanship in the context of international relations. Briefly, legal gamesmanship can be defined as *conduct by a nation-state, or that is otherwise attributable to a nation-state, that uses the structural, normative, or instrumental functions of international law in order to achieve that nation-state's objectives within a competitive environment*. Each element of this definition of legal gamesmanship warrants some further elaboration or explanation.

First, legal gamesmanship involves overt international conduct undertaken either by a particular nation-state or that is otherwise attributable to a particular nation-state.[281] Conduct can be acts, actions, and activities, including statements. It can also be either positive action or deliberate inaction, particularly in situations when a state might otherwise have an obligation to act. Whatever form of conduct it might be, it is international in nature. International relations are relations between nation-states, and international law is the body of law applicable to relations between nation-states.[282] Under the body of customary international law known as the law of state responsibility, nation-states are legally responsible for actions taken in relation to other states. In reality, a state is an inanimate concept, which, "cannot act of itself," thus any act of a state, "must involve some action or omission by a human being or group."[283] Under the legal theory of agency, the actions or omissions of a nation-state must be conducted by that state's representatives or its agents. As a matter of international law, conduct can be attributable to a nation-state if such conduct was undertaken by a state "organ," was "empowered by law," or was at the government's "instruction, direction, or control."[284] Therefore, actions can be planned and executed by a military organization or military personnel, by any other government organization or government personnel, or even by non-government organizations and personnel if they are empowered by the law of the nation-state or under that nation-state's instruction, direction, or control. This could include, for example, groups and individuals that are commonly described as proxies.

Second, legal gamesmanship involves activities that use international law. Typically, such use of law will involve either leveraging the law or exploiting the law. Leverage denotes actions that use a strength or advantage of the law that favors the acting nation-state. Exploitation denotes actions that use a weakness or disadvantage of the law that benefits the action nation-state.

Third, legal gamesmanship involves a nation-state's use of one or more of the three key functions of international law. One key function of international law is structural in nature. That is, specific elements of international law form the structure of the international system of relations between nation-states, such as the structure of the

United Nations and its organizations that was codified in the UN Charter. Another key function of international law is normative in nature. That is, international law includes rules of treaties and customary law that specify the norms of behavior between states deemed acceptable and unacceptable. A third key function of international law is instrumental in nature. That is, international law can serve as an instrument that arranges or facilitates relations between and among states, such as mutual security treaties and intelligence sharing agreements. Each of these three key functions of international law can be either leveraged or exploited by states engaged in legal gamesmanship.

Fourth, legal gamesmanship involves actions that either are intended to achieve the acting nation-state's objective or objectives, or are otherwise in furtherance of its objective or objectives. These objectives can advance one or more of the national interests of the acting state, such as its diplomatic interests, its informational interests, its military interests, or its economic interests. These objectives can affect efforts at the strategic (i.e., national or policy), operational (i.e., military), or tactical (i.e., local or short duration) levels of governance.[285]

Fifth, legal gamesmanship involves activities undertaken in direct or indirect competition between or among nation-states. In other words, actions undertaken in the otherwise competitive environment of international relations. As discussed previously, elements of relationships between states can involve cooperation, competition, and conflict. Cooperation involves situations when a state, "take actions with" another state or states in pursuit of common or complimentary policy objectives.[286] Armed conflict involves situations when a state, "takes actions against" another state or states in pursuit of diverging policy objectives, "in which law and policy permit the employment of armed force in ways commonly employed in declared war or hostilities."[287] In contrast to cooperation and conflict, "competition below armed conflict" involves situations when a state, "takes action against" another state or states in pursuit of diverging national interests, policy objectives, or desired outcomes.

Of note, the concept of legal gamesmanship can be more appropriate than the existing concepts of legal instrumentalism, lawfare, and legal warfare for multiple reasons. In contrast to legal instrumentalism, legal gamesmanship is not general in nature but rather is focused on capturing the behavior of nation-states of using law in the context of their geopolitical competition with one another. In contrast to lawfare and legal warfare, legal gamesmanship is not limited to military-related actions or situations. That is, it can capture actions by any government agency or non-government proxy (when their actions are attributable to a nation-state) and not merely actions by

military organizations. Additionally, legal gamesmanship can capture actions that are intended to achieve any national policy objectives and protect any national interests, including ones that are not military in nature. Legal gamesmanship can also capture actions occurring throughout the competition continuum, including actions in cooperation, competition below armed conflict, and in armed conflict. The concept of legal gamesmanship is not necessarily intended to supplant existing law-related concepts such as lawfare and legal warfare, but to subsume them. In short, lawfare and legal warfare are subsets of legal gamesmanship activities that are employed by nation-states in armed conflicts. Lastly, legal gamesmanship is a neutral and objective concept that recognizes and describes the competitive uses of law by any nation-state (i.e., either "us" or "them"). For these reasons, the concept of legal gamesmanship can provide a valuable shift of official and academic discourse away from the militaristic and potentially meaningless label of "warfare," which can disaffect non-military audiences, to a more appropriate and inclusive dialogue about the competition between nation-states and their use of international law in such competition.

Examples of Legal Gamesmanship

It would be impossible in this single chapter to catalogue all of the instances of when nation-states have engaged in legal gamesmanship in their relations with other states. Nevertheless, there is value in identifying and briefly analyzing a few examples of the practice of legal gamesmanship, both to validate the concept of legal gamesmanship and to aid readers in analyzing other potential or future situations that might also involve it. For such analysis of situations, one should consider several questions, including but not limited to: Which particular nation-state has engaged in the conduct or is legally responsible for the conduct? What body of international law and specific rules of international law has this state used in this particular instance? How specifically has this state used international law in this instance? For what purpose or objective was this state using international law in this manner? When this state used international law in this instance, which other state or states was involved in the competition? The answers to these questions for a particular situation will help determine whether legal gamesmanship has been employed.

Mindful of these analytical questions, consider the following examples of legal gamesmanship employed by China and Russia in recent years:

- China has engaged in legal gamesmanship in its competition with other East Asian claimant states, such as Japan, the Republic of Korea, the Republic of the Philippines, and Socialist Republic of Vietnam, through the way in

which it has created and deployed its maritime militia. Specifically, China has exploited the structural function of international law in which states are responsible for their actions in relation to other states.[288] On numerous occasions, China-flagged fishing vessels have engaged in unsafe behavior at sea during encounters with the Navy and Coast Guard vessels of other nation-states in the waters of the Yellow Sea, the East China Sea, and the South China Sea. When these incidents have occurred, Beijing has pushed a narrative that these were merely "patriotic Chinese fishermen," and they were not the official actions of the PRC government.[289] In recent years, however, experts have exposed documentation that prove many of these China-flagged fishing vessels were actually the PRC maritime militia, which is funded by and under the instruction, direction, and control of the PRC government.[290] By attempting to employ its maritime militia with plausible deniability, China intended to undermine the efforts of its neighbors to effectively control activities within their respective maritime zones coastal states, and strengthen maritime claims to some of these disputed areas.[291]

- Russia has engaged in legal gamesmanship in its competition with the United States, other members of the North Atlantic Treaty Organization (NATO), and several of its neighboring states (such as Ukraine) through the way in which it has voted at meetings of the UN Security Council. Specifically, Russia has leveraged the structural function of international law in which the five permanent members of the Security Council have veto authority on matters relating to maintenance of international peace and security.[292] On multiple occasions involving the security of Russia's neighbors, such as Georgia and Ukraine, Moscow has voted against draft Security Council resolutions that were aimed at addressing insecurity that it was either partially or entirely responsible for creating within the sovereign territory of those neighboring states.[293] By exercising its veto authority over these draft resolutions, Russia intended to prevent the international authorization of collective action by other states to protect smaller neighboring states and to preserve regional dominance.

- Russia has also engaged in legal gamesmanship in its competition with its neighboring states, such as Georgia and Ukraine, through its mass issuance of passports to residents of bordering sovereign states, coupled with a plan to send saboteurs to commit false-flag terrorist attacks.[294] Specifically, Russia has leveraged the normative function of international law, particularly the norm

that nation-states have the discretional authority to issue passports to selected persons and that nation-states have the right of self-defense, including the right to defend and protect their respective citizens and nationals.[295] Prior to the February 2022 invasion of Ukraine, the Russian government issued Russian passports to over 650,000 residents of eastern Ukraine.[296] When Russia then invaded Ukraine, President Vladimir Putin of Russia invoked the right of self-defense under Article 51 of the UN Charter and claimed that the purpose of the "operation" was to "defend Russia and our people."[297] By issuing these passports to Ukrainian residents, Russia sought to fabricate a legal basis to justify its invasion of another sovereign state and annex its territory.

- Both China and Russia have engaged in legal gamesmanship in their competition with other neighboring claimant states and with extra-regional powers, such as the United States, through the way in which they have asserted expansive maritime claims. Specifically, China and Russia have each leveraged the instrumental function of international law in which coastal states have the right to establish their maritime zones, and may adopt laws and regulations relating to these maritime zones. These national legal authorities, however, must "conform" to the rights and jurisdiction afforded to coastal states under the international law of the sea.[298] Disregarding this prerequisite, China and Russia have enacted national laws and regulations to assert some of the most comprehensive regimes of excessive maritime claims of any coastal states in the world.[299] When other nation-states transit and operate their military vessels and aircraft within China's maritime zones, Beijing responds by declaring publicly that these transits and operations violate international law and China's national laws. Such legal regimes by China and Russia are intended to deny other states lawful access to oceans and airspace and create a greater stand-off distance and defense-in-depth from land territory.

These are merely a few examples of these two states engaging in conduct that would satisfy all of the definitional elements of legal gamesmanship outlined above.

Conclusion

Given the reality that nation-states—including but not limited to China and Russia—engage in legal gamesmanship, what can other states do to respond to or to counter such conduct? There is no one-size-fits-all solution for addressing legal gamesmanship, but rather it would depend upon the particular facts and circumstances of the situation, and the specific way in which a state engages in legal gamesmanship. The

responding or countering actions of another state or other states can involve any of the instruments of national power, including diplomacy, information, military, economic, financial, intelligence, and law enforcement. Of note, some of these responding or countering actions can involve: law-related efforts, such as initiating a case before an international judicial body; indicting agent-actors and attributing their actions to a competitor-state; and legislating to require agent-actors who are engaged in political influence activities on the legislating state's sovereign territory to register or disclose their status as agents of a foreign government. Whatever responding or countering actions are considered, each state must ensure that its conduct conforms to international law... or else they could undermine the existing international rules-based order that they are seeking to uphold. At the same time, however, states should also recognize and have the political courage to invoke the existing limited bases under which states have the right to engage in actions that would otherwise violate their obligations under international law (e.g., the right of self-defense, countermeasures, reprisals, etc.), when another state like China or Russia first violates its obligations under international law.[300] Invoking these unpleasant but lawful exceptions, when appropriate, is also an essential means for nation-states to help preserve the international rules-based order. Ultimately, what matters most in this context is that nation-states recognize when other states are gaming the rules of international law to their advantage and that they employ effective measures to lawfully outcompete opposing states.

About the Author

Jonathan G. Odom is a licensed attorney in the U.S. Navy. Currently, he serves as the Military Professor of International Law at the George C. Marshall European Center for Security Studies (Germany). Previously, he served for four years as a Military Professor of Law and Maritime Security at the Daniel K. Inouye Asia-Pacific Center for Security Studies (Hawai'i). During his 27-year Naval career, he has provided legal and policy advice on matters involving international law and national security law to senior U.S. policy leaders, U.S. and multi-national military commanders, headquarters staffs, and deployed forces around the world for military operations at sea, in the air, on land,

and in cyberspace. Of note, his headquarters assignments have included serving as the Oceans Policy Advisor in the Office of the U.S. Secretary of Defense (Washington, DC) and as the Deputy Legal Advisor to Commander, U.S. Pacific Command (Hawai'i). His operational assignments have included deployments to sea in the Arabian Gulf, Indian Ocean, South China Sea, and East China Sea, and deployments ashore in Iraq, Kosovo, and Japan. He holds a Bachelor of Arts in History with Distinction from Duke University, a Juris Doctor from Wake Forest University, and a Master of Laws with Distinction from Georgetown University. The views expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of Defense, or any of its components.

Discussion Questions:

1. Has a nation-state been subject to legal gamesmanship activities by another state? If so, which nation-states were involved, which body of international law was used, which specific rules of international law were leveraged or exploited, how specifically was the law used, and what was the intended purpose or objective?

2. What specific measures, if any, has your government taken to counter legal gamesmanship by other states?

3. More generally, what do you think are the best ways for states to counter the use of legal gamesmanship?

4. To what extent can rule-of-law democracies cooperate to engage in legal gamesmanship?

Recommended Reading:

- Aurel Sari, "Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats," *Exeter Centre for International Law*, February 10, 2020.
- Jonathan G. Odom, "Understanding China's Legal Gamesmanship in the Rules-Based Global Order," in China's Global Influence, eds. Scott D. McDonald & Michael C. Burgoyne, October 1, 2019.
- Mark Voyger, "Waging Lawfare: Russia's Weaponization of International and Domestic Law", *Per Concordiam*, December 10, 2019.

How Russia, China, and Iran Weaponize Information for Internal Social Control and External Influence

Christopher Paul and Mike Schwille

ABSTRACT

The governments of Russia, China, and Iran weaponize information for two primary purposes: domestic social control and foreign malign influence. While domestic populations are their main audiences, all three exert domestic control, and seek to influence foreign mass audiences, in slightly different ways. Russia uses a combination of censorship and a, "firehose of falsehood" aimed at both domestic and foreign audiences to sow confusion and chaos. China uses tight digital authoritarianism, social surveillance, and physical control to keep their own population in line, as well as floods to create incentives to self-censorship among those who might raise opposing narratives abroad. Iran blends physical threat and coercion with a range of surveillance and propaganda activities at home and abroad. Because information plays an outsized role in strategic competition, the United States should be particularly concerned about these actors' weaponization of information, especially against external audiences.

Introduction

The history of using information as a weapon is as old as weapons themselves. Writing in the 5th century BCE, Sun Tzu noted that, "all warfare is based on deception." The

importance of having accurate situational awareness and the benefits from promoting poor situational awareness for enemies, through deception and ruses or through effective counter-reconnaissance, is a long-standing ingredient for success in war. The use of propaganda in war, mass information aimed at citizens and publics in adversary nations, dates back to ancient times. However, the weaponization of information during peacetime as part of strategic competition, in support of irregular warfare objectives or as a mechanism of domestic social control, has seen a dramatic increase since the turn of the century.[301] As information technology has proliferated, and become more accessible to more people, it has brought communities together, created new ones, and connected people in dramatic ways. However, it has also provided a powerful tool to autocrats, dictators, and malign, aggressive regimes.

The United States' various competitors and adversaries weaponize information in slightly different ways. For example, Russia's government heavily propagandizes its domestic audience *and* international audiences largely without regard for the truth. The People's Republic of China (PRC) seeks editorial control of information, preventing the generation and flow of stories or conversations opposed to Chinese Communist Party (CCP) interests inside China and abroad through censorship, bullying, and economic coercion. The PRC collects copious amounts of information on its own citizens at home and abroad, and uses that information to identify and punish those who share dissenting views. The Iranian government also uses a mix of censorship and internal repression to influence and control its citizens.

This chapter explores the ways in which the governments of Russia, China, and Iran weaponize information, the role such information plays in strategic competition and irregular warfare, and why weaponized information should be of concern to the United States. To summarize the chapter in six words: the truth does not always win.

Information in Great Power Confrontation

There is still considerable debate about the terms and definitions of great power confrontation, great power competition, gray zone conflict, or irregular warfare. While other chapters in this volume address these definitional challenges in greater detail, we will note some areas of consensus among them. First, there is a spectrum or continuum of competition and conflict. Second, thresholds are important in strategic competition, as crossing them can lead to escalation. Escalation is extremely consequential between nuclear-armed competitors. Third, ambiguity is an inherent characteristic of aggression in competition and irregular warfare, which complicates responses. Fourth, strategic

competition draws on all types of national power: diplomatic, information, military, and economic.[302]

What do these four consensus characteristics mean for the role of information in strategic competition? Participation at any point on the continuum of competition and conflict is fueled by information in the form of intelligence. Being able to understand the nature of the threat and being aware of and able to visualize likely competitor actions is a prerequisite for effective response. Detailed information about conditions, preferences, systems, and networks within a competitor nation or third country in which competition is unfolding is a prerequisite for effective action. That same sort of knowledge and understanding can help identify where a competitor's thresholds for response or escalation might be, to design actions that remain below those thresholds. Information for effect—that is, information for influence, persuasion, or control—rather than just information as intelligence is minimally provocative and unlikely to trigger extreme responses or escalation. Information is one lever of power that can be pulled with minimal risks of escalation at any point on the continuum of conflict. Finally, information can be both an antidote to, or the source of, ambiguity. Fighting for and against ambiguity, including efforts in reconnaissance and counter-reconnaissance, or intelligence and counterintelligence, are central to irregular warfare.

Moving beyond the struggle for information and sensemaking, there are a range of possible uses of information "for effect" as part of strategic competition. Adversaries and competitors use propaganda to widen divisions between different groups in a target society, or drive wedges between partners and allies. China, at least, hopes to "win without fighting" and might be able to do so if they are able to sufficiently undermine the cohesion of partners and allies, or reduce the national will to fight and will to resist of the United States.[303] Public opinion and public sentiment matters in a democracy whose principal allies are also democracies. If most Americans do not want to resist aggression by one of the nation's adversaries, it will be difficult for leaders to mobilize an effective response. Similarly, if there is a lack of public support among the citizens of needed partners and allies, their governments may be unable to meaningfully support resistance to aggression. With that in mind, U.S. information efforts in competition should counter the divisive messages of America's adversaries and work to promote the legitimacy of responses to aggression. In addition, they should foster and sustain positive relationships to increase the likelihood of foreign partners allowing U.S. forces to have the access, basing, or overflight rights necessary for power projection and to conduct operations in a crisis, contingency, or conflict. Deterrence is another key example of information for effect: successful deterrence relies on having

kinetic capabilities sufficient to prevent an aggressor from reaping positive gains from a proscribed action, demonstrating the commitment to using those capabilities, and on the potential adversary correctly perceiving both these capabilities and the willingness to use them, all of which depend on information.

The Weaponization of Information

Information matters in great power competition and irregular warfare in two ways: the fight *for* information, or gaining situational awareness, and preventing adversaries from having good situational awareness; and fighting *with* information, or using information for effect, to influence or persuade others, or to undermine or bolster the national will to fight of a nation's own citizens or those of other nations. The weaponization of information often only implicitly considers fighting *with* information, about governments selectively projecting (or denying) information to selected audiences, either domestically or internationally, in pursuit of policy objectives. For this discussion, we will focus on those targeted and the related purpose: is information being weaponized against a nation's own domestic population for purposes of social control, or is the information being weaponized against the citizens of foreign nations for the purpose of influence?

Human Psychology: Why Propaganda Works

Does information weaponized in the form of propaganda work? The answer depends on how one defines "work." Propaganda is not an all-powerful superweapon that has allowed one country to surpass or overwhelm another country without firing a shot. Propaganda can exacerbate pre-existing tensions within a population and, under certain circumstances, can be quite persuasive. The term "propaganda" needs examination to help one understand motivations and uses. In general terms, propaganda is the dissemination of facts, arguments, opinions, rumors, half-truths, and lies to sway public opinion. Contemporary discussions draw distinctions between types of propaganda to distinguish different combinations of intent and factuality. These include:

- *Misinformation*, which is false, inaccurate, or misleading information regardless of the intent to deceive, including the accidental dissemination of false information;
- *Disinformation*, which is deliberately created, distributed, and amplified false information with the express purpose to mislead;

- *Malinformation*, which is factual information distorted for the purpose of persuasion; and
- *Hate speech*, which is the use of discriminatory language referencing a person's group, religion, ethnicity, nationality, ability, sexual orientation or gender.[304]

There is a natural tendency to be skeptical about the effectiveness of propaganda, especially that based on falsehood. As virtuous people, most of us are inclined to impute effectiveness to virtuous approaches. We naturally assume that truthful persuasion is much more effective than falsehood-based persuasion. Unfortunately, that is not necessarily the case.[305]

Much propaganda, especially propaganda propagated by nations, relies on volume for effect. Research in social psychology supports a high-volume approach: quantity has a quality all its own. The number and frequency of messages received makes messages more persuasive, as does the presentation of similar arguments by multiple sources.[306] The persuasiveness of volume holds for accurate information, as well as for false and misleading information. Falsehood-based propaganda is often rapid and frequently repeated. Frequency leads to familiarity, which is strongly correlated with persuasiveness. Rapidity leads to first impressions that are consistent with the propaganda, and first impressions are notoriously hard to dislodge.[307] The property of being false is not in itself persuasive, but humans are poor judges of truth and falsehood. The contemporary information environment places enormous burdens on our cognitive processes, forcing us to use heuristics, or shortcuts, that are easily exploited by those who wish to deceive us.[308] We often use "peripheral cues" to make truth or falsehood judgements, so if a presenter is attractive, or a recording looks like a news broadcast, or if the information presented is consistent with our world view, we tend to make a quick unconscious determination to accept the information even if it happens to be totally false.[309] Once we have accepted false information, we tend to cling to it, reinforcing the power first impressions have.[310] Propaganda unrecognizable as such, and thoughtlessly disregarded, can change our accounts of certain events, and our views in general.

Using Information Against Your Own: Digital Authoritarianism and Social Control

Digital authoritarianism is the use of digital technology by authoritarian regimes to monitor, repress, intimidate, and influence domestic audiences. Authoritarians see information control as key to regime security and stability. Russia, China, and Iran each have a distinctive playbook for digital authoritarianism to maintain control over domestic

populations and to bolster other authoritarian regimes. Digital authoritarianism takes many forms, and uses multiple tools, but has the ultimate goal of keeping the regime in power. Russia, for example, successfully uses low-cost digital tools to rapidly spread disinformation domestically.[311] China uses high-tech social control measures that collect and leverage large amounts of data combined with advanced algorithms to create an advanced domestic surveillance system. Iran harnesses information coupled with a robust security apparatus to silence internal decent, propagandize its population and maintain regime control. While each country has its own system for maintaining control, all possess certain similarities in tactics and nature, including the following activities:

- *Censorship*, or the suppression of the free flow of ideas, and the prohibition of books, films, television (TV), and social media content which the government deems to be inappropriate or illegal (e.g., the Chinese "Great Firewall");
- *Domestic surveillance*, such as online and visual (digital or physical) monitoring of the population to include the use of sensors; closed-circuit TV (CCTV); automated systems; and human networks to track individuals, activities, and behaviors;
- *Flooding*, or using a large volume of propaganda to crowd out contrary viewpoints;
- *Ownership of digital and print media*, which is used to directly spread pro-regime information. A related effective way to silence a critical or independent media outlet is to buy them and shut them down;
- *Repressive legal regimes*, or using the legal system to intimidate companies and civil society into either supporting the regime or maintaining their silence;
- *Intimidation*, or using artificial intelligence (AI)-power bots and human networks, to coerce an individual or group;
- *Sovereign internet spaces*, involving legislation to control the free access to information, which includes the "sovereign Russian internet," and Chinese-controlled internet; and
- *Propaganda*, or biased and deliberately misleading information used to bolster a regime's image.[312]

These are just some of the ways that authoritarian regimes craft the information environment to suit their domestic needs, silence dissension, and maintain control.

Using Information Against Others

We now shift the discussion to the weaponization of information against the citizens of foreign nations for influence purposes. The first example of such an activity is the export of digital authoritarianism: selling tools and technologies used for domestic social control to other nations to better control and repress their own population. Exports of information-related technology is advantageous to the exporting country for a variety of reasons. First, the technology is sold, so there is a direct financial benefit. Second, providing such technology to another country often draws the importing regime into a closer relationship with the exporting government. Third, such transactions make the two governments and two countries more alike in their policies and approaches, also potentially aligning them in their foreign policy outlook. Finally, the exporter may well retain access to the data feeds associated with the technology, drawing even more information in to feed their algorithms, and allowing the exporter to track the presence and behavior of people in the importing nation.

Beyond the export of digital authoritarianism, the principal way in which American adversaries weaponize information is through internet-based propaganda. "Internet-based" as a category is quite broad. Propaganda can be propagated through social media, including platforms familiar to U.S. audiences such as Meta (Facebook), X, YouTube, Reddit, Pinterest, Instagram, Tumblr, and TikTok, as well as social media platforms more popular in other linguistic or geographic regions such as WeChat or Vkontakte.[313] In addition to direct posting and diffusing information via social media, digital authoritarians also participate in and spread propaganda through the comments sections on various websites. Propaganda can also originate and be spread through various encrypted or non-encrypted messaging applications, such as LINE, Telegram, WhatsApp, Facebook Messenger, Signal, or Vibr. Niche communities are another avenue by which propaganda can be spread, such as the communications platforms used by gamers to exchange information about or during games, such as Discord, Twitch, Xbox Live, or PlayStation Online. Propagandists also use traditional web pages, and web pages associated with state-run media, to spread weaponized information. These web pages can be optimized to pop up in search engines such as Google, Yahoo, and Bing, to increase their spread. In addition to internet-based propaganda, U.S. adversaries also spread weaponized information through news and televisions stations, some acknowledged to be state-owned and operated, and some more surreptitiously operated by their government. Other traditional media can support propaganda, such as graffiti or handbills. While still in use, both methods reach far narrower audiences than internet content. State-funded visits and exchanges that lavish gifts on journalists,

and expose them to carefully curated presentations of life in repressed areas, rounds out the modes commonly used by U.S. adversaries to selectively convey information to influence foreign audiences.

Adversary propagandists come in many forms. Most are some sort of paid agent of the state, though propaganda relies on viral spread through social media communities, through echoes and repetition by "useful idiots."[314] Some adversary nations also rely on patriotic volunteers to help spread their propaganda, pay small bounties to citizens who help promote state themes, or hire foreign mercenaries to propagate messages. State propagandists can be professional spokespersons, "journalists" on news programs, or paid trolls working in shifts with quotas for propagandistic posts or comments.[315] Many propagandists act under assumed cover identities or personas, and manage a large number of them, so that they can spread messages that appear to represent a broader range of perspectives. Some of these personas are custom built for propaganda purposes, while other are purchased or stolen accounts from real users.[316] Some inauthentic accounts lack the basic trappings of persona characteristics and are "bot" accounts, established by automated means, and following or rebroadcasting material under automated control. Propagandists also pay to have their content served to consumers as part of AdTech.[317]

What does information weaponized in the form of foreign propaganda look like? The information provided is almost always manipulated to be more appealing, convincing, or reaction-inducing. This might include:[318]

- *Fabrication*, in which part or all of the content is made up, false, or misleading (to include fabricated video, audio, still imagery, or memes, as well as text or documents);
- *Misappropriation*, or misrepresenting real events, people, or evidence in ways that lead to incorrect conclusions about what took place;
- *Deceptive identities*, through impersonation of either genuine sources of information (such as a specific scholar), a member of credible category (such as journalists, or a "witness" to events), or just a cover persona;
- *Obfuscation*, or seeking to cloud public discourse by offering multiple contradictory accounts of events;
- *Conspiracy theories*, such as proposing covert plots by shadowy organizations or cabals;
- *Selective use of facts*, or presenting factual information in a manipulative way, also known as "partial truth;"

- *Rhetorical fallacies*, including content appealing to flawed logic (whataboutism, false dilemma, slippery slope, false equivalency, straw man, etc.); and
- *Appeals to emotion or authority*, such as content intended to bypass audience reasoning and provoke a response.

Propagandists use these techniques for a range of purposes. These include: slandering other countries' officials, representatives, actions, policies, institutions, or culture; promoting other countries' actors, either because they are friendly to the propagandizing nation or because their actions are internally divisive; promoting the image and views of the propagandizing nation; stopping or drowning out views that contradict the propagandizing nation's preferred narrative; and deflecting or denying wrong-doing on the part of the propagandizing nation.

Russia Weaponizes Information in a Destructive Way

Russia has a long history of employing information warfare, with many concepts still in use today having their antecedents during the Cold War. Cornerstones of Russian military thinking about information include *maskirovka* (deception and obfuscation) and *reflexive control* (the notion of sharing information with someone to get them to do something specific while thinking it was their own choice or idea).[319] The Russian government uses weaponized information as propaganda across a wide range of media, including internet social media as well as traditional news media in print, television, and radio.[320] The Russian government seeks to control its domestic audience and silence internal dissent, as well as influence international audiences in support of their policy objectives. Its approach, however, is fundamentally destructive in nature. Rather than fostering goodwill toward Russia or its policies or seeking to build credible voices which can then promote friendly narratives, the Kremlin's propaganda seeks to discredit all sources of information. Consider the slogan on one of Russia's state-run international broadcasting efforts, RT (formerly Russia Today), whose slogan is "Question More." This nihilistic approach to information and its weaponization has been characterized by some as a "war *on* information," a desire to destroy trust and credibility for everyone and undermine any foundation for fact-based political discourse.[321] With a domestic audience numb and skeptical from years of falsehood-based internal propaganda, Russia would like to share this unhealthy skepticism of any information source with the world.

Characteristics of the Russian Approach

Russia seeks to promote distrust and fear through the targeted sharing of information. The Russian government wants its own citizens to fear imaginary threats from an aggressive NATO and other forces seeking to contain and constrain their country. In addition, the Russian government desires its opponents to fear what it might do, accede to its demands, and allow its aggressions to stand.

Russia's approach to propaganda has been likened to a "firehose of falsehood" with four distinguishing characteristics:[322]

- *High volume and multi-channel*, in numerous mediums and modes;
- *Rapid, continuous, and repetitive*, broadcast 24 hours a day with no delays for fact-checking;
- *No commitment to objective reality*, often broadcasting false or partially false content backed up with fabricated evidence, or presented by sources intended to seem credible, or are consistent with an audience's preexisting beliefs; and
- *No commitment to consistency*, with different Russian sources and voices presenting contradictory accounts of events, and sometimes even an individual speaker or channel contradicting themselves in a relatively short span of time.

Scholar Ben Nimmo has characterized Russian engagement in the information environment as following "4 D's": dismiss, distort, distract, and dismay.[323]

Target Audiences – Internal and External

The primary audience for Russian propaganda is its domestic one. For external audience propaganda, the Russian government prioritizes the countries closest (such as former Soviet republics), then those slightly further abroad (the remainder of eastern Europe, for example), then further still (the rest of Europe), and then on to the rest of the world (starting with transatlantic NATO members).

The focus of Russian propaganda employed toward the domestic population is generally favorable stories that promote narratives of a Western threat to the *rodina*. Inside of Russia, propaganda is spread through state-controlled media, which is basically all media. Russia controls external media through censorship, such as refusing to license or allow foreign broadcasting or access to domestic broadcast channels, and by imposing highly restrictive and arbitrary rules on foreign journalists attempting to operate in the country. Russian social control starts with propaganda, but ends with: heavy handed approaches to dissent, including censorship; denial of service and flooding attacks against critics; and mass arrests.

Russian international propaganda is disseminated through a wide range of media and channels. These include what purport to be news channels, such as *RT* and *Sputnik News*.[324] The media employed also include a substantial force of paid internet "trolls" who propagate Russian propaganda and attack or undermine views or information that runs counter to government-approved themes, doing so through internet chat rooms, discussion forums, and comments sections on news and other websites.[325] The Russian government's investment in engaging foreign audiences in their native language is particularly noteworthy. Russia's propaganda apparatus thoughtfully tailors content not just by language, but by region and culture. Russian propaganda considers a target country or region's culture, political history, religion, and is especially mindful of current events or divisions. It is much easier to sow chaos when targeting specific societal divisions rather than general ones.

Capabilities and Organizations

Russia invests considerably in its propaganda apparatus. *RT* has a budget of over $300 million per year, broadcasting in English, French, German, Spanish, Russian, and several Eastern European languages.[326] The channel is particularly popular online, where it claims over a billion page views; if true, *RT* would be the most-accessed news source on the internet.[327] According to a former Russian-paid internet troll, they are on duty 24 hours a day and, in a 12-hour shift, each individual has a quota of 135 posted comments of at least 200 characters.[328] Between acknowledged state-run media and paid Russian trolls, there are a range of government aligned media sources that are either state-funded but not acknowledged, or are proxies paid either by the government or by government-aligned kleptocrats.[329]

Details on the structure, organization, and location of information warfare capabilities within the Russian military are not publicly available, but there are reports of whole formations specializing in information warfare.[330] A range of Russian governmental entities play, at the very least, a supporting role in information warfare: the intelligence services, the legal apparatus, the military, and the Russian security council.[331] Russian internal security, the Federal Security Service or FSB, oversees internal social control and is responsible for internal surveillance and repression.

China's Reputation Management and Control[332]

Internally, the PRC has built systems and processes to control data, manipulate their citizens, and maintain CCP control. Globally, they are in the business of exporting authoritarian control products and systems and promoting the image of a strong

China. The main goal of the party is to stay in power, with control of information a central tenet in their efforts to accomplish this task. This includes access to information, the flow of information, and ability to present information in a manner that puts the CCP in a favorable light. Multiple organizations and entities are used to accomplish this, including government and military organizations, non-governmental and private society organizations, and quasi-governmental groups. They are part of an all-of society approach that does not distinguish between government organizations, civil society, or private business. All are useful in enacting the will of the party.[333]

Characteristics of the Chinese Approach

When it seized power in 1949, the CCP instituted the use of propaganda and censorship. The Tiananmen Square protests in the early 1990s reinforced the need for control as CCP leaders realized that free and open access to information via the internet could lead to dangerous outcomes. To increase CCP control, the party relies on information control through a steady state-sponsored diet of propaganda and information collection, censorship, and societal control measures. The CCP pushes propaganda through both traditional and emerging technologies. Where once radio, print media, and television were the primary vectors, everything connected to the internet is now being used to influence Chinese citizens in an increasingly digital state. This includes collecting virtual mountains of data on citizens monitoring what they do, where they go, and what they think. Data is collected through pay transactions, CCTV, wireless sensors, and the extensive use of facial recognition software that is then coupled with increasingly advanced Artificial Intelligence (AI) and Machine Learning (ML) tools to identify potential areas of concern within the population.[334]

Surveillance and physical control over some populations have also been effective methods of control. It is characterized by the large-scale use of public monitoring: through a network of informants, the use of autonomous sensors, a reliance on the population to report on other citizens, and limiting the movement of populations. Such monitoring is one of the ways that the CCP was so effective at keeping their population locked down for nearly three years during the COVID pandemic.[335] The large amount of data available to CCP authorities, when coupled with physical control methods, provides the ability to micro-target individuals for intimidation, coercion, and manipulation.

Another part of the state's control apparatus is the social credit system, which the CCP has been refining for years.[336] This system incentivizes behaviors that are deemed to be positive for the state, while disincentivizing actions deemed to be negative through

a unified "score" that members of an individual's social network can affect. While these efforts are not yet standardized across China, there are many variations of this systems already being implemented.

Target Audiences – Internal and External

China wants to control all its population, including those outside mainland China. In general, there are three categories of population that are relevant: the majority Han, domestic minority groups such as the Uyghur and Tibetans, and the Chinese diaspora communities living abroad. Efforts vary by group, with more physical control aspects being implemented in the autonomous zones of Xinjian and Tibet, places with the largest population of the minority groups mentioned.

External audiences also include three groups: populations in China's near abroad; countries to which China wants to sell its surveillance equipment; and global audiences which include Western democracies, international organizations, and countries and governments the CCP wants to influence.

Capabilities and Organizations

There is a virtual army of personnel dedicated to the collection and use of information for control purposes. Organizations focused on internal control include the Ministry of Information Technology, the Ministry of Public Security, and the Ministry of State Security. As mentioned, China uses a whole of government approach to information control with many efforts blending together. Diplomatic organizations include the Ministry of Foreign Affairs and the use of "wolf warrior" diplomats. The information element of national power relies on the use of state-owned media and television companies, including a large apparatus to censor the internet, print media, radio, television and social media. China is also known for its "50-cent army," which floods social media and content boards with pro-regime messaging, or uses benign comments to drown out critical comments.[337] The military primarily focuses on external control includes the People's Liberation Army, specifically the intelligence and cyber organizations, the Strategic Support Force, and the United Front. Economically, China relies heavily on its Belt and Road Initiative to push cheap economic loans to countries for large infrastructure projects, which are then leveraged to debt-trap the target. The CCP also leverages Chinese companies to provide foundational data and internet functionality, a plethora of digital surveillance and facial recognition technologies, and advanced artificial intelligence and machine learning technologies and services.

Bolstering the Iranian Regime through Information

Iran focuses on strategic persuasion to gain and maintain influence. It has two overarching objectives: to promote the regime and Iranian culture through a campaign of strategic persuasion to both internal and external audiences, and to undermine the resiliency of external audiences and governmental organizations.[338] Since before the 1979 revolution, Iran has used information and perception control as a means to an end. During the times of the Shah, Iran used posters, recordings, and propaganda to persuade internal audiences. After the 1979 revolution, the Islamic Republic adopted these methods to ensure the survival of the regime.[339] As with the CCP, the Iranian regime is primarily focused on regime survival. Its primary threat ultimately emanates from the Iranian people. Regional audiences and primary targets include Syria, Yemen, Afghanistan, Iraq, the Gulf states, Lebanon, Saudi Arabia, and other countries in the Middle East and North Africa (MENA).[340] Iran also targets global audiences as well as those its religious leaders deem to be primary adversaries: the United States and Israel.

Characteristics of Iranian Approach

Iran leverages public diplomacy, strategic communications, and cyber efforts as part of its well-established doctrine of non-military warfare.[341] The regime uses this approach because it lacks the military power to completely destroy its perceived enemies. To do this, Iran often combines military activities and threats, along with a sustained information campaign to emphasize its perceived successes. Such successes include combatting the West and supporting multiple resistance organizations.[342] Iran often leverages its offensive cyber capabilities to suppress social and political activity, and to intimidate regional and international adversaries. The tactics they employ include website defacement, the use of trolls and bots to flood social media, spear phishing, distributed denial-of-service attacks, and theft of personally identifiable information to target individuals and organizations in a concerted influence campaign.[343]

The U.S. intelligence community and various private sector threat organizations have identified Iran's Islamic Revolutionary Guard Corps (IRGC) as a driving force behind the country's state-sponsored cyberattacks and disinformation efforts, either through IRGC contractors in the Iranian private sector or through IRGC units. According to the U.S. Office of the Director of National Intelligence Annual Threat Assessment (2021), "Iran's expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US and allied networks and data." The assessment adds that, "Iran has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities."[344]

Target Audiences – Internal and External

Iran has three primary categories of targets for its weaponized information: internal audiences; countries in its near abroad, including the Middle East and MENA; and the United States and Israel. Internal audiences are saturated with propaganda coupled with internal security supervision and repression. Online content is blocked or filtered and those that the regime deems to be dissidents can be arbitrarily arrested and imprisoned. Iran takes a more nuanced approach to messaging and influence operations in its near abroad. These efforts range from purchasing and promoting television and news shows, the use of financial aid, and overt and covert military operations coupled with strong influence campaigns. For U.S. audiences, Iran's most frequently employed method of influence is persuasion, rather than division. Unlike Russia, which seeks to sow mass confusion and have Americans turn on each other, Iran seeks to persuade audiences and often attacks the U.S. government more directly.[345] Recent examples, however, highlight that Iran is not above attempting to cause friction by promoting multiple sides of an argument.[346]

Capabilities and Organizations

Iran utilizes its intelligence and security apparatus along with subsidiary organizations to conduct influence operations. Its use of bots and trolls on fake websites and social media is prolific. Iran also leverages public diplomacy through traditional state-run media. In countries where the population is more likely to get their information from the television, Iran has invested in television stations and broadcast capabilities. It has *Al-Alam* for MENA region, *Hispan TV* in Latin America, and *Press TV* for English-speaking audiences. Iran also funds a network of inauthentic news outlets which have typically hidden their link to the regime. The Iranian use of cyber-attacks and influence operations, conducted by proxy forces and private citizens, is a frequently employed capability which provides the regime a level of plausible deniability.

What Can We Do About Weaponized Information?

Social science research suggests numerous ways influence operations can be counteracted.[347] To counteract the export of digital authoritarianism, democracies will need to develop a robust model of digital governance that can effectively compete against the authoritarian model. Doing so requires strong institutions with the ability to punish states that do not play by the rules, as well as export controls placed on technologies that China, Russia and Iran do not yet possess. Efforts for slowing the spread of digital

authoritarianism could also include targeted sanctions on those individuals, companies, and countries responsible for spreading the technology without proper safeguards and the creation of global norms for digital governance.

There are a host of techniques to counter propaganda including: mapping narrative campaigns; fact checking; attributing, or "naming and shaming;" and platform notification. [344] Ultimately, resources need to be dedicated to the problem of combating weaponized information. Such resources include personnel trained to understand and engage, organizations that have the mission to respond, and the tools and capabilities to engage. Currently, responsibilities to combat weaponized information are spread across federal, state, and local governments; the Departments of Homeland Security, Defense, and State; civil society organizations; technology platforms, and, last and perhaps most importantly, individual citizens. Education and understanding of the nature of the threat digital authoritarianism and propaganda pose to the U.S. government, private companies, and private citizens is key to developing the resiliency needed to confront them.

Access to accurate information for one's own purposes and denial of information to adversaries is a critical element to warfare. Russia, China, and Iran are actively engaged in controlling their own populations and exporting methods to control and influence those in other countries. While using different methods, they share a common ultimate goal: regime control. With a better understanding of these challenges and by building up capabilities, personnel, and institutions to confront adversaries in this space, democracies can start to stop the spread of digital authoritarianism and help inoculate their own populations from the threat of propaganda.

About the Authors

Dr. Christopher Paul is the inaugural LtCol Kevin Shea USMC Chair for Information at Naval Postgraduate School. Prior to joining the NPS faculty in August of 2023, Paul worked at the RAND Corporation for more than 20 years. During his time at RAND, he provided research support related to operations in the information environment, information warfare, the information joint/warfighting function,

counterpropaganda, cyber operations, and related policy to a range of Department of Defense and U.S. Government offices, organizations, and commands. His work has influenced defense doctrine and policy in the United States and internationally. Paul completed his Ph.D., M.A., and B.A. in sociology at the University of California, Los Angeles, in 2001.

Mike Schwille is a Full Political Scientist at RAND. He is also qualified as a Civil Affairs, Psychological Operations, and Information Operations officer currently serving as the battalion commander of the 15th Psychological Operations Battalion (Army Reserve). He has deployed multiple times with the U.S. Army to the Middle East and Africa and has worked at numerous military commands. He earned his B.A. from the University of Pittsburgh and M.A. in international development studies from George Washington University. His primary research interest focuses on the integration of information into combined arms warfare. He has experience with Joint, Army, and Marine Corps concept development, operations in the information environment, countering anti-access/area denial (A2AD) strategies, strategic workforce analysis, and force development.

Discussion Questions:

1. What does it mean for information to be weaponized?
2. How can control of the flow and content of information lead to the control of citizens?
3. What does "digital authoritarianism" mean?
4. How do the regimes in Russia, China, and Iran differ in their approaches to the use of information?
5. Which aspects of weaponized information should be most concerning to American citizens? To the U.S. Government?

Recommended Reading:

- Christopher Paul, Michael Schwille, Michael Vasseur, Elizabeth M. Bartels, and Ryan Bauer, *The Role of Information in U.S. Concepts for Strategic Competition*. Santa Monica, CA: RAND Corporation, 2022.

- Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*. Santa Monica, CA: RAND Corporation, 2018.
- Christopher Paul, James Dobbins, Scott W. Harold, Howard J. Shatz, Rand Waltzman, and Lauren Skrabala, *A Guide to Extreme Competition with China*. Santa Monica, CA: RAND Corporation, 2021.

Russia and Ukraine: Three Lessons in Economic Warfare

James R. Sullivan, Parsley Ong, and Greg Rattray

IT'S THE ECONOMY...

The United States Department of Defense defines irregular warfare as a "struggle to influence populations and affect legitimacy."[348] This definition goes on to list five core missions and six enabling activities, none of which detail economic warfare, while at the same time recognizing adversary use of economic coercion. Kevin Bilms has argued that this definition of irregular warfare has created an "image problem" where the term is alternatively associated with either elite units blowing things up, or "little green men."[349] This chapter suggests that the image problem is even deeper, residing in its refusal to include whole-of-society strategic responses inclusive of economic warfare.

This omission occurs despite the rich history that economic warfare strategies have occupied historically in inter-state competition, ranging from Athenian blockades triggered by the Megarian Decree, to the British creation of an economic warfare "blade, newly forged, masterfully tempered, and believed lethal" to confront World War I-era Germany, to American plans to bankrupt Japan to prevent World War II.[350]

Moreover, specific historical tactics might find present day parallels. In the 1500s, England and other nations issued "letters of marque" to privately owned ships to attack and harass adversaries to inflict economic harm, in an interesting precursor to the nation-state use of private actors for similar purposes in the cyber realm, such as hackers-for-hire or troll farms. Eighth century South Asian and Middle Eastern *hawala* (money transfer) networks can be seen as precursors to current methods to sidestep the global financial system such as blockchain technologies and cryptocurrencies. The old adage about history rhyming, if not repeating, seems apropos here.[351]

The Department of Defense's omission of economic warfare from its definition of irregular warfare occurs as the world re-enters a multi-polar environment with challenges to the United States' economic hegemony and to the international rules-based system. Chinese leaders have discussed "changes not seen in a century" in creating a requirement for their nation to take a more active role in global affairs due to a more "balanced international system."[352] President Xi Jinping's October 2017 speech to the 19th National Party Congress argued China's economic growth, "offers a new option for other countries and nations who want to speed up their development while preserving their independence," explicitly linking economic strength to sovereignty.[353] United States President Donald Trump struck similar tones that same year, linking U.S. economic prosperity to both American leadership and security.[354]

A country's economy is core to its ability to provide a better life for its people, maintain critical social services, and ultimately to create the means for war.[355] The criticality of economics to nation-state competition should therefore not be in question. That said, there remains a stream of questions on the relationship between economics and warfare requiring further debate and analysis, which this chapter will attempt to illuminate. The chapter begins with a discussion on the current state of affairs regarding American economic warfare tactics and strategies. It then provides case studies examining the use of economic tools in the current Russia-Ukraine crisis, with a focus on the specific sectors of finance, energy, and the cyber-economy. This analysis illustrates what has worked and what has not, with recommendations for future implementations.

This chapter highlights three overarching lessons. First, economic measures deployed must have a clear definition of not only success—meaning what specific goals the measures are designed to accomplish—but also a timeline for these accomplishments. Often, economic warfare measures sacrifice a degree of short-term impact in order to maintain a coalition of partner nations, as will be seen in the section below regarding energy related sanctions. Tradeoffs between short-term efficacy and long-term coalition

cohesion should be made clear upfront to avoid confusion and the potential loss of support when implementation is *designed* to take time, as this chapter will show. Second, most of these measures extensively leverage private sector actors, such as banks, oil companies, and cybersecurity firms. This leverage must be both intentional and coordinated with government actors to achieve maximum efficacy. Third, many measures will require defensive tactics as well as offensive tactics. In many instances, current planning and discussion focuses only on offensive tactics.

This analysis suggests areas of incremental research in this field, including the critical question of how *far* to pursue tactics designed to weaken an adversary's economy. Despite current skepticism, empirical research has shown a positive correlation between economic integration and a country's democracy score.[356] There is also evidence that weakened economies can drive conflict through multiple channels. In an unsettling nod to popular films such as "Wag the Dog," research has shown that the odds of a conflict being escalated during a presidential election year *with* a weak economy is 60 percent, double that during a non-presidential election year and/or a strong economy.[357] An additional potential driver of conflict is a weakened economy in a society in which the government has staked its legitimacy on a combination of economic development and nationalism.[358] A relevant contention from the field of ontological security studies is that states seek identity security as well as physical security.[359] An economically-impaired opponent may begin to reinforce identity security by emphasizing a nationalism which looks to reverse perceived attempts by outside powers to subjugate the country.[360] A cornered adversary is a dangerous adversary, and the application of economic tools can perhaps be taken too far.[361]

The State of Sanctions

Academics like Nicholas Mulder, along with current and former government officials such as Agathe Demarais, represent a rising chorus of voices arguing that while sanctions, "fill the void between empty diplomatic declarations and deadly military interventions," their overuse means that "the golden days of U.S. sanctions may soon be over."[362] In fact, sanctions use increased 933 percent from 2000-2021.[363] Other commentators, including Council on Foreign Relations President Richard Haass, have suggested that despite the rapid expansion of the economic tool chest, "all too often sanctions turn out to be little more than expressions of U.S. preference that hurt American interests without changing the target's behavior for the better."[364]

These arguments ignore both the significant evolution of the financial and economic tools deployed, particularly in the post-9/11 era, as well as their effectiveness in bringing parties such as Iran and North Korea to the negotiating table.[365] The case studies below will attempt to illustrate this effectiveness, as well as limits to it that policy makers should seek to address.

These impediments include:

- Lack of clarity regarding the trade-off between short term sanctions effectiveness and the ability to hold a coalition together. The sanctions levied on Moscow after its invasion of Ukraine, for example, were never designed to bring the Russian economy to its knees in the short-term, given the criticality of energy market stability to coalition stability;
- Lack of coordination between private sector and government entities, which is particularly clear in the cyber realm;
- An excessive focus on offensive versus defensive strategies, meaning the ratio of strategies designed to harm or inhibit the Russian economy to those designed to strengthen the Ukrainian economy.

The Russia Case Study

The sanctions regime currently levied against Russia (the 11th-largest economy in the world) is the most comprehensive since the 1930s, when 52 of the roughly 60 sovereign states at the time sanctioned Italy, then the eighth-largest economy.[366] At the time Italy was running a significant current account deficit, meaning that it imported more than it exported (and that some of its exports likely relied on imported content for production). This required it to run a capital account surplus (i.e., inflows of foreign capital and investment) to fund this current account deficit. These critical liabilities (a reliance on both exports of goods and imports of capital) allowed League of Nations organized sanctions to inflict a significant toll on the Italian economy, given the ability to constrain inputs to production and throttle access to the required foreign capital. This drove exports down 47 percent and industrial production down 21 percent from 1935-1936, even though the largest and third-largest economies in the world (non-League of Nations members the United States and Germany) did not participate.[367]

There are early signs of similar, if narrower, impacts on production in Russia today with 60-80 percent reductions in specialized manufacturing dependent on Western imports (particularly technology) such as locomotives, refrigerators, internal

combustion engines, and freight cars.[368] Others estimate that more than one-quarter of Russia's aircraft will be unsafe to fly by 2025 due to a lack of spare parts and a reduced ability to perform basic maintenance.[369]

United States Deputy Secretary of the Treasury Wally Adeyemo notes that the sanctions applied to Russia are similarly multilateral in nature to those deployed against Italy, launched with more than 30 partners.[370] These partners include the entire European Union, the United States, Japan, South Korea, and Singapore, among others, which together represent approximately 70 percent of global GDP.[371]

Current sanctions deployed against Russia have been structured around three main limitations, according to Adeyemo.

First, these sanctions had to address a clearly-articulated foreign policy goal, in this case the degradation of Russia's ability to wage war. Three core pillars of the Russian economy were targeted: its financial system, the wealth and assets of its oligarchs, and its military-industrial complex (with over 700 companies and more than 2 million employees forming a backbone of political support for President Putin).[372]

Second, they had to be implemented by the broadest coalition possible.

Third, proper cost-benefit had to be conducted relative to potential options other than sanctions, such as military and covert action, public and private diplomacy, among others.[373] This analysis needed to include the potential tradeoffs between short-term effectiveness and efforts undertaken to broaden the coalition adopting sanctions. One historical example is the Oil for Food program, initiated for Iraq in 1995 in response to criticism that sanctions against Saddam Hussein's regime were unduly harming civilians. Although implemented to keep a broader sanctions coalition in place, this occurred at the cost of allowing the Hussein regime greater opportunities to evade financial controls, in a potential precursor of current efforts to create a two-tier market for Russian oil, as will be seen below.[374]

The sections to follow will show how these lessons play out across three specific areas of the Russian and Ukrainian economies, namely their financial markets, energy markets, and cyber-economies.[375]

Financial Market Sanctions and Tactics

As previously noted, the current financial market sanctions leveled against Russia are the most comprehensive since the 1930s. These sanction packages continue to evolve and expand, but currently include: import and export restrictions; the termination of Russian

bank access to the Society for Worldwide Interbank Financial Telecommunication (SWIFT, the global messaging system underpinning interbank money transfers); and seizures of assets from the Russian central bank and government, along with seizures of personal assets of officials.[376] The private sector, largely financial services firms, have implemented the majority of these actions after government encouragement.

Unlike 1930s Italy, however, Russia is a large energy exporter, thus increasing the global impact of the current sanctions regime and complicating implementation. High energy prices for much of 2022 led to a record current account surplus for Russia, a 3.4-fold increase over the prior year.[377] This significantly dampened the impact of Western economic tools targeting Russia (particularly relative to 1930s current account deficit Italy) and buttressed the value of the ruble, which initially crashed 90 percent on sanction implementation but quickly recovered to levels almost 20 percent stronger than before the sanctions.

This chapter argues that the chorus of pundits and academics proclaiming the failure of the current financial market sanctions regime suffer from one primary error, in that their definition of success is not cognizant of the inherent tradeoffs between the achievement of the goals of the sanctions regime, and the steps necessary to maintain the implementing coalition long enough to achieve them.[378] The goal of this sanctions regime is to degrade Russia's capacity to sustain the war in Ukraine. The timing of achievement of this goal will, however, in many instances conflict with the need to achieve implementation by the widest coalition possible. The sanctions regime was specifically constructed to reduce Russia's capacity for war, but at the same time also reduce the impact on global energy markets given the presence of large oil and gas importers in the coalition, a topic that will be explored in more detail in the next section. Allowance of oil and gas exports precluded the repetition of the current account deficit which made the sanctions on Italy in the 1930's so effective.

Declaring the failure of sanctions which were designed to allow capital inflows from their inception (to maintain the broader coalition) because they did not immediately stop capital inflows is illogical. Similarly, the "failure" of the ruble to collapse ignores the fact that the sanctions were designed allowed inbound capital. An immediate catastrophic stoppage of the Russian economy was never the goal.

The overall package of sanctions is, however, forecast to preclude any real economic growth in Russia for years to come, due to the significant impact on capital flows, productivity, and labor. Capital flows have been constrained, even if not stopped, by implemented investment restrictions, with the Atlantic Council estimating that Russia

has lost more than US$648bn in foreign direct investment (representing 34 percent of 2019 GDP) through 2020 (more recent statistics are unreliable), removing foreign capital, expertise, and knowledge.[379] Productivity measures have been depressed for years, and lack of access to almost any advanced technology from the West will not help. Directly linking loss of access to advanced technologies to productivity is a critical piece of incremental analysis in light of the growing prominence of technology restrictions placed on other global powers inclusive of the People's Republic of China (PRC). Labor has been negatively impacted both directly and indirectly, as declining macroeconomic prospects drove more than nine hundred thousand Russians offshore, many of whom are centered in high technology and high productivity businesses. Added to this are battlefield casualties, currently estimated at approximately 300,000 and counting.[380] The recent mobilization of an additional 300,000 troops have also removed them from the Russian labor force.

None of these factors are expected to rebound, leaving Russia stuck in time and losing ground in an evolving world. This zero-growth environment will also see a significant and growing percentage of Russian economic activity devoted to replacing used or destroyed war materiel, a remarkably unproductive form of economic activity (i.e., the broken windows fallacy) which will set the country further behind.[381]

One area of fault that can perhaps be levied on existing financial market policies is the lack of defensively-oriented policies. If sanctions, trade bans, and asset seizures represent *offensive* tactics, then efforts to shore up the financial markets and overall economy of the state under attack are *defensive* tactics, and just as critical. Russia, a US$1.8 trillion-sized economy, has indeed been stopped in its tracks, but only fallen 3 percent. Meanwhile Ukraine, a US$200 billion-sized economy, has lost at least 33 percent of its productive capacity. Investments across the board to shore up the Ukrainian economy are as important as offensive economic measures deployed against Russia. This will require significant planning from many parties to implement. However, there is little sign this has begun.[382]

Financial market policies therefore illustrate this chapter's three key take-aways. First, the definition of success must be made clear and consistent with the structure of a sanctions regime to enable public understanding and support. The trade-offs that exist between goals, such as the timeliness of impact versus sustaining a broad implementing coalition, should be made clear. Second, private sector participation is critical. In this instance, processes involving large banks and financial services companies were well-established through frequent use of sanctions regimes, particularly in the post-9/11 era, which allowed for efficient execution. Third, there is both an offensive as well as

a defensive component to most sanctions policies. *Both* must be considered, as well as implemented.

Energy Sanctions and Tactics

Energy sector sanctions perhaps most clearly illustrate the complexity of balancing short-term impact (restraining Russia's ability to pursue the war) with coalition cohesion (driven by the requirement to mute energy price volatility to enable more countries to participate in sanctions). The following section will expand on the significant complexity involved in this balancing act, given the experience of the first major conflict between oil producers and consumers. It will also show how energy sector sanctions provide strong evidence for this chapter's two other lessons: the importance of private sector actors and the need for both defensive as well as offensive strategies.

The Russia-Ukraine conflict has been the largest shock to global energy markets since the 1970s. It is unique as it represented the first major economic battle between oil consumers and oil producers, with the Group of 7 (G7) and European Union countries representing 38 percent of global oil consumption, while Russia represented 12 percent of global oil supply.[383] Throughout history, other major oil-related economic battles have largely occurred between energy producers. These included the Saudi-Russian price wars of 1986 and 2020, as well as the competition for market share between Saudi Arabia and the U.S. shale industry in 2015.

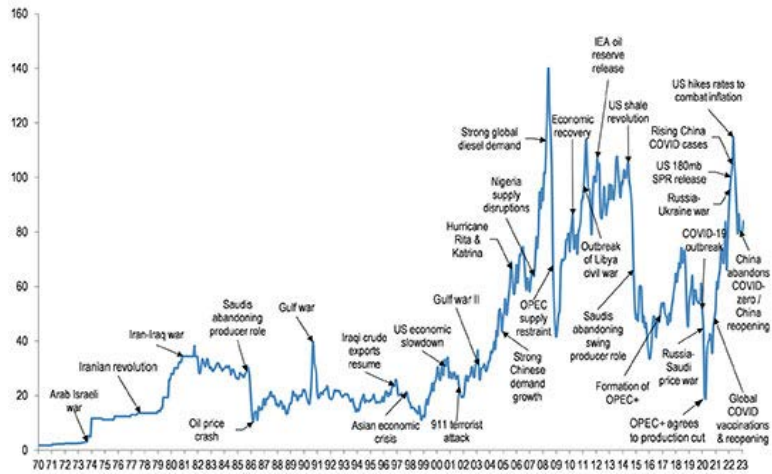

Figure 1. A lesson in oil history: Major events in the oil market from 1970s to present

The economic impact of conflict among oil producers since the 1970s was sharply felt in the form of short duration oil price collapses, painful for some but beneficial for energy-importing nations. The effects of the current economic conflict between oil consumers (EU/G7 nations) and an oil producer (Russia), however, is far more likely to drive significant spikes in energy prices that can prove damaging to energy importers globally.[384] Analysts estimate that a total removal of Russian oil exports from the market by the current round of sanctions would drive global oil prices as high as $380 per barrel.[385] This would trigger severe economic stress, if not outright collapse, for many oil-importing countries around the world. Oil prices that high would also allow Russia to achieve supranormal profits on any oil that successfully evaded sanctions. The sanctions regime was thus forced to balance curtailing overall Russian economic activity while also avoiding undue volatility in global energy markets. The sanctions regime therefore included mechanisms to allow some Russian oil sales in order to maintain coalition cohesion.

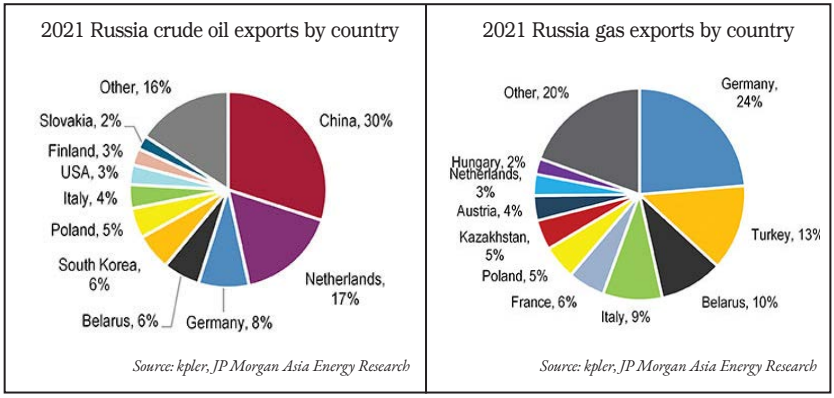

Figure 2. Russian Oil and Gas Exports

The following table outlines the major policies implemented to inhibit Russia's ability to fund its war chest using oil sales. These included: the exit of major international oil companies from Russia; a ban on G7 and EU nations from purchasing Russian energy and providing oil transport, financing, and insurance services; and a price cap on oil sold to countries outside of the G7 and EU bloc of nations.[386] Prior to the sanctions, Russia produced roughly 11 million barrels per day of crude oil and condensate, of which roughly 5.5 million barrels per day were used for domestic refining, and about 1 million barrels per day were exported via pipeline, with the remainder being seaborne crude oil exports. Of these seaborne exports, G7/EU regions received roughly 50 percent, falling to zero when the sanctions kicked in. As such, these Russian barrels had

to find a new home. The majority ended up re-routed to India, processed by Chinese privately-owned refiners, or towards emerging markets and the Middle East. While the ban was meant to lower demand for Russian crude oil, producers weaning off this oil supply would have to find their oil elsewhere, and care had to be taken to prevent an inadvertent hike in prices resulting in higher revenues for the oil Moscow still managed to sell.

EU and G7 countries could not buy Russian oil, regardless of the price, under the sanctions regime. Limiting Russian oil revenue, while still allowing these barrels to reach the market, was a core part of the balancing strategy inherent in these sanctions. A price cap mechanism was thus created, which allowed non-EU and non-G7 countries to purchase Russian oil using EU transport, insurance, and freight services if the purchase price was below the price cap, initially set at $60 per barrel. This was intended to allow Russian barrels to continue to flow, and prevent a sharp rise in global energy prices, while also placing downward pressure on Moscow's realized oil selling price. However, the G7 price cap was viewed by some as a "pointless gesture." For instance, a common criticism was that the cap was set at $60 a barrel at a time when the price of Urals crude grade oil was trading closer to $50 per barrel.[387]

Overall, the sanctions, combined with the price cap, did achieve a modest degree of success, considering the reality of major oil consumers waging economic warfare against a major oil producer on whom they were reliant for energy. While the goal of the energy market sanctions on Russia were never clearly defined publicly, based on the policies put forth there appeared to be several implicit goals: 1) to reduce Moscow's near-term oil and gas revenue streams; 2) to avoid causing excessive commodity price inflation; and 3) to gradually suffocate the Russian oil and gas industry, negatively impacting the industry's mid- to long-term prospects.

The sanctions as implemented have made clear progress towards these goals. Oil traded through the Urals route (transiting to China and India) has traded at a consistent $20 to $40 per barrel discount compared to that of Brent crude, which is oil destined for Europe to which Russia can no longer sell, since March 2022. Assuming 10 million barrels per day of Russian oil production, this represented an annualized US$73 billion to US$146 billion negative impact on Russia's oil revenues, or 4-8 percent of the country's 2021 GDP. Meanwhile, Russian tax receipts from the oil industry were negative 48 percent with a year – all indicators of the price cap "having its intended effect."[388] Russian oil receipts were therefore constrained, even while their oil continued to flow, allowing global oil prices to stabilize between $70 and $100 per barrel.

This is not to suggest that there are not areas for potential future improvement by policy makers. First among these rests the fact that China and India chose not to subscribe to the price cap. Unfortunately, these nations are now two of the largest buyers of Russian crude oil, representing greater than 50 percent of Russian crude oil exports today. Customs data shows China's purchases of Russian crude oil have remained at a steady 1.5 to 2 million barrels per day. However, India's purchases of Russian oil have increased by more than 30 times to 1.4 million barrels per day, as of January 2023, a new record high.[389] Both China and India are buying Russian oil at prices above the $60 per barrel price cap. As shown in the following table, Chinese customs data shows that China's average Russia crude oil purchase price in December 2022 was $80 per barrel.

Energy sanctions thus clearly illustrate the first lesson of this chapter, in terms of the complexities inherent in the balancing act between timeliness of impact and maintenance of the implementing coalition. Energy sanctions also demonstrate the second lesson, the importance of the private sector in economic warfare strategies, in action. The Russian energy industry has been a revolving door for international oil companies since the 1900s, with foreign enterprises lured by the scent of profit, only to be eventually forced out by a mistrustful government unwilling to cede too much ownership to the West. Moscow lacks the technical knowledge, financing, or equipment to harness the full potential of its oil reserves on its own – a technological challenge that even neighboring China could struggle to help with given Russia's harsh terrain.[390] Russia typically spends roughly $20 billion to $25 billion on drilling and other oil services per year. Sanctions implemented since March 2022 have banned major oil field service companies like Halliburton, Schlumberger, and Baker Hughes from making new investments in the Russian energy sector, and in some cases these firms have begun to exit. Halliburton, for example, announced a sale of its Russian operations to some of its local former employees in September 2022.[391] The diminished presence, or outright removal, of international oil companies will impede the Russian oil industry's mid- to long-term growth prospects.

The previous table summarizes major international oil companies that have announced exits from the Russian energy industry due to sanctions since the start of the Ukraine war, as well as some companies that still have minor presence in the country. Once-promising projects now face an uncertain outlook – including Gazprom's Nadym-Pur-Taz, Yamal, and Kharasaveiskoye gas fields (negatively impacted by the Nord Stream 1 pipeline), and Vostok Oil (originally intended to sell to the EU). The lack of investment coupled with Russia's roughly 10 percent natural rate of decline might see oil production start to structurally fall, dramatically changing the future direction of the Russian economy.

Energy policy also provides rich ground to examine chapter lesson three, the importance of defensive economic warfare measures in addition to offensive. The sanctions discussed thus far are primarily focused on offense, i.e., harming the Russian economy in an effort to reduce its ability to conduct war. Defensive economic warfare focuses on reducing the power of an adversary to negatively impact one's own economy, or that of partner nations. A domestically focused piece of legislation like the U.S. Inflation Reduction Act might not appear at first glance to be an economic warfare action, but it contains key defensive strategies to reduce reliance on externally supplied energy and the components required to produce energy. The Act's USD200bn in (defensive) subsidies seeks to strengthen the U.S. solar and electric vehicle supply chain to reduce long-term dependance on fossil fuels.[392]

With China already a dominant player in the renewables sector. It provides more than 80 percent of world's polysilicon supply for the manufacture of solar panels, controls more than 60 percent of the global EV battery supply chain, and contains a majority of the world's critical mineral supply. In short, a lot of unlikely events would need to take place before the United States and its allies would be equipped to achieve *true* energy independence and the ability to wage economic warfare without having to worry about energy security. American reliance on Middle Eastern oil for global market stability shaped its foreign policies for decades. Care must be taken to ensure that the same critical over-reliance does not repeat itself with either Russia in oil and gas or, more likely, China in renewables, to facilitate next-generation energy security.

Cyber Sanctions and Tactics

Analysis of the cyber realm in the Ukraine-Russia conflict provides strong examples of both lesson two, the criticality of private sector coordination, and lesson three, the importance of both defensive and offensive tactics.

Technology development, particularly within a country's digital economy, is critical for overall productivity and therefore for GDP growth. Prior to the Russian invasion in February 2022, Ukrainian leaders in government and the private sector sought to foster the growth of the country's digital economy and its emerging cyber security industry. The government launched the Ministry of Digital Transformation in January 2020 with the mission to promote the introduction of electronic services for the government and the private sector. The widely-used Digital Country (Diia) application launched by the Ministry of Digital Transformation allows Ukrainian citizens to use electronic documents from their smartphones instead of physical ones for identification and informational purposes, and enables access to over 50 governmental services.[393] The

country has a strong technical education system, and thus digital talent pool, which Western companies were increasingly using for coding and other outsourced activities, with over 16,000 tech specialists entering the workforce annually.[394] Government and local business leaders sought to leverage the entrepreneurial spirit of the younger generation to drive overall economic growth.

The centrality of cybersecurity to cyber economy growth strategies led experts, including a panel organized by the UK National Cyber Security Center, to fear that Russia might take steps to disrupt the digital domain in Ukraine.[395] The United States Cyber and Infrastructure Security Agency warned of potential Russian cyber-attacks on both industry as well as government players in both Ukraine and the West.[396] Experts commonly made statements such as "conflict in Ukraine presents perhaps the most acute cyber risk U.S. and western corporations have ever faced."[397] Expectations were that Russia's advanced cyber capabilities would be a major feature of the initial onslaught and heavily disrupt Ukraine's digital economy.

In the initial phase of the conflict, Russia did launch cyber-attacks against a range of targets, including communications infrastructure as well as government services, but with limited success. The attack with the widest impact was the disruption of the ViaSat satellite communications network, which impacted even European nations outside Ukraine.[398] Russia also sought to overwhelm Ukrainian government web services with denial-of-service attacks and emplace wiper malware in critical infrastructure.[399] However, the impact of these attacks waned fairly quickly, and Russia has largely refrained from disruptive cyber activity outside Ukraine.

Ukrainian cyber defenders took actions quickly to establish continuity of digital communications and services in several ways, all highlighting the criticality of lessons two and three, private sector coordination and defensive tactics alongside their offensive components. Elon Musk, through his satellite constellation Starlink, rapidly provided an alternative means of satellite communications, though controversial interruptions to that service also highlight the importance of close, ongoing coordination with private sector actors. Microsoft, Amazon Web Services, and Google all helped in an accelerated transition of digital infrastructure to provide services on Western cloud platforms that Russians did not, or could not, attack. Brad Smith, the president of Microsoft, has stated, "$107 million of assistance went to literally move the government and much of the country of Ukraine from on-premises servers to the cloud. And I think that ability to disperse services and data to the cloud, and really put them in data centres that we run across Europe, has been one of the indispensable elements in defending

Ukraine."[400] The company Cloudflare volunteered externally-provided protection that proved essential in quickly reducing the impact of denial-of-service attacks.[401] Ukrainian initiative and technical acumen was crucial in achieving an unexpectedly high level of digital resilience, combined with the unprecedented speed and scale of action critically facilitated by Western companies in the first weeks.

As the war progressed, so has the digital struggle with results that so far favor the Ukrainians. The Russians have continued efforts to disrupt the digital environment, though as with other critical infrastructure the most effective attacks have been physical strikes against data centers and the loss of Internet services due to a lack of electric power. The Russians have manipulated the digital environment in areas they occupy with extensive forced switching of routing and service to Russian internet service providers. They have also used access to systems in occupied territories as a foothold inside of Ukrainian networks to launch wiper attacks designed to erase data, spread disinformation, and conduct denial-of-service attacks. Overall, cyber-attacks continue at a pace much higher than pre-war levels, including efforts to emplace destructive malware in critical infrastructure, but these attacks have been largely thwarted.[402] Why?

The actions of the Ukrainian cyber defenders and network operators particularly as supported by UA-CERT (Computer Emergency Response Team – Ukraine) have continued to prove agile in response, strongly enabled by assistance of private sector actors from Europe and the United States. The cybersecurity community, from the individual to the corporate level, has continued to volunteer significant assistance in the form of threat intelligence, attack surface monitoring, threat hunting, providing tools and training to national cyber response, and the full range of government organizations as well as critical infrastructures. The high degree of monitoring activity and rapid communication to provide warnings of malicious activity is shining a bright light on the Ukrainian digital environment, making Russian cyber-attacks very difficult.

Cyber defense assistance in Ukraine has been conducted almost completely by the private sector with little facilitation or funding from governments outside of Ukraine. One locus of activity has become the Cyber Defense Assistance Collaborative (CDAC) for Ukraine which has established an ongoing effort to match requirements provided by the Ukrainian National Security and Defense Council as well as from the Global Cyber Cooperation Center, a public-private partnership with a collective of over 15 Western cyber security and technology companies.[403] CDAC efforts, while only a subset of the assistance being provided, do illuminate how quickly the private sector self-organized to provide assistance and where the real capabilities to help the Ukrainians achieve digital resiliency in the face of the Russian onslaught are present.

This analysis highlights some of the key achievements of private sector participation in defensive tactics. It also, however, offers clear areas for future improvement, particularly in the area of coordination. Western governments have yet to engage fully and effectively in the Ukrainian conflict. While the United Kingdom and others were able to provide funds to enhance the scale of private sector efforts, the scale was severely limited in comparison to other sorts of assistance provided to Ukraine. The U.S. government has been hampered in giving assistance based on a lack of clear policy guidance and appropriate funding mechanisms. The U.S. Agency for International Development (USAID) funds that are available have largely not been deployed given lack of coordinated planning.[404]

Further, ensuring that the Ukrainians establish their own capacity for cyber defense and digital resiliency is crucial in an environment where Russian use of irregular warfare likely continues after the current military conflict stops. While discussions have begun to examine digital resiliency for Ukraine and its economy, the U.S. government and its allies lack a coherent process for engaging with the Ukrainians in this crucial element of conflict resolution and post-conflict stability. No evidence exists that ensuring a strong Ukrainian cyber defense program or broader digital resiliency has become part of a considered, broader U.S., NATO, or Western strategy of increasing costs for the Russians during this war or in the future.

The cyber dimension of the conflict in Ukraine highlights the operational challenges of deploying both offensive and defensive tactics in the cyber realm, with analysts pondering whether sustained, disruptive cyber-attacks are maybe harder than previously thought or assessing Russian incompetence in integrating cyber into Moscow's broader strategic plans. Examining what made the digital environment resilient in this case, understanding the fundamental value of being able to transition government services to the cloud, and providing cloud-based cyber defense services to Ukrainian organizations has proved crucial to success, making attacks against the digital environment less impactful. The private sector largely acted on its own in achieving these successes, with the acquiescence of the government but with neither guidance for nor guardrails on its activities. As of early 2023, the ramp-up of private sector assistance for Ukraine's cyber defense is still anemic compared to the necessary longer-term digital resilience needed to resist potential Russian aggression, leaving significant residual risk for Ukraine as we ponder its uncertain future.

A structured, strategic program of cyber-defense assistance and enhancing digital resilience needs to be part of U.S. and allied strategy for conflict resolution

and competition with Russia in Ukraine. As Ukraine rebuilds, their leaders today are stressing the need to leverage both their human talent and entrepreneurial spirit to establish a vibrant tech sector and digital economy. The National Council for the Recovery of Ukraine from the Consequences of the War has established a digitalization working group which has already outlined a draft plan.[405] A coordinated, large-scale public and private effort to provide technology, services, and training to establish strong Ukrainian cyber defense capabilities can also provide a new model for buttressing allies in other areas around the globe, enhancing deterrence and imposing costs against the coercive aims of our adversaries. The U.S. government with its allies can clearly define the need for an active private role, provide resources to scale assistance and ensure laws and regulations clearly set the conditions. The Russians, Chinese and other aggressors should view the landscape for potential digital aggression as filled with porcupines and armadillos.[406]

Summary

This chapter's analysis of economic warfare tools deployed in the Russia-Ukrainian conflict provides clear evidence of its three core lessons, alongside areas for potential incremental improvement for the consideration of policymakers.

Lesson one cautions the importance of the clear identification of goals, combined with an upfront recognition of the tradeoffs that exist between rapid achievement and steps that, while lengthening the timeline of impact, maintain the cohesiveness of the implementing coalition. The unique nature of the first conflict pitting energy producers (Russia) against energy consumers (most of the world) is a prime illustration of this trade off at work. Revenue from Russian oil sales had to be constrained, while still allowing enough oil to flow to prevent a spike in prices that would cripple the global economy and dismantle the very coalition of nations implementing the sanctions. Policymakers must clearly and consistently identify key goals as well as tradeoffs required and avoid heralding early signs of success as a meaningful victory. The U.S. Administration's commentary around the initial collapse of the ruble is a clear example of the dangers of claiming premature success while driving perceptions of medium-term failure. Sanctions are in many instances powerful but slow-moving tools, requiring sustained support over meaningful periods.

Lesson two emphasizes the importance of private sector coordination. This was seen in the critical role played by private sector financial companies to the implementation

of tactics targeting capital flows into and out of Russia; international oil companies to current and future Russian oil production capacity; and the central role of private cyber security and technology companies in the defense of Ukraine's digital infrastructure. The latter provides perhaps the best example of a situation where private sector efforts have been poorly coordinated with government efforts. Private sector actors have carried the day thus far but are unlikely to be able to carry the torch indefinitely. Policymakers must engage in early and ongoing coordination efforts with private sector players to ensure maximum impact. This may in some instances require new forms of public-private partnerships for effective implementation.

Lesson three centers on the requirement for both defensive economic warfare strategies in addition to the more common offensive strategies. Steps taken by the U.S. government to invest in green energy to reduce energy dependance and increase degrees of freedom when faced with an energy producing adversary are one example. Aggressive steps taken to defend Ukrainian cyber infrastructure is another. Policymakers must recognize that offensive plans to reduce an adversary's capacity to engage in war must be matched with a Marshall Plan-scale initiative to strengthen allied capacity to withstand said war.

About the Authors

James Sullivan is Managing Director, Head of Asia Pacific Equity Research at J.P. Morgan. He has held Asia-based roles in equity research (Credit Suisse) and hedge fund management (Citadel, Millennium, Oaktree) since 1998, before which he held strategy consulting, trade finance, and government relations roles at IBM in Washington, D.C. and New York City. He holds a Master's degree in International Relations (Dean's List Academic Achievement Award) from Harvard University's Extension School, an MBA from Duke University's Fuqua School of Business, and a Bachelor's degree in Political Science (Summa Cum Laude) from Marist College. James has held various advisory roles including as a WSD-Handa Fellow at the Pacific Forum, an External Associate for the Economic Conflict & Competition Research Group in the Defence Studies Department at King's College London, a Visiting Scholar at the Daniel K. Inouye Asia Pacific Center

for Security Studies and sits on Advisory Boards for the Fuqua School of Business and Duke Corporate Education. His academic work has appeared in publications inclusive of International Affairs, Security Nexus, and the Journal of Muslim Minority Affairs. He also serves as Deputy Director of the International Affairs Directorate for the United States Coast Guard Auxiliary and holds multiple marine safety qualifications.

Parsley Ong is J.P. Morgan's Head of Asia Energy & Chemicals Research, with over a decade of experience covering physical commodities and equities. She also covers the Asia EV battery & materials sector, with market-leading insights on global energy transition. In 2014, Parsley moved from the commodities team in Singapore to equity research in Hong Kong. Her primary stock coverage is in China, Korea and Taiwan. She is a graduate of the National University of Singapore.

Dr. Greg Rattray is Partner and Founder of Next Peak LLC, a cybersecurity risk management firm, and adjunct Senior Research Professor at Columbia University. He also serves as the Executive Director of the Cyber Defense Assistance Collaborative for Ukraine, which has facilitated over $30 million in voluntary cyber defense assistance to Ukraine from over 20 companies and organization from March 2022 to March 2024. He is also a Senior Advisor to Oliver Wyman, a global risk consultancy. Previously, Greg served at J.P. Morgan Chase from 2014-2019 as the Global Chief Information Security Officer (CISO), then Head of Global Cyber Partnerships. He established the JPMC cyber defense strategy and program. Dr. Rattray led the establishment of the Financial Systemic Analysis & Resilience Center (FSARC), a private-public initiative to address systemic cyber risks to the financial system and enhance the level of operational collaboration. Dr. Rattray retired from the U.S. Air Force in 2007 as a Colonel after 23 years including as Director for Cybersecurity on the National Security Council in the White House and commanding the Operations Group of the Air Force Information Warfare Center responsible for cyber operations and defending against cyber threats. He pioneered Defense Department and US national cyber exercise programs and initiated the AF and DoD partnership with defense industry. He has a B.S. degree from the U.S. Air Force Academy, a M.P.P. from the John F. Kennedy School of Government, Harvard University and a Ph.D. from the Fletcher School of Law and Diplomacy, Tufts University. He authored Strategic Warfare in Cyberspace and numerous other books and articles related to cyber and national security.

Discussion Questions:

1. How might organizational change improve implementation of economic warfare tools and increase their efficacy? For example, at present, traditional warfighting strategy for the United States sits with the Department of Defense, while economic warfare strategies are split between the Departments of Treasury, Commerce, Homeland Security, etc.

2. Why are defensive economic warfare strategies so rare? Are there differences between public support for offensive actions and defensive actions?

3. What are potential best practices to manage the interplay between public and private actors when pursuing economic warfare strategies?

4. When is enough too much? How can an actor know how far to push an adversary economically, without putting them so far in a corner that their leadership lashes out in unexpected ways?

Recommended Reading:

- Lambert, Nicholas A. *Planning Armageddon: British Economic Warfare and the First World War*. Cambridge, Mass.: Harvard University Press, 2012.
- Miller, Edward S. *Bankrupting the Enemy: The U.S. Financial Siege of Japan before Pearl Harbor*. Annapolis, Md.: Naval Institute Press, 2007.
- Mulder, Nicholas. *The Economic Weapon: The Rise of Sanctions As a Tool of Modern War*. New Haven: Yale University Press, 2022.
- Zarate, Juan Carlos. *Treasury's War: The Unleashing of a New Era of Financial Warfare*. First edition. New York: PublicAffairs, 2013.

The American Way of Proxy War[407] Rethinking U.S. Unconventional Warfare Doctrine and Concepts in the Context of Modern Irregular Warfare and Strategic Competition

Christian Ramthun, DeVan Shannon, and Maurice "Duc" DuClos

ABSTRACT

This chapter delves into the concept of proxy warfare, in particular, The American Way of Proxy War, by analyzing precepts, evolution, and offering recommendations for doctrine.

There is often a "sharp contrast between the adversary we combat and the ally we back."[408] When analyzing proxy war, this paper uses the cases provided by North Korea, Iran, Russia, and the Chinese Communist Party (CCP) to understand the recent past and the decade ahead. It explores the concept of proxy war as seen through the American lens of strategic competition. Given the changing security environment and the growing importance of proxies in irregular warfare, military leaders and decision-makers cannot rely upon dated understandings. This article offers insights into how to effectively leverage the proxy warfare principles of: objective, selection, management,

and control. Ideally, this exploration of the American Way of Proxy War will drive the discussions of decision makers to better employ proxies and to achieve U.S. strategic objectives against the CCP.

Introduction

Let us start with a question: why do states resort to the use of intermediaries to perform deniable operations, expand their influence beyond their borders, or gain a localized advantage? The answer is simple, because no matter what it is called—guerrilla warfare, surrogate warfare, proxy warfare, or Unconventional Warfare (UW)—its efficacy has been proven by every major power throughout history, and it is perhaps even more effective in today's rapidly changing strategic environment.[409]

This article offers insights into proxy warfare, which while called "irregular," has been a regular feature of warfare throughout history. It examines the historical use of proxies by various great powers as well as the underlying precepts that drove the evolution of the American Way of Proxy War, which continue to be factors today. Finally, it offers recommendations for how the concept of proxy warfare can be updated by taking best practices from other fields of study to stay ahead of rapidly evolving security challenges, and meet the demands of modern irregular warfare.

What are Proxies?

The utilization of proxies as a tool in both conventional and irregular warfare has a rich and diverse historical background, encompassing a range of cultures and civilizations that dates back to antiquity. However, despite its prevalence throughout history, the concept remains shrouded in ambiguity, with little formal definition or comprehensive analysis within the framework of U.S. military doctrine. This gap presents significant challenges for the effective implementation and utilization of proxy warfare as a strategic tool, highlighting the need for further examination and development of doctrine focused on the use of proxies.[410]

Due to the consistent disconnect between how the U.S. military designs, builds, trains, and employs its forces, the use of proxies by its government has caused much consternation. As currently (mis)understood, proxy warfare has a long tradition and was written into the U.S. Constitution as part of Article I, § 8, clause 11 through Letters of Marque and Reprisal. Such letters formally authorized a "proxy" to act on behalf of the government.[411]

While there are various terms for proxies and proxy warfare. For this chapter we use the following definitions:

> Proxy—authority given to a person to act for someone else.[412]
>
> Proxy war—a war fought between groups or smaller countries where each represent the interests of other larger powers, and may have help and support from these larger powers.[413]

Proxies come in various forms to suit specific circumstances. They operate on behalf of another power that cannot, or chooses not to, act during periods of deterrence, war, and competition. Proxies range from exotic guerilla bands, recruited spies, or saboteurs on one side of the spectrum, to locally recruited and trained armies and security forces on the other. All perform tasks that a government decides it would prefer that someone else conduct due to factors that include cost, risk, access, legitimacy, and/or attribution.

Freedom fighters, spies, local police, constabulary, mercenaries, porters, guides, sabotage cells, surrogates, guerrilla bands, ethnic armed groups, and host nation forces are all types of proxies that the United States has deployed in the modern era.[414] Regardless of the form they take, proxies can be either recognized or unrecognized. Recognized proxies have various levels of overt recognition, but their central feature is that an external power officially, in some capacity, admits to a relationship with the proxy. Unrecognized proxies are more complicated and lack official recognition by the sponsoring power. This lack of recognition can range from subtle fig leaves in the form of official statements of denial, to multiple layers of deception and misattribution that conceal the true relationship between a proxy and an external power.

Everything Old is New Again: The Rise of Creative Revisionist Powers

The United States is not unique in having a long history of using proxies in warfare. The various powers that oppose the current rules-based order have their own unique histories of involvement in proxy warfare. They learned from the Cold War and Gulf War that, to achieve ends that would normally require military force, their hand would need to be concealed. These powers realize that more subtle and complex techniques are required to keep the level of violence below a certain threshold. They adopted the Taoist concept of formlessness through their use of deniable and less attributed proxies.

> *Water is fluid, soft, and yielding. But water will wear away rock, which is rigid and cannot yield. As a rule, whatever is fluid, soft, and yielding will overcome whatever is rigid and hard. This is another paradox: what is soft is strong.*
>
> *—Lao Tzu*[415]

North Korea: Devious Hermits

North Korea, or the Democratic People's Republic of Korea (DPRK), decided to expand its proxy forces primarily through the Korean diaspora such as the Chosen Soren in Japan.[416] The DPRK would complete its transformation into a criminal enterprise by raising capital through crypto crime, dark web dealing, synthetic methamphetamine production, the sale of its population as slave labor, and targeted assassination.[417] The killing of Kim Jong Nam, Kim Jong Un's half-brother, was a textbook example of DPRK proxy operations. Two unwitting, want-to-be actresses, one from Vietnam and the other from Indonesia, were told they were going take part in a prank show. They were trained in how to conduct the "prank," and, after a few iterations, they were directed to conduct the prank on Kim Jong Nam in the Kuala Lumpur International Airport. However, this time the prank involved VX they were told to spray on the "target." VX, one of the world's most deadly nerve agents, was smuggled from the DPRK to Malaysia through state commercial airlines.[418] Dramatic assassinations combining unwitting proxies and chemical warfare agents with state sponsored criminal activity sends a clear message to any power that it is best to leave the Devious Hermit Kingdom alone.

Iran: Shadow Hand of the Mullahs

Iran, more formally the Islamic Republic of Iran, decided that it did not want to be the next Iraq on America's hitlist. Unique among the four nations listed in the U.S. National Security Strategy, Iran leaned into the development and funding of armed groups to serve as their proxies.[419] Lebanese Hezbollah (LH) became the most successful Shia co-religionist proxy force created by Iran's Iranian Revolutionary Guard Corps (IRGC).[420] LH was not the only proxy force created by the IRGC; it was designed to serve as part of the Shia vanguard and bring Iran's form of Revolutionary Theocracy to the Middle East. In Yemen, the IRGC trained, equipped, and directed the Houthis. They continue to wage a civil war in Yemen and conduct attacks against Saudi Arabia.[421] In Iraq, the number and variety of proxy organizations and militias are substantial, and

fall under the quasi-governmental banner of the Popular Mobilization Forces. Many began as part of the Badr Organization, an IRGC-created organization designed during the Iran-Iraq war to train and employ Iraqi Shia fighters against Iraq.[422] Badr's leader, Hadi al Amiri, began leading it during the Iran-Iraq War and continues to lead the group and the political party that represents the many Shia militias it nurtured in Iraq.[423] Asa'ib Ahl al-Haq, Kata'ib Hezbollah, and numerous other smaller groups, supported in different ways by the IRGC, ensure that Iraq stays weak and under the control of Iran after the departure of the majority of U.S. combat forces.[424]

These proxies, though easily connected to the IRGC, are hard to target and only conduct operations when they have the advantage, as they are able to blend back into the population. Proxy forces enable Iran to threaten the United States and its allies with limited fear of retaliation. This is because the United States will focus on the knife—the proxy—and not the hand that wields it—the IRGC. The funding, training, and equipping of these proxies is a cost-effective way to keep the Sunni powers in the Middle East at bay and avoid providing the United States with enough justification to directly target the IRGC.[425] To support these proxy forces and their operations, the IRGC maintains a network of semi-legal and illicit activities. This network primarily focuses on the drug trade, smuggling petroleum products, and other high return operations through an extensive Shia Iranian and Lebanese diaspora. These proxy enablers support and facilitate a global network the IRGC can use to circumvent Western sanctions, fund operations, and move people and things to where they are needed.[426]

Russia: Return of the Czar and Boyars

The Russian Federation inherited the extensive illicit and proxy networks built up by the Soviet Union and its civilian intelligence agency, the KGB, a precursor of the modern FSB.[427] The fact that Putin was himself part of this organization, and surrounds himself with former KGB operatives, indicates the extensive connection between these proxy activities and current Russian state leadership. The military intelligence wing, the GRU, had even more extensive experience during the Cold War developing, training, equipping, and directing proxy forces through the Soviet-supported wars of national liberation across Southeast Asia, Africa, and South and Central America.[428] Targeted assassinations through poisoning, the sabotage of European munition supplies, the funding of various left and right extreme parties, disruptive propaganda, the development of mercenary forces, and support to terrorist organizations, is a rough encapsulation of FSB and GRU proxy activities that fall under the Russian operational concept of Active Measures.[429] The operational concept of Active Measures is bound up in the current

Russian Hybrid warfare doctrine, named after its author, the Gerasimov Doctrine.

The only innovation that Russia has added is a reversion to Czarist Russian Feudal techniques where ethnic strongmen and disgraced nobles would raise private armies on behalf of the Czar to accomplish tasks the Czar did not trust the Imperial Army with conducting.[430] The Wagner Group, among other mercenary organizations, fit this classic feudal mold. Indeed, Cossack, Tartar, Mongol, and Kazak war bands, historically led by disgraced Russian nobles working themselves back into the good graces of the Czar, were originally used to inexpensively expand the Russian Empire. Wagner Group chief

Table 1. Punitive measures imposed on Russia post Ukraine invasion

Country/ Region	2021 crude oil production (Thousand barrels per day)	2021 refinery throughput (Thousand barrels per day)	Sanctions/action details	Status (as of Jan 2023)
European Union	366	9,453	Banned Russian seaborne crude oil imports from 5 Dec 2022, and oil product imports from 5 Feb 2023. Ban on providing insurance/finance/freight to transport Russian oil unless G7 price cap is met: From 5 Dec 2022, EU operators will be prohibited from insuring and financing the transport of Russian crude oil to third party countries unless the buyer complies with the G7 oil price cap.	In effect
Germany	Nil	1,691	Suspended certification of Nord Stream 2 pipeline. Banned Russian crude oil and oil product imports by end-2022	In effect
U.K.	874	879	Banned imports of Russian crude oil and products by end-2022 (phase out from Mar-Dec 2022)	In effect
U.S.	16,585	15,148	Banned all imports of Russian oil, LNG and coal from March 2022 From 5 Dec 2022, US financial institutions will be banned from processing transactions related to Russian energy sales.	In effect
Canada	5,429	1,653	Banned imports of Russian oil products from Feb 2022. Prohibits the provision of key services to Russia oil, gas and chemical sectors from 8 Jan 2022.	In effect

Country/ Region	2021 crude oil production (Thousand barrels per day)	2021 refinery throughput (Thousand barrels per day)	Sanctions/action details	Status (as of Jan 2023)
G7 & Australia	roughly 17,000	23,769	SWIFT ban: EU and allies banned 7 Russian banks from international payment system SWIFT on 2 March 2022, with Sberbank and Gazprombank excluded from the ban to allow Russian energy and commodity trade to continue. Sberbank was added to the SWIFT ban on 14 Jun 2022, while Gazprombank remained exempt. G7 oil price cap: From 5 Dec 2022, non-US/ EU buyers of Russian crude oil were only allowed to use crucial services provided by the EU (eg. Shipping, insurance, financing) if they can provide proof that the transaction price is at or below the G7 price cap ($60/bbl as of Jan 2023). From 5 Feb 2023, similar price caps were imposed on oil product ($100/ bbl for "oil products at a premium to crude" like diesel and gasoline, and $40/bbl for "oil products at a discount to crude" like fuel oil). The price caps are adjusted every 2 months from mid-March 2023 based on market conditions.	In effect
Other			Most listed refiners (Japan, Korea, Thailand, Taiwan etc) stopped purchasing Russian crude oil despite being technically able to do so as long as they complied with the G7 oil price cap, due logistical issues or ESG concerns.	-
China	3,994	14,461	Increased imports of Russian crude oil and gas. Russian crude oil as a % of total imports rose from 15% in March 2022, to 18% in October 2022, with an average $10-15/bbl discount versus other grades	No sanction
India	746	4,792	Increased imports of Russian crude oil	No sanction

Source: European Commission, J.P. Morgan Asia Energy Research.

Yevgeny Prigozhin, and Chechnya Warlord Ramzan Akhmadovich Kadyrov, fit this profile and do things the "Czar" cannot trust Russian state forces to conduct.[431] Russia has reverted to its Czarist past while retaining all the proxy skills built up throughout the Soviet period and their ill-fated efforts to create a world socialist revolution.

China: Unrestricted Dragon

Of the four nation states discussed here, the Chinese Communist Party (CCP) is the most dangerous of the revisionist states that desire to overthrow the current rules-based world order and replace it with their version of communism.[432] When discussing Chinese leadership, this paper will refer to the Chinese Communist Party rather than the People's Republic of China (PRC). This is because in the PRC primary documents, the CCP stands above and over the state, so it is better to focus on the organization that holds true power.[433] The elements of national power, such as the Ministry of State Security (MSS), People's Armed Police (PAP), or the People's Liberation Army (PLA), do not pledge their loyalty and allegiance to the state but to the CCP. The CCP is the last revolutionary Marxist-Leninist party bent on global socialist revolution that retains control of a powerful state.[434] An inherently secretive, cellular, and clandestine organization whose doctrine reinforces the Sun Tzu maxim, "All warfare is based on deception."[435] The CCP is the most proficient in the use of proxy forces below the threshold of armed conflict.

Through the Maoist period, the CCP focused on supporting the most extreme communist revolutionaries. Mao cultivated the most ruthless and diabolical proxies such as Pol Pot and his Khmer Rouge, Robert Mugabe and his ZANU, the Indonesian Communist Party, Abimael Guzman's blood-soaked Shining Path in Peru, Enver Hoxha's People's Socialist Republic of Albania, and numerous other Maoist revolutionary proxies across the globe, including Maoist groups in the United States.[436]

Under Deng Xiaoping, the CCP toned down support for violent revolutionary organizations in exchange for American investments and concessions.[437] Deng focused on reorienting the CCP propaganda department into a modern organization. Deng and his CCP successors, Jiang Zemen and Hu Jintao, followed Deng's dicta, "[o]bserve calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership."[438] With the collapse of the Soviet Union, the lopsided American victory in the Gulf War, and the crushing of the Tiananmen Square protests, the CCP conducted a massive post-mortem and came up with a new strategy to defeat the United States.[439] This strategy would focus on several key concepts that would each require their own unique proxy forces in

order to hide the hand of the CCP.[440] The CCP would not give up its ability to support revolutionary armed groups, as demonstrated by the Party's deft use of the United Wa State Army to exert influence over the Generals of the Myanmar Tatmadaw to remove the democratically elected government and reinstate the CCP's Belt and Road Initiative projects.[441] As Sun Tzu stated, "[t]hus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations."[442]

Unlike the other revisionist actors who use structures familiar to Western audiences, the CCP operates in a completely different manner based on its own revolutionary experience.[443] Therefore, the closest analogue, responsible for the majority of CCP proxy operations, is the United Front Work Department (UFWD). However, the UFWD is not the only organization that conducts proxy operations, the CCP also has a CIA analogue in the form of the Ministry of State Security (MSS), a Homeland Security analogue in the form of the People's Armed Police (PAP), and the People's Liberation Army. All of these organizations are responsible for their respective proxy operations, but none compare to the scope and scale of those conducted by the UFWD.[444] Due to the fluid nature of the CCP party cadre structure which allocates capabilities that are not necessarily part of certain perceived organizational structures, it is hard to determine where the UFWD ends and MSS, PAP, and PLA-covered overseas operations begin. At times, the UFWD appears to provide cover and support for MSS, PAP, and PLA overseas operations. At other times, it appears that the UFWD is directing MSS, PAP, and PLA operatives to achieve UFWD clandestine objectives.

At the core of the United Front Work Department (UFWD) is a massive influence apparatus with control over religious, scholarly, and cultural organizations. The UFWD is responsible for cultivating relationships with non-Communist groups through several efforts aimed at advancing the interests of the CCP. While the exact nature of efforts undertaken by the UFWD to bring those groups into line with CCP policy, and neutralize any potential opposition, are difficult to ascertain, it is known that these operations include co-opting key individuals and organizations, influencing overseas Chinese communities, countering dissent, shaping global discourse, and shaping public opinion.[445] The statement at the end of the U.S. National Security Council Paper 68 (NSC-68), concerning the threat of the Soviet Union, is also true today when dealing with the CCP. "The whole success...hangs ultimately on recognition by this Government, the American people, and all free peoples, that the cold war is in fact a real war in which the survival of the free world is at stake."[446]

Table 2. China crude oil import mix and purchase price

	China crude oil import mix %							Price premium/(discount) vs China avg ($/bbl)						China avg purchase price ($/bbl)	Monthly import (kbd)		
	Saudi	Russia	Angola	Iraq	Oman	Malaysia + Iran	Other	Saudi	Russia	Angola	Iraq	Oman	Malaysia + Iran		Saudi	Russia	China total
2013	19%	9%	14%	8%	9%	8%	33%										
2014	16%	11%	13%	9%	10%	9%	32%										
2021	17%	16%	8%	11%	9%	4%	37%										
2022	17%	17%	6%	11%	8%	7%	34%										
Jan-22	16%	15%	6%	14%	11%	3%	35%	1.5	(1.3)	2.1	(2.4)	0.1	(8.8)	77.9	1,882	1,716	11,538
Feb-22	18%	15%	9%	9%	10%	2%	37%	(1.1)	(0.0)	(1.6)	(3.5)	1.0	(5.0)	85.0	1,740	1,416	9,513
Mar-22	16%	15%	7%	11%	7%	4%	40%	(1.4)	1.4	2.2	(4.7)	(2.5)	(0.3)	96.3	1,622	1,510	10,099
Apr-22	21%	15%	6%	10%	7%	5%	36%	1.7	(8.7)	3.5	0.5	0.8	(13.2)	108.2	2,182	1,601	10,514
May-22	17%	18%	7%	10%	9%	5%	33%	5.0	(11.6)	4.5	0.6	5.1	(13.8)	104.6	1,849	1,991	10,835
Jun-22	14%	20%	7%	9%	6%	8%	36%	7.7	(14.2)	4.1	2.2	9.6	(14.7)	108.6	1,236	1,780	8,752
Jul-22	18%	19%	6%	10%	7%	9%	31%	5.7	(16.0)	8.4	3.4	8.0	(22.0)	110.0	1,552	1,690	8,826
Aug-22	21%	21%	5%	11%	7%	8%	27%	6.2	(13.2)	11.6	3.1	6.0	(23.6)	102.9	2,004	1,973	9,542
Sep-22	19%	19%	5%	13%	8%	10%	27%	6.5	(11.4)	6.3	2.5	8.8	(22.7)	97.5	1,840	1,823	9,832
Oct-22	18%	18%	5%	11%	7%	8%	33%	4.0	(8.4)	5.0	0.2	8.8	(19.5)	94.1	1,874	1,824	10,200
Nov-22	14%	17%	4%	12%	7%	10%	36%	4.4	(3.5)	3.0	(0.8)	8.1	(12.6)	91.9	1,616	1,909	11,420
Dec-22	15%	13%	5%	11%	7%	11%	37%	4.0	(6.5)	5.7	(0.4)	8.6	(18.1)	87.0	1,683	1,530	11,365

Source: General Administration of Customs, JP Morgan Asia Energy Research

International IOCs have announced over $50bn in Russia asset impairments

Major IOC	Russia as % 2021 1P	Russia as % 2021 NP	Comments	Status
BP	53%	23%	BP held 19.8% stake in Rosneft. Booked a total of ~$26bn pre-tax losses in 2022 from the Rosneft exit (of which $13.5bn impairment, $11.1 FX losses accumulated since 2013 and $1.5bn from the write off of other business with Rosneft).	Impaired over $26bn. Exited Rosneft
Total	21%	na	Total owned 19.4% stake in Novatek (owns 60% stake in Arctic LNG 2, 50.1% stake in Yamal LNG and other Russia gas fields), 10% stake in Arctic LNG 2, 10% stake in Yamal LNG, 49% stake in TerneftеGaz and 20% stake in Kharyaga. Total also had a 10% direct stake in Arctic LNG 2 and 10% direct stake in Yamal LNG. Total booked a total of ~$14.8bn impairments in 2022 from the exit of Novatek ($10.7bn) and Arctic LNG ($4.1bn). Total maintained 10% stake in Yamal LNG as the asset is not affected by sanctions.	Impaired over $10bn. Exited Novatek and Arctic LNG
ExxonMobil	1%	na	XOM held 30% stake in Sakhalin-1. Booked $4.6bn of impairment in 2022.	Impaired over $4.5bn. Exited
Shell	na	na	Shell owned 27.5% stake in Sakhalin-2, 50% stake in Salym JV, 50% stake in Gydan JV and also had service stations and lubricant business in Russia. In addition, Shell is a loan provider for the Nord Stream 2 project. Shell booked a total of $4.5bn impairments from the Russia exit in 2022, of which $1.6bn was related to Sakhalin-2 and $1.1bn was related to loans provided to Nord Stream 2.	Impaired over $4.5bn. Exited Sakhalin-2, Nord Stream 2 financing.
CNOOC	<0.1%	Negligible	Holds 10% in Arctic LNG 2, production starting over 2023-2026 with 19.8 Mtpa LNG when fully ramped. Payments represent max ~5% of market cap	No impact currently
Sinopec	<0.1%	1.5%	Holds 10% stake in SIBUR (Russian petchem company) and 49% stake in Taihu (Russia E&P JV with Rosneft). The 2.4Mtpa JV cracker (Amur GCC) with Sibur under construction from Aug'20, target complete by May 2024 (note potential funding issues due to sanctions).	No impact currently
PetroChina	<0.1%	Negligible (E&P only). Gas imports loss-making in 2021	Indirectly holds 20% equity interest in OAO Yamal LNG and 10% equity interest in Arctic LNG 2, in both of which OAO Novatek holds more than 50% interest. Russia represents ~15% of gas import mix, rising to 30% by 2025	No impact currently
ONGC	18.5%	~1.1%	Primarily Sakhalin-1 (20% stake), Imperial and Vankor projects.	No impact currently

Source: Company data, JP Morgan Asia Energy Research.

General Precepts in the use of Proxies in Irregular Warfare

Taking America's adversaries into account, the United Sates must figure out the best way to use its own proxies. The employment of proxies is a means of accomplishing strategic objectives while mitigating the costs, risks, and responsibilities inherent in direct involvement. This is especially important in irregular warfare, where one party may lack the military capability or political fortitude to engage in direct confrontation with a more formidable adversary. By harnessing the resources, capabilities, and indigenous knowledge of proxy forces, the United States can achieve its goals without incurring direct accountability for the actions of these forces.

The use of proxies is not without its risks and challenges and is not bereft of consequences. Proxies can prove unpredictable and difficult to control, and may act in ways that are counter to the interests of the supporting power. Proxies can create a perception of ambiguity and deniability, which can erode the legitimacy of a power's actions and undermine its moral authority. The utilization of proxies in irregular warfare is a sophisticated and nuanced instrument that demands careful consideration of potential benefits and associated risks. Despite its historical and contemporary significance, the use of proxies must be weighed against the broader strategic objectives of the state and evaluated within the context of the specific circumstances of each conflict.

The general precepts of proxy warfare, listed below, are informed by history and experiences from nations across the world, including the United States. These overarching concepts are derived from timeless and universal tenets not specific to any sponsor or proxy. They encapsulate the critical elements necessary for the successful utilization of proxy forces. Central to these elements is: the establishment of well-defined objectives, the careful selection of proxies, the efficient management of proxy relationships, and the ability to maintain control and terminate the relationship when necessary.[447]

Objectives: Defining clear objectives is one of the most critical aspects of utilizing proxies in conventional or irregular warfare. It is crucial to have a clear and concise understanding of what is to be achieved before initiating any proxy operation. A clear objective guides the development of the operation, ensuring that it is focused and directed towards achieving the desired outcome.

Well-defined objectives provide a roadmap for the use of resources and assets. When a state lacks clear objectives, it runs the risk of investing significant resources in proxy

operations that are poorly targeted, and thus unlikely to achieve desired outcomes. This leads to wasted time, money, and manpower, as well as avoidable political and strategic consequences that proper planning would negate. Clear objectives ensure that proxy operations are aligned with the state's strategic goals. This helps maximize the chances of success, and minimize the risk of unintended consequences. All relationships are inherently transactional.[448] In order for that transaction to meet desired objectives, it's best if there is a clear understanding of the desired end state, or "what winning looks like."[449]

Unfortunately, winning through proxies is often hampered by sponsors who miss the most important question; "what do we need the proxy to do?" Instead, they focus on the proxy's organizational structure, grievances, ideology, or level of training in maneuver warfare tasks. Having a clear understanding of the task or objective the state wants a proxy to accomplish, leads to the question of "who can do it?" Then, "what do they need from us?"

Selection: States must carefully evaluate the abilities and motivations of potential proxy forces. Choosing the wrong proxy can have significant negative consequences. Proxies must have the necessary skills and capabilities to achieve the state's objectives, and must also be motivated to participate in conflict in the desired ways. The reliability and trustworthiness of proxies is critical for the success of proxy operations. Past efforts in human terrain and network mapping, along with civil reconnaissance, provide valuable tools in identifying the most suitable proxy candidates.[450] These efforts help states to better understand the local context and actors involved, and to identify those who are capable of meeting or assisting in their objectives.[451]

Management: Effective management of proxies is critical to proxy operations and is essential for ensuring success. States must have a clear understanding of the nature of their relationship with their proxies, and must differentiate between an *exploitative model* that is driven by the sponsor, and a *transactional model* that is driven by the proxy.[452] This differentiation is crucial for establishing an effective working relationship and ensuring that the proxies can achieve the state's objectives.

In an exploitative model, the sponsor holds power over and dictates the terms of the relationship, with the proxy playing a secondary role. This model is often used when the sponsor has limited resources or capabilities, and must rely on the proxy to carry out the operation. It is important to understand the limitations of this model. The proxies may lack motivation and not fully commit to achieving the sponsor's objectives.

In a transactional model, the proxy is empowered and has an active role in the operation. This model is often used when the sponsor seeks to establish a more collaborative relationship with the proxy. Transactional relationships are suited for complex operations that require the autonomous actions of the proxy.

Effective management of proxies requires a well-structured command and control system, with clear lines of communication and regular reporting requirements. The sponsor must provide the proxies with the necessary support and resources, while having the capability to monitor proxy actions to ensure they remain aligned with the objectives of the operation.

Control: The capacity to disengage from the relationship with proxies in irregular warfare is a critical tenet. States must prepare to terminate the relationship if its underlying objectives are no longer achievable, or if the situation on the ground changes in such a manner that makes the continuation of the conflict untenable. This ability to disengage minimizes the risk of exposure, and mitigates the potential political and strategic implications of proxy failure. An effective exit or transition strategy, careful contingency planning, and a consideration of the political and strategic implications of disengagement ensure the success of any proxy operation and minimize the risk of exposure and its attendant negative consequences.[453]

While these four general precepts—*objectives*, *selection*, *management*, and *control*—are common across the spectrum of historical use of proxies, they are in no way exhaustive or inherently prescriptive. Every conflict is unique, and has its own set of constraints, challenges, and dependent variables that the sponsor and proxy should consider to achieve their objectives.

Leveraging "Like Fields" to Better Understand Proxy and Unconventional Warfare Doctrine

Doctrine is not dogma. It is the foundation the force stands on, not the ceiling that limits creativity. One can argue that the doctrinal and common use terms—unconventional warfare, foreign internal defense, security force assistance, training and advising, partnered force operations, and through and with—are all "code switching" for the underlying meta concept, proxy warfare.[454] To keep pace with the dynamic operational landscape and shifting mission requirements, it is imperative that U.S. doctrine regarding proxy warfare, regardless of its current moniker, incorporate and integrate the most effective and proven practices derived from other established areas

of both intellectual inquiry and practical application, such as principle-agent theory, outsourcing, and venture capitalism.

Principal-agent theory, outsourcing, and venture capitalism are three such fields that offer valuable insights into the optimization and refinement of proxy warfare. These "like fields" have a wealth of research, practical applications, and successful case studies to draw upon.

Principal-agent theory is a fundamental concept in management and organizational behavior that explains the relationship between a principal (such as a company or government) and an agent (such as an employee or sub-contractor) who acts on the principal's behalf.[455] In the case of proxy warfare, the framework provides a way of understanding the dynamic relationship between a principal (i.e., the state) and its agent (i.e., the proxy force). This theory helps us understand how to align the interests of the state and the proxy to maximize their collective impact, while minimizing the risks associated with delegation.

In the context of irregular warfare, the principal-agent relationship between the sponsor and their proxies can be viewed as a complex and dynamic partnership that must be managed effectively in order to achieve the desired outcome. Principal-agent theory sheds light on the motivations and control of proxies, and highlights the potential for recurrent conflicting interests.

One of the key lessons from the principal-agent theory is the importance of aligning incentives and interests between the principal and the agent. In the case of proxy warfare, this means that the sponsor must ensure that their proxies have a clear understanding of the objectives and desired outcomes of the mission, as well as the resources and support they need to accomplish the task. In addition, the sponsor should track the actions and performance of its proxies, and provide feedback and guidance as needed. It is the sponsor's responsibility to manage both the relationship and their own objectives, with the assumption that the proxy will manage their own interests. To achieve this, there is a need for clear communication between the principal and the agent.

Outsourcing has important implications for proxy warfare. Outsourcing involves the transfer of certain business functions or processes to a third-party provider. Outsourcing, a common practice in the business world, has important lessons that transfer to the effective management of proxies.[456] Outsourcing minimizes the costs and risks of direct involvement in specific actions, while leveraging the skills and capabilities of external partners to achieve mutually beneficial objectives.[457]

Outsourcing has already changed the way many nations "fight" wars, but is not fully accounted for in existing doctrine. It requires careful consideration to fully appreciate the versatility outsourcing offers, as well as the associated risks. In proxy warfare, the state outsources certain activities to the proxy. It provides flexibility in how the state achieves certain objectives, while focusing military assets on strategic tasks.[458] This agility is critical in irregular warfare, where the outcome is often determined by the ability of the state to quickly respond to shifting conditions.[459]

Venture capitalism can inform the evolution of proxy warfare. Venture capitalism involves investing in start-up companies with the potential for high growth, in exchange for a share of the ownership and profits. In the context of irregular warfare, this could include investing in nascent proxy forces with resources, training, and support, in exchange for some degree of operational control.[460]

Looking at proxy warfare through the lens of venture capitalism provides a fresh perspective on how the sponsor can effectively invest and cultivate proxies for a sustained return on investment over time. The venture capital methodology approaches the sponsor as a business entity, or financial institution, which makes investments in nascent startups with the expectation of realizing potential future profits. The proxy investments are managed in a manner that prioritizes the attainment of tangible return on investment (ROI). Thereby aligning the interests of the sponsor with that of the invested startups. Venture capitalism can foster innovation and entrepreneurship among local proxies, leading to new and more effective ways of achieving operational objectives.

The integration of insights from three related disciplines—principal-agent theory, outsourcing, and venture capitalism—presents a unique opportunity to broaden and enrich the comprehension of the fundamental principles and successful practices of proxy warfare. These interrelated fields offer distinct valuable perspectives to doctrine development.

Conclusion

In an era of strategic competition, the United States must remain at the forefront of developments in the use of proxies in irregular warfare, while remaining true to American values. Historical studies of proxy warfare utilized by the United States and its competitors can help planners and decision-makers understand the way proxy warfare was used in the past, and develop theories and strategies for proxy management today. The principles of clear objectives, selective proxy recruitment, effective control, and the ability to terminate the relationship, established over centuries of experience, remain

relevant in strategic competition with the CCP. By following these principles, the United States can successfully navigate the changing landscape of military strategy, and close the gaps between the ideals of traditional war, and the realities of irregular war today.

About the Authors

Christian J. Ramthun is a Master Instructor with the Joint Special Operations University, U.S. Special Operations Command, located at MacDill AFB, Florida. Mr. Ramthun is responsible for developing, instructing, and managing courses as part of the College of Special Operations and Low Intensity Conflict. Christian's current research focus is redefining joint SOF education.

DeVan Shannon is a retired U.S. Army Special Forces Lieutenant Colonel, who served at each level of Special Operations from team leader to staff officer at USSOCOM. With five combat tours in Iraq and the Philippines, along with numerous deployments across Asia and the Middle East. He holds a master's degree in history, from the National University of Singapore, writes and teaches on resistance and resilience, special operations, Asian security issues, and U.S. doctrine.

Chief Warrant Officer Five Maurice "Duc" DuClos is an active-duty Special Forces warrant officer. His career spans the SOF enterprise from the 2nd Battalion of the 75th Ranger Regiment to the 1st Special Forces Group in Okinawa and JBLM Washington. While working as a doctrine developer at the U.S. Army John F. Kennedy Special Warfare Center and School, Mr. DuClos helped write key doctrine in the field of Unconventional Warfare and is recognized as one of the SOF subject matter experts in the field. He is currently assigned to USSOCOM where he advises the command on Irregular and Unconventional Warfare.

Discussion Questions:

1. Which proxies should the United States support to achieve its strategic goal of bolstering the rules-based international order, or is that a contradiction?

2. What training and education should the U.S. Military add to its Professional Military Education program for officers and NCOs, to ensure the better management of proxies in future operations?

3. Based on past lessons recorded on the failure of proxy forces in Iraq and Afghanistan, how should the United States adjust its Security Forces Assistance programs to ensure better results?

4. Clear, hierarchical chains of command are at the heart of U.S. military culture. Where should the United States focus its efforts to adjust its military culture, so that NCOs and officers can embrace their role as inherently indirect leaders of proxies?

Recommended Reading:

- Mead, Walter R. 2002. *Special Providence: American Foreign Policy and How it Changed the World*. New York, New York: Routledge.
- Rid, Thomas. 2021. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York, New York: Picador.
- Kretchik, Walter E. 2011. *U.S. Army Doctrine: From the American Revolution to the War on Terror*. Lawrence, Kansas: University Press of Kansas.
- McClintock, Michael. 1992. *Instruments of Statecraft: U.S. Guerrilla Warfare, Counterinsurgency, and Counter-terrorism, 1940-1990*. New York, New York: Pantheon Books.

Terrorism and Irregular Warfare: The Four-Headed Challenge of Massed Terrorists, Terrorist Dispersal, State-Sponsored Terrorism, and Terrorist Franchising

Thomas Searle

ABSTRACT

Terrorism and counterterrorism (CT) are vital parts of irregular warfare, but they risk being neglected as the focus shifts to irregular warfare by authoritarian states. Terrorists in a far-off country may not directly threaten the U.S. homeland; however, the way the local government conducts CT will determine whether that nation becomes more democratic or more authoritarian. As a result, CT is critical to the current era of international strategic competition between democracy and authoritarianism. The best way to improve our chances of success in CT and hence in strategic competition is to build on what we learned about terrorism since the 11 September 2001 attacks on the United States. This chapter frames that understanding in terms of four concepts: Massed Terrorists, Terrorist Dispersal, State- Sponsored Terrorism, and Terrorist Franchising. The 7 October 2023 terrorist attack on Israel provides a high-profile

opportunity to validate these four concepts as ways to analyze terrorism and CT. Terrorism and counterterrorism (CT) are vital parts of irregular warfare, but they risk being neglected as the focus shifts to irregular warfare by authoritarian states. Terrorists in a far-off country may not directly threaten the U.S. homeland; however, the way the local government conducts CT will determine whether that nation becomes more democratic or more authoritarian. As a result, CT is critical to the current era of international strategic competition between democracy and authoritarianism. The best way to improve our chances of success in CT and hence in strategic competition is to build on what we learned about terrorism since the 11 September 2001 attacks on the United States. This chapter frames that understanding in terms of four concepts: Massed Terrorists, Terrorist Dispersal, State- Sponsored Terrorism, and Terrorist Franchising. The 7 October 2023 terrorist attack on Israel provides a high-profile opportunity to validate these four concepts as ways to analyze terrorism and CT.

Introduction

Terrorism has an uncomfortable relationship with special operations and irregular warfare. On the one hand, some of history's most famous terrorist attacks, such as the 1914 assassination of Austrian Archduke Franz Ferdinand,[461] used techniques similar to direct action raids, were state sponsored, and were part of irregular warfare campaigns waged by nation-states. On the other hand, virtually every nation denies involvement in terrorism while simultaneously advertising its expertise in special operations and irregular warfare.[462] Counterterrorism, by contrast, is warmly embraced as a special operation and form of irregular warfare.[463] This chapter will follow the U.S. Naval War College's Center for Irregular Warfare and Armed Groups and other sources in considering both terrorism and counterterrorism as forms of irregular warfare (IW), and, hence, valid topics for this volume.[464] This is true even though the United States does not conduct terrorist operations or sponsor terrorist groups. This chapter focuses on overseas terrorism by non-U.S. persons and organizations that threatens the United States and its interests and excludes U.S. domestic terrorism.

This chapter will start by pointing out the vital role of CT in the current era of strategic competition between democracy and authoritarianism. It will then assess our post-9/11 understanding of terrorism in terms of four concepts: Massed Terrorists, Terrorist Dispersal, State Sponsorship of terrorism, and Terrorist Franchising. It will end by applying these concepts to the 7 October 2023 terrorist attack on Israel and subsequent Israeli response.

Counterterrorism: A Wicked Distraction or the Main Event?

Within this volume, irregular warfare is seen primarily as a tool used in strategic competition between nation-states. Terrorism, on the other hand, is conducted by non-state actors.[465] Since terrorists are non-state actors and strategic competition is focused on rival states, the issues are seen as distinct. This, in turn, suggests resources devoted to counterterrorism represent a diversion of resources from the main threat, namely state-level strategic competitors, to secondary nuisances, such as the violent extremist organizations (VEOs) that conduct terrorist attacks. From this perspective, counterterrorism (CT) must accept an economy-of-force effort where the goal is to employ the fewest resources possible to prevent terrorist attacks from distracting the United States from the main effort: strategic competition with other states. The two most recent U.S. National Security Strategies, signed by Presidents Donald Trump (2018) and Joseph Biden (2022), reflect this view.[466] Since terrorist attacks on the U.S. homeland are most likely to divert attention and resources from strategic competition, such threats are the focus of CT efforts. These efforts have been broadly successful, since the latest United Nations report on terrorism indicates a relatively low terrorist threat to the U.S. homeland.[467]

Unfortunately, terrorism is more than merely a distraction, and the economy-of-force model of CT is misguided. If, as the Biden Administration often claims, the current era of strategic competition is a contest between democracy and authoritarianism, CT is at the center of that contest.[468] After all, the key difference between democratic and authoritarian governance is how each handles political opposition, and the most challenging form of this opposition consists of VEOs conducting terrorist attacks. There is a democratic method of countering terrorism by VEOs and an authoritarian method. Once a government embraces authoritarian CT, it is usually locked into a similar approach to governance from which it cannot recover. For example, Napoleon Bonaparte's use of cannons against a Paris mob on 13 Vendémiaire,[469] Adolf Hitler's response to the Reichstag fire,[470] Vladimir Putin's handling of Chechnya,[471] and the thirty-year "state of emergency" in Egypt after the 1981 assassination of Anwar Sadat[472] were defining events in the governance of each regime, driven by their responses to terrorism. How a state handles violent extremist organizations is an essential aspect of how it governs. If a budding democracy gets CT right (i.e., conducts successful CT in line with democratic values), it is well on its way to long-term success. In contrast, a state getting CT wrong (i.e., conducting CT in an authoritarian manner) is probably locked into an authoritarian model for decades.

Unfortunately, the Biden Administration and its allies fail to see the connection between CT and the global strategic competition between democratic and authoritarian governance. Until they do, CT will be relegated to an economy-of-force role, and terrorists will be seen as a distraction rather than the all-important test case for defining whether a partner state's governance is democratic or authoritarian.

This approach leaves practitioners in the U.S. government stuck with the challenge of conducting CT with minimal resources. To understand the terrorist challenge, we will look at four separate aspects of terrorism—massed terrorists, terrorist dispersion, state-sponsored terrorism, and terrorist franchising—and develop CT methods to handle each one with minimal resources.

Massed Terrorists

Massed terrorists seem like an oxymoron since we usually imagine terrorists in small, clandestine groups, but they will mass when they can and disperse when the must. Since 9/11, the United States and its Western allies have faced and defeated the challenge of thousands of terrorists openly massing in one place at least five different times. We shall examine the methods used in each of these five instances and assess whether the techniques that succeeded before will work in Taliban-ruled Afghanistan, assuming terrorists will mass there in the 2020s.

Afghanistan 2001

The first post-9/11 instance of massed terrorists was in Afghanistan in 2001. Under the leadership of Mullah Mohammed Omar, the Taliban government made Afghanistan a welcoming safe haven for Salafi Jihadi terrorists from all over the world. In the spirit of thinking globally while acting locally, the Taliban focused its efforts on governing Afghanistan, while also making the country a home-away-from-home for virtually every Salafi Jihadi terrorist group in the world.[473] Osama bin Laden's al-Qaeda was just one of many groups that established themselves in this friendly environment prior to 9/11.

After the 9/11 terrorist attacks, the U.S. Government demanded the Taliban hand over Osama bin Laden for trial. When the Taliban refused, the United States employed a potent ground force, through the provision of advice and assistance, to anti-Taliban irregular forces inside Afghanistan. The United States also secured basing and overflight permission from neighboring countries, most critically Pakistan and Uzbekistan, which enabled a massive air campaign against the Taliban. The combination of indigenous

ground forces and U.S. airpower, linked together by small teams of advisors on the ground, was too much for the Taliban and their terrorist allies. A few months after 9/11, the Taliban and their massed terrorist allies had been driven from every major city in Afghanistan.[474]

Al Qaeda in Iraq (AQI)

The second time the United States confronted the challenge of massed terrorists was in Iraq after the fall of Saddam. The 2003 United States invasion of Iraq brought down Saddam's regime and the country's governing institutions, including the police and the military, collapsed. Immediately after the invasion, the United States was anxious to leave Iraq and rapidly withdrew most of its forces. In the absence of Iraqi and foreign forces, security deteriorated. Prior to the invasion, Saddam had invited foreign jihadis to come and fight the Americans. Thousands answered his call and continued to fight after Saddam's regime collapsed.[475] As a Sunni insurgency developed in western Iraq, jihadi terrorists from all over the Islamic world continued to flow into Iraq. Anbar Province in western Iraq, in particular, became the epicenter of global terrorism. Abu Musab al-Zarqawi gained control of the Sunni terrorists in Iraq, swore allegiance to Osama bin Laden, and made Al Qaeda in Iraq (AQI) the deadliest terrorist organization in the world.[476]

The United States was slow to recognize and respond to the terrorist threat in post-Saddam Iraq, but the worsening security situation forced the George W. Bush Administration to address the threat along multiple lines of effort. One line of effort was to increase the size and sophistication of U.S. CT forces, particularly Task Force 714.[477] Another line of effort was the development of post-Saddam Iraqi security forces. Collaboration with irregular Iraqi forces were another critical element. Variously known as the Desert Protectors, the Anbar Awakening, the Sons of Iraq, among other names, these local forces played a key role in making Iraq inhospitable to massed terrorists. The Iraq Surge also massed U.S. conventional ground forces against these massed terrorists. Finally, U.S. airpower continued to give CT forces escalation dominance even when the terrorists massed to conduct conventional defensive operations, such as during the two battles of Fallujah.[478] Casualties among the CT forces, both those of Iraq and the United States, climbed to alarming levels but, eventually, the massed terrorists were defeated by relentless CT operations. With the terrorists dispersed and AQI defeated in Iraq, the Barack Obama Administration pulled the last U.S. troops out of Iraq and ceased CT operations there in 2011.

In terms of CT technique, the methods that worked in Afghanistan to defeat massed terrorists in 2001 and 2002, massive airpower supporting local allies through a small U.S. ground element, proved inadequate in Iraq between 2003 and 2011. Instead, defeating massed terrorists in Iraq required the United States to employ a massive conventional ground force in the form of the Surge, and also the construction of a powerful unilateral CT element in the form of TF 714. This method was repeated with somewhat less success in the Afghan Surge under President Barack Obama.

Daesh Physical Caliphate

The third post-9/11 instance of massed terrorists came in the form of the Islamic State in Iraq and Syria (ISIS) which we will refer to by its Arabic acronym "Daesh." As the United States completed its withdrawal from Iraq, the so-called Arab Spring revolts swept across the region in 2011. In Syria, the Assad regime responded to protesters in classic authoritarian fashion with a brutal crackdown, which led to a civil war that rages there to this day. The surviving remnants of AQI went to Syria after their defeat in neighboring Iraq. As the civil war began, they joined the anti-regime forces in rebellion, broke with al-Qaeda, and eventually grew into Daesh and declared a new caliphate. By 2014, Daesh and its physical caliphate governed a large area and millions of people in Syria and Iraq. Daesh was the new global leader in terrorism and its caliphate, crossing northern Iraq and southern Syria, was the new center of massed terrorists.[479]

Fortunately for the CT cause, Daesh was so brutal, its ambitions were so vast, and it threatened so many people and nations, that the United States was able to build an enormous coalition to defeat it (incorporating more than 80 different nations and international organizations).[480] In 2014, when the United States began a campaign to defeat Daesh in its physical caliphate, a massive ground presence like the one that defeated AQI was not palatable to either the U.S. government or its regional allies and partners. Instead, the United States reverted to a model that was larger than the tiny ground presence in 2001 Afghanistan, but much smaller than the massive presence that resulted from the Iraq Surge. The overwhelming majority of the anti-Daesh ground forces inside Syria were Syrian irregular forces, under the umbrella of the Syrian Democratic Forces. In Iraq, they were a mix of Iraqi government forces and Shiite militias receiving support from the governments of Iraq and Iran but with some independence from both governments. Once again, U.S. airpower was the critical factor that guaranteed CT forces a firepower advantage in virtually every fight. Progress against Daesh was much slower than it had been in Afghanistan in 2001, but much less costly in money or U.S. casualties than the Iraq Surge. By the end of 2017, with the

liberation of Mosul, Iraq, and Raqqa, Syria, the Daesh physical caliphate was destroyed, and massed terrorists were again defeated and dispersed.[481]

These three cases provide three different U.S.-led, post-9/11 models for defeating massed terrorists: 1) a heavy model relying on a large U.S. ground force, such as the Iraq Surge that defeated AQI; 2) a light footprint model using an extremely small number of U.S. ground forces, such as was used in Afghanistan in 2001 to defeat the Taliban and its terrorist allies; and 3) a medium model using a larger U.S. ground force than in Afghanistan in 2001 employing ground-based firepower like artillery, but a much smaller U.S. ground force than the Iraq Surge. This third model defeated the Daesh physical caliphate between 2014 and 2017. All three of these models rely on overwhelming U.S. airpower.

Two Versions of Partner-Led, U.S.-Enabled CT

There is another successful model for addressing post-9/11 massed terrorists, one which anticipated the Biden Administration's policy of shifting from U.S.-led, partner-enabled operations to partner-led, U.S.-enabled operations. This model was used in Somalia in 2006 and Mali in 2012. In Somalia, in early 2006, the Islamic Courts Union (ICU), a Salafi extremist group with connections to Islamic terrorists, took control of the capital, Mogadishu, and much of southern Somalia. Somalia's neighbors, Kenya to the south and Ethiopia to the west, became alarmed at the direction the ICU was taking Somalia, and the United States became concerned that the ICU was strengthening its ties to Al-Qaeda and would turn Somalia into a safe haven where terrorists could mass. With limited U.S. support, Ethiopian forces swept into Somalia, defeated the ICU, and helped establish a new government in Mogadishu.[482]

A partner-led approach was used again in Mali in 2012, but, this time, the partner was a major Western power rather than a neighboring country. Tuareg tribesmen from Mali had long served in the armed forces of Muammar Qaddafi's regime in Libya. The fall of Qaddafi in 2011 left these heavily armed fighters unemployed, and they went home to northern Mali where they launched an insurrection and quickly drove the government out of the Tuareg region in the north. However, the Tuaregs had allied themselves with Al-Qaeda in the Islamic Maghreb (AQIM) and other jihadi terrorist groups. Once government forces were out of northern Mali, the jihadists turned on the Tuareg leaders and imposed an Islamic extremist government along Al-Qaeda lines and looked to establish a safe haven where terrorists could mass. None of the neighboring

countries could meet this challenge, but, a major Western power, France, was willing and able to step in. With U.S. support, French forces rushed to Mali where they rapidly defeated AQIM forces and restored a level of Malian government control.[483]

The partner-led model was flexible enough to rely on a relatively stable neighboring country, such as Ethiopia, or a major Western power, such as France, to provide the necessary combat power with very limited U.S. assistance. Combined with the heavy, medium, and light options, the Somalia and Mali models of minimal U.S. involvement provide the United States with an impressive array of proven CT techniques for defeating massed terrorists. Unfortunately, none of them are now possible in Afghanistan where terrorists appear to be massing in the 2020s.

The Problem of Massed Terrorists in Afghanistan in the 2020s

The United States has enjoyed consistent success in defeating massed terrorists. From Afghanistan in 2001, to Somalia in 2006, to Iraq in 2007, to Mali in 2012, to Daesh in 2017, terrorists have repeatedly tried to mass in the post-9/11 era. When they have, U.S. CT operations have repeatedly defeated and dispersed them. Unfortunately, two decades of consistent success have induced overconfidence in the West. The August 2021 U.S. withdrawal from Afghanistan, and the concurrent takeover of the country by the Taliban, revived the threat of massed terrorists in Afghanistan. If there were any doubts that international terrorists would return to a Taliban-led Afghanistan, they were dispelled when a 2022 U.S. drone strike in Kabul killed Ayman al-Zawahiri, the leader of al-Qaeda.[484]

None of the proven models for defeating massed terrorists are feasible in Afghanistan in the 2020s. U.S. combat airpower is at the center of the light, medium, and heavy U.S.-led CT models for addressing massed terrorists, and a large, multi-month campaign of airstrikes will not be possible in Afghanistan in the 2020s. Large-scale combat air operations over a landlocked country like Afghanistan require basing and overflight agreements with neighboring countries. Unlike the post-9/11 era, such agreements are highly unlikely. Afghanistan's neighbors are Iran, China, Pakistan, and the central Asian states of Turkmenistan, Uzbekistan, and Tajikistan. Iran will not allow U.S. overflight, and relations with Russia and China are such that they will not grant the United States basing or overflight, or allow the Central Asian states to do so. Pakistan is the only nation currently allowing U.S. overflight to Afghanistan and

thus enabled the killing of Ayman al-Zawahiri.[485] Its national leaders, however, remain distrustful of the United States. Backed up by an increasingly close relationship with China, Pakistan would likely deny overflight for a campaign of airstrikes of the size and duration (thousands of strikes over several months) required to defeat massed terrorists in Afghanistan in the 2020s.[486]

The partner-led, U.S.-enabled model is also infeasible inside Afghanistan in the 2020s because there are no partners who could lead the effort. The same geographic and political challenges that make it impossible for the United States to defeat and disperse massed terrorists in Afghanistan in the 2020s also preclude Western nations, like France or Australia, from leading a CT effort in Afghanistan of the required size and scope. Of Afghanistan's neighbors, only Pakistan has the capability and capacity to defeat massed terrorists in the country. The Pakistani military, however, will never divert the required resources away from the existential threat of India in the east to fight terrorists in the west. Russia, China, and Iran could, perhaps, address this challenge, but prefer to fight terrorists domestically. The recent United States and NATO experience in Afghanistan will almost certainly encourage them to continue their historic practices and avoid large-scale operations inside Afghanistan. The Russian Wagner Group has conducted overseas CT, but it has only done smaller operations where it could turn a profit, removing Afghanistan from consideration.

There are at least 22 different armed groups inside Afghanistan that claim to be operating against the Taliban, but none of these pose a serious threat to the regime or its terrorist friends.[487] For any combination of these groups to eliminate massed terrorists inside Afghanistan, they would need massive U.S. assistance on the scale of 2001, which will not be possible for the reasons described above. Relying on anti-Taliban actors inside Afghanistan is also problematic because the most effective resistance force currently operating there is the Islamic State-Khorasan (IS-K) group, a terrorist organization subordinate to Daesh. In this case, the adage that the enemy of my enemy is my friend does not apply, since success for IS-K is likely to increase, rather than decrease, the terrorist threat to the United States.[488]

The Biden Administration has responded to the threat of massed terrorists in Afghanistan and its inability to address it through any of the successful models described above by developing a new slogan: "over the horizon" CT.[489] The administration claims that the United States can conduct adequate CT operations without a presence inside Afghanistan. The killing of Zawahiri seems to validate this approach, but that was a single strike against a single target. Defeating Daesh's physical caliphate required the

United States and its CT partners to kill tens-of-thousands of Daesh fighters, and the methods that killed Zawahiri are not scalable.

There is another, older model for managing, rather than defeating, massed terrorists. This model saw the United States use diplomatic and economic pressure against Sudan and Taliban-led Afghanistan before September 11, 2001. It succeeded in forcing many terrorist organizations, such as al-Qaeda, to leave Sudan. However, the 9/11 attacks demonstrated its failure to manage the global threat of massed terrorists in Afghanistan in 2001. It is an open question whether non-military pressure on the Taliban regime, infrequent airstrikes, and careful monitoring will be sufficient to manage the threat of terrorists massing in Afghanistan in the 2020s.

Terrorist Dispersal

It is common to hear complaints that terrorists are present in more places than ever before, but terrorist dispersal was an inevitable byproduct of success in defeating massed terrorists.[490] When you hit a grape with a hammer, you destroy the grape but scatter fragments around the room. Similarly, when massed terrorists were crushed in one place, surviving terrorists scattered to many different locations. Whereas the challenge of massed terrorists is a military one with a large role for the armed forces and a small role for police forces and legal systems, that of dispersed terrorists is closer to a law enforcement challenge with a smaller role for military forces and a much larger role for police forces and legal systems.

Three Related Challenges

The challenge of CT operations against dispersed terrorists is really comprised of three related challenges. Each has an analogy in routine law enforcement.

The first challenge is countering specific acts of terrorism. This involves defensive measures such as those used by the U.S. Transportation Safety Administration (TSA) to prevent terrorist attacks on the civilian aviation industry. It also involves offensive measures such as building hostage rescue and rapid reaction forces, and keeping them on alert to respond quickly to terrorist acts. These measures will not keep people from becoming terrorists, or eliminate them other than those caught in the act, but it will mitigate the immediate damage they can do. The law enforcement analogues would be locks and alarm systems to discourage criminal activity, established police presence before crimes are committed, and prompt police response to 911 calls when crimes are in progress.

The second challenge is hunting down individual terrorists, while dismantling and disempowering their organizations. This will not keep people from becoming terrorists, or thwart an ongoing act of terrorism, but it will punish and eliminate known terrorists and disempower or even eliminate the organizations that make terrorists more effective. Examples include killing or capturing individual terrorists, such as Osama bin Laden, confiscating terrorist funds, and arresting people who run safe houses for suicide bombers and otherwise support terrorists without necessarily participating in terrorist violence. The law enforcement analogy here is finding and arresting criminals after they have committed crimes and dismantling organized crime networks.

The third challenge is attacking the root causes of terrorism. This will not thwart an ongoing act of terrorism, or eliminate existing terrorists, but it will decrease the number of people who decide to become terrorists and might decrease the ardor of some existing terrorists. Examples are economic development and political reforms that address some terrorist grievances, as well as deradicalization initiatives to tone down the rhetorical and ideological aspects of terrorist recruiting and motivation. Law enforcement analogues are, among others, jobs programs for at-risk youth, police athletic leagues that give young people better ways to spend their time, and local mentors teaching non-violent dispute resolution.

Jurisdictional Issues

Like law enforcement challenges, the three related challenges in countering dispersed terrorists are complicated by competing jurisdictions with different resources and different laws. We will now consider how jurisdiction impacts each of the three CT challenges posed by dispersed terrorists.

Defensive measures against terrorism vary enormously depending on jurisdiction and are driven by the available resources and the perception of the threat. For example, in Israel, or the Xinjiang region of the People's Republic of China, defensive measures against terrorism are quite extensive since the government has substantial resources and views the terrorist threat as serious. Defensive measures are much less intense where the government feels little terrorist threat (e.g., bus travel inside the United States) or faces severe resource constraints (e.g., most of Africa). The United States offers advice and assistance to foreign partners on defensive CT measures, but their adoption by partners reflects each partner's cost-benefit analysis with limited U.S. ability to influence their decisions. The United States has had better success imposing American standards on air travel since entry can be denied to flights that do not meet these standards even when the departure point is not under U.S. jurisdiction.

Response to acts of terrorism is extremely sensitive to where they occur. For example, when Israeli athletes were taken hostage during the 1972 Munich Olympics, the terrorist act took place inside the Federal Republic of Germany, and the response was handled ineffectively by the appropriate authorities.[491] The situation becomes more complicated when the jurisdiction supports the terrorists rather than the hostages. For example, in 1976, when terrorists hijacked an Air France flight and directed it to Entebbe, the Ugandan armed forces protected the hijackers, and the Israeli rescue force had to overcome both the terrorists and the security forces that had jurisdiction over the site.[492] The United States faced a similar challenge during the Iran hostage crisis in 1980-81. Similar techniques are used in areas where no authority exercises obvious jurisdiction, since outside parties could attack the CT force without consequence. Such was the case in disputed regions in Syria, where the United States has killed various Daesh leaders.[493] With notable exceptions like Entebbe, CT missions inside hostile states or insecure areas have usually been lethal operations, such as the U.S. cruise missile strikes inside Afghanistan and Sudan in 1998, the raid in Pakistan that killed Osama bin Laden in 2011, and the previously mentioned 2022 strike that killed Zawahiri.[494]

In places where there is a clear governing authority, and it is not actively supporting the terrorists, the situation becomes different rather than easier. No nation wants to be responsible for a deadly fiasco like the one in Munich in 1972, but neither do governments want foreigners conducting potentially lethal operations inside their jurisdiction. This has the positive effect of making many nations receptive to advice and training for their own quick-reaction CT forces but also makes coordinating rescues of U.S. citizens held captive overseas a complex activity involving delicate negotiations with the host nation where the pride of the local leadership may exceed their capabilities. Scores of U.S. hostages have been rescued from dozens of countries with little notice from the press or the public, but only after a great deal of work by embassy staff, along with American and local CT forces.[495]

The legal and jurisdictional challenges of defending against terrorist attacks, and managing ongoing acts of terrorism, pale in comparison with eliminating terrorists by killing or capturing them. The jurisdictional challenge of killing terrorists becomes clear when we consider Pakistan's response to the raid that killed Osama bin Laden. Government leaders of Pakistan were furious the United States killed him without prior coordination and, according to one poll, 85 percent of Pakistanis disapproved of the raid being conducted without providing advance notification or warning.[496] [497]

The legal and jurisdictional challenges of capturing terrorists are even bigger

than those involved in killing them. Who has a right to arrest a terrorist, where, and on what grounds? Where can a terrorist be held? How, where, and by whom will the detained terrorist be tried, for what crimes, and based on what evidence? These challenges become even trickier when we consider the supporters of terrorism and the networks that facilitate terrorist activity. Significant new legislation may be required to close loopholes in each country's laws without criminalizing so much legitimate activity that they become counterproductive.[498] All the while, international terrorists and their supporters and networks are actively seeking out the jurisdictions where they can operate with the least chance of capture and prosecution.

The challenges of legal reform, detaining terrorists, and prosecuting them are not limited to struggling countries with weak institutions. In the United States, CT legislation such as the so-called Patriot Act became highly controversial.[499] Scandals and controversies surrounding U.S. detention facilities at Guantanamo Bay and Abu Ghraib demonstrate the challenges of detaining accused terrorists.[500] The controversy over U.S. military tribunals to prosecute terrorists illustrates the challenges of dealing with terrorists through a legal system.[501] Given the difficulties the United States has encountered, it is hardly surprising that other nations also struggle to meet these challenges.

The challenge of enforcing long-term detention is probably the most serious CT challenge. Daesh was built out of terrorists detained by the United States, and either later released or broken out of prison by Daesh assaults.[502] The Taliban resurgence in Afghanistan was similarly fueled by prison breaks and the Trump Administration's decision to force Kabul to release thousands of detainees. One of the top priorities of many terrorist organizations is breaking their detained members out of prison. Preventing prison breaks and keeping terrorists detained must be a top priority in any CT effort, but it is too often neglected.

If the challenge of managing the long-term detention of terrorists seems difficult, managing their family members is even harder. Are the wives and children of terrorists victims or future terrorist threats? For example, thousands of people who lived under Daesh control are currently detained in the al-Hawl refugee camp in Syria. Many of them experienced terrible mistreatment at the hands of Daesh, but some mistreated others. While the children have not committed any crimes yet, Daesh calls them the "Cubs of the Caliphate" and counts on them to become the next generation of terrorists and suicide bombers.[503] How can a non-state actor, like the Syrian Democratic Forces (SDF) that runs the al-Hawl camp, prevent these children from following in their

fathers' footsteps and becoming terrorists themselves while also meeting all the other challenges the SDF faces, including a threatened invasion by Turkey?[504]

Countering terrorism by addressing root causes is likewise enormously challenging. The grievances that cause people to become terrorists are typically the result of complex and interrelated political, economic, and social systems that are not easily reformed. Proposed reforms are likely to be opposed by powerful interests that benefit from the current system and prefer to address the symptoms of violent terrorism and ignore the underlying causes. Every day, around the world, U.S. embassy staff advocate for local political, economic, and social reform. Their achievements are rarely noted and hard to measure. Progress in the information space is even harder to measure and even less likely to be noticed. However, implementing democratic reforms and publicizing those reforms are critical to long-term, democratic success against the terrorist threat and in strategic competition against authoritarian state rivals.

As this section has demonstrated, terrorist dispersal poses a wide variety of different and difficult challenges. Assisting partner nations in meeting these challenges requires patience, persistence, and creativity from the entire interagency community, in addition to all possible help from like-minded governments, civil society, and non-governmental organizations. As suggested at the beginning of this chapter, many of these efforts are better seen as strategic competition and democracy promotion through government reform, with benefits in mitigating terrorism, rather than primarily as CT measures.

The Challenge of Conducting and Countering State-Sponsored Terrorism

Terrorist organizations backed by nation-states have the potential to be the most dangerous VEOs since states can provide them with enormous resources. State-sponsored terrorism exists because it benefits both parties.[505] States offer terrorists technology, training, money, advice, sanctuary, and myriad other benefits that the terrorists and their organizations need and cannot necessarily find on their own. By retaining their status as independent organizations, and not official representatives of states, sponsored terrorists also retain more autonomy and control than they would enjoy as members of the military or intelligence services of the sponsoring state. States, in turn, gain the ability to attack their enemies indirectly while denying responsibility for their actions and, ideally, evading retaliation from the target of the attack. States can also gain the benefits of the terrorist acts without having to provide all the funding

needed by the sponsored terrorist organization. For example, Hezbollah in Lebanon receives substantial Iranian funding but also has its own formidable sources, giving Tehran access to operations at a significant discount compared with using its own forces.[506]

From the perspective of massed terrorists, a state sponsor provides a robust military force that can turn any attempt to defeat massed terrorists into an expensive and extended period of large-scale conventional combat operations against the state sponsor. From the perspective of dispersed terrorists, state sponsors can provide technology, training, and planning to enable more effective operations, conceal and protect individual terrorists from retaliation, and provide ideological and media support on a scale very few non-state actors can match.

In addition to the advantages already listed, a state-sponsored terrorist organization immediately gains another center of gravity and set of interests associated with the sponsor in addition to its own. For example, Hezbollah has a center of gravity and a set of interests associated with its popular base among the Shiites of Lebanon, but it also has an additional center of gravity and a set of interests associated with its sponsor, the Islamic Republic of Iran. The new interests and centers of gravity make sponsored terrorist organizations more complicated and harder to predict than they would be without a sponsor.[507]

Since the United States does not sponsor terrorists, Americans rarely consider how challenging and risky it is to do so. Sponsoring terrorists is challenging because terrorists and other revolutionaries are, almost by definition, bad house guests, unsatisfactory employees, and not team players. They are rebels who do so, at least in part, because they prefer violence over compromise and overvalue their own opinions compared to those of others. They are also captivated by grandiose visions of dramatically changing the world through their individual acts of spectacular violence. They think they are world historic figures who have no business sweeping floors, filing expense vouchers, or doing any of the mundane tasks required to make organizations function. Instead, they love to quarrel over who is the most correct in their thoughts and actions and find fault with the views and policies of those who are trying to lead them.

The risks of sponsoring terrorists are even greater than the challenges. For example, the 9/11 attacks were both the most spectacular terrorist acts ever committed and a nightmare scenario for state sponsors of terrorism. Consider the attacks from the point of view of al-Qaeda's sponsor, the Taliban, as well as the Taliban's sponsor, the government of Pakistan. Mullah Mohamed Omar and the Taliban thought of themselves

as the sponsors and protectors of Osama bin Laden and al-Qaeda. They welcomed bin Laden and his colleagues when Sudan evicted them and Osama bin Laden swore personal allegiance (*bay'ah*) to Mullah Omar, indicating he and his organization were subordinate to the Taliban.[508] The Taliban certainly expected bin Laden to obey Mullah Omar and avoid doing anything contrary to their interests.

For its part, the government of Pakistan devoted a great deal of effort to supporting the Taliban and enabling them to take and hold power in Afghanistan before 9/11.[509] As sponsor and patron of the Taliban, Pakistan expected the Taliban to advance Pakistani interests and avoid doing anything contrary to Pakistan's interests.

Despite these sponsorship relationships, in 2001, bin Laden and al-Qaeda were plotting the 9/11 attacks on the United States without consulting Mullah Omar, the Taliban, or the Pakistani government. While al-Qaeda achieved its epic success on 9/11, the result for its Taliban sponsors were catastrophic. Mullah Omar lost his position as head of state and appears to have died under house arrest in Pakistan.[510] The Taliban were driven out of Afghanistan and did not retake Kabul for twenty years. In the Taliban's generation-long war to recapture Kabul after 9/11, tens of thousands of fighters lost their lives, and even more were wounded and dispossessed. For the Taliban, the 9/11 attacks were the worst disaster in the thirty-year history of the organization, one imposed on them by their supposed al-Qaeda subordinates. Like the Taliban, the government of Pakistan would never have approved of the 9/11 attacks if they had known about them in advance. The consequences were disastrous, including attacks in Pakistan leading to more than 70,000 deaths, economic losses in excess of $100 billion, and internal social and political disruptions that set back Pakistani development for years.[511] For the government of Pakistan, 9/11 was the worst disaster since it lost half the country to Bangladeshi independence in 1972, and Pakistanis consider themselves the biggest long-term victims of 9/11.[512]

Iran's handling of al-Qaeda, post 9/11, demonstrates a sophisticated understanding of the risks and rewards of state sponsorship of terrorism. On the one hand, to preserve the al-Qaeda threat to the United States, Iran has protected al-Qaeda leaders from American attacks. In fact, Sayf al-'Adl, the most likely current leader of al-Qaeda, lives in Iran.[513] On the other, Iran has attempted to limit al-Qaeda activity that can be traced back to Iran to avoid suffering the sort of damage the Taliban and Pakistan suffered from their sponsorship.[514] This has the paradoxical result that al-Qaeda leadership inside Iran is simultaneously less effective than if it were outside the country but also much harder to remove.

U.S. strategic competitors in Moscow, Beijing, and Tehran have long histories of state sponsorship of terrorism. Their broader irregular warfare (IW) efforts are covered elsewhere in this volume, so we will tightly limit the discussion here to their sponsorship of terrorist organizations. The Union of Soviet Socialist Republics (USSR) came to power through a communist revolution. Throughout its history, the USSR supported the strategic goal of spreading its revolution globally. In pursuit of this goal, the USSR supported a wide array of governments, communist parties, insurgencies, and terrorists. However, with the dissolution of the USSR, leaders in Moscow stopped funding leftist terrorists. The leaders of the successor to the USSR, the Russian Federation, seem content with the level of deniability they receive from covert operations, such as assassinations and sabotage in western Europe conducted by its own forces, including the notorious GRU Unit 29155.[515] Rather than sponsoring terrorists, Russia has used private military companies like the Wagner Group, to put itself at the forefront of a particularly violent version of authoritarian counterterrorism.[516] However, given its highly disruptive role in the international system, Russia might reconsider its choice not to sponsor terrorists. Should it do so, Russian sponsorship could spectacularly increase the threat posed by a terrorist organization.

The People's Republic of China (PRC), initially under the leadership of Mao Zedong, sponsored communist terrorist organizations around the world.[517] After Mao's death in 1976, the PRC abandoned its pursuit of a global Maoist revolution and stopped being a major state sponsor of terrorism. The PRC leadership seems unlikely to change this policy in the foreseeable future because the Chinese Communist Party, under Xi Jinping, has focused primarily on control and stability, and, as described above, terrorist groups are hard to control and often destabilizing.

While Moscow and Beijing currently prefer covert operations by their own forces, Tehran has long been the world's leading state sponsor of terrorism.[518] Iranian sponsorship has made Hezbollah the most powerful terrorist organization in the world, often referred to as "the A-team of terrorists."[519] Hezbollah has advanced its own interests as well as those of Iran through attacks on Israel and operations in Lebanon.[520] However, in Syria, Hezbollah placed Iranian interests ahead of its own preferences and sent tens of thousands of fighters to defend the Assad regime.[521] Hezbollah and other Iranian-sponsored groups (Hamas, Houthis, Shiite militias in Iraq, etc.) pose a continuing threat to U.S. interests in the Middle East and elsewhere.[522] Identifying and countering these threats will be an ongoing challenge in the future as Tehran employs its terrorists proxies in its strategic competition against the West.

Terrorist Franchising

One of the unique features of terrorism in the 21st century is the terrorist franchising networks provided by al-Qaeda and Daesh. In some ways, these terrorist franchising networks act like state sponsors by providing international expertise and resources to local terrorists.[523] The existence of Daesh speaks to the risks and challenges of sponsorship/franchising since Daesh started out as subordinate to al-Qaeda but is now in competition with it for leadership of the global Salafi jihadist movement and fighting against it in Afghanistan, the Sahel, and elsewhere.

While there are important ideological and methodological differences between the two, they have converged on a model where affiliates, such as al-Shabab and Islamic State in Khorasan (IS-K), are subordinate to the central leadership but have a high degree of autonomy in their day-to-day operations. In return for subordination to al-Qaeda or Daesh, local jihadis get the traditional advantages of franchisees, such as international brand recognition, assistance acquiring and operating new technology, and funding provided by the more successful affiliates to new and struggling affiliates.

CT forces benefit from the infighting between the two groups and their affiliates, and those benefits include not only the casualties they impose on each other, but also their willingness to provide intelligence on each other. Most importantly, the existence of two competing visions and networks for violent Salafi jihadis calls into question the validity of each vision.

Unfortunately, the competition between al-Qaeda and Daesh also pushes them to generate new affiliates as quickly as possible in any region that offers the potential for jihadi terrorism. This puts international terrorist resources into the hands of local malcontents sooner than might have been the case without the competition between al-Qaeda and Daesh. Furthermore, the defeat of the local affiliate of one sponsor, if it is not accompanied by successful reforms to eliminate the root causes of local terrorism, can create an expansion opportunity for the other sponsor. For example, the government of the Philippines, with U.S. assistance, achieved significant success against al-Qaeda affiliated terrorists between 2002 and 2015. These victories led the United States to end its main CT effort there, Operation Enduring Freedom-Philippines, in 2015 and study it as an example of a successful CT operation.[524] However, after Manila subsequently reneged on parts of the peace agreement with the terrorists, Daesh made itself an attractive partner to Philippine jihadis through its 2014 successes in Iraq and Syria, and the destruction of the massed terrorists in the physical caliphate sent surviving terrorists

elsewhere. The result was the revival of jihadi terrorism on the Philippine Island of Mindanao and the five-month-long battle of Marawi in 2017.[525]

Hamas and 7 October 2023 as a case study

On October 7, 2023 Hamas—the terrorist group that became a major recipient of Iranian support when it took control of the Gaza Strip in 2006-2007—launched a massive attack on Israel. What does this recent, spectacular terrorist attack tell us about our concepts of Massed Terrorists, Terrorist Dispersal, State- Sponsored Terrorism, and Terrorist Franchising?

Massed Terrorists: Hamas rule over the Gaza Strip is a classic example of massed terrorists and the risks they pose. It did not attract much U.S. attention, since Hamas did not threaten the U.S. homeland, and Israel, which was the target of Hamas terrorism, was confident that it had the threat under control.[526] Unfortunately, Israel was mistaken, and we were reminded that massed terrorists are extremely dangerous and hence that we might be facing greater risks than we think from terrorists massing in Afghanistan. At the time of this writing (February 2024) it appears that Israel will be less successful in eliminating massed terrorists in Gaza[527] than the U.S. and its allies were in the cases described earlier in this chapter. This relative lack of success makes sense given Israel's inability to find local allies in Gaza[528] comparable to the Northern Alliance in Afghanistan or the Syrian Democratic Forces in Syria.

Terrorist Dispersal: addressing the challenge of massed terrorists usually kills and captures thousands of terrorists, but also results in the surviving terrorists scattering to distant places to continue their activities in a dispersed rather than massed approach. The Israeli operations in Gaza seem unlikely to follow this pattern because the borders of Gaza are tightly controlled and large numbers of terrorist are unlikely to escape Gaza to continue their activities elsewhere. However, some of the key themes from that section still apply to Hamas and the 7 October attack. For example, the challenge of successful long-term detention of terrorists is front and center since key Hamas leaders, like Yahya Sinwar, are convicted terrorists who were released from Israeli prisons and the 7 October attack was specifically designed to capture Israelis who could be exchanged for imprisoned Hamas terrorists.[529] The continuing fighting between Israel and Hamas also reinforces the point that addressing root causes of terrorism can be extraordinarily difficult. Seemingly every U.S. President since the creation of Israel has tried to reconcile the Israelis and Palestinians, but after 7 October, it appears that neither side is close to reconciliation.

State Sponsorship: the October 7, 2023, attack is a sparkling example of the value of state sponsorship of terrorism to both terrorists and their sponsors. Hamas achieved its most spectacular success on 7 October, and no one believes Hamas could have achieve this without Iranian support.[530] Iran, via Hamas, was able to harm Israel to the greatest degree that is has so far achieved by sponsoring a terrorist proxy group, and the reliance on proxies has enabled Iran to evaded direct retaliation against Iranian territory by either Israel or the U.S. while its proxies attack both Israel and U.S. interests.[531] Of course, state sponsorship is not risk free. The 7 October attacks put Iran and its proxies at greater risk of attack from the U.S. and Israel and it seems likely that the ongoing fighting will leave Hamas, and perhaps other Iranian proxies, weaker than they were before October 2023.

Terrorist Franchising: Hamas, and other terrorist groups in Gaza, could have affiliate themselves with Daesh or al-Qaeda, as the Daesh affiliate in the Saini did, but they have chosen not to.[532] This is a good sign since it indicates that, at least in the Sunni Arab world, affiliation with either Daesh or al-Qaeda is even less appealing than affiliation with the Shia Persians of Iran. It might be too early and optimistic to suggest that Daesh and al-Qaeda are losing their luster in the Arab world, but the clear preference of terrorists in Gaza is Iranian state sponsorship rather than becoming franchisees under Daesh or al-Qaeda.

The Hamas attack on 7 October 2023 was an attack on Israel, not the United States, and the subsequent war in Gaza has been fought by Hamas and Israel with the U.S. in a supporting role and not a direct participant. However, the attack reinforced the themes discussed in the rest of this chapter by demonstrating: (a) the risks associated with massed terrorists; (b) the challenges of incarcerating terrorists for long prison terms; (c) the challenges of addressing the root causes of terrorism, and (d) the effectiveness of state sponsorship of terrorism. Iran has also used the Israeli response to the 7 October attacks as an excuse to employ its Hothi and Iraqi terrorist proxies against U.S. assets and presence in the region. If these attacks prove successful in advancing Iranian interests in strategic competition against the United States, Russia and the PRC might reconsider their current preferences and return to their Cold War policies of sponsoring terrorist organizations.

Conclusion

Terrorism and counterterrorism have been with us for centuries and are vital parts of irregular warfare. While terrorists in some far-off country may not be a threat to the U.S. homeland, how the local government conducts counterterrorism is a key aspect

of governance and critical to whether that nation becomes more democratic or more authoritarian and, hence, are critical to the current era of strategic competition.

The United States and its partners have repeatedly defeated massed terrorists since 9/11, but the terrorists currently massing in Afghanistan will not be defeated and must instead be managed. Dispersed terrorists will remain a chronic problem that must be addressed holistically, with as many partners as possible and a focus on democracy promotion and governmental reform.

Aside from Iran, few states are providing substantial sponsorship to terrorist organizations, but the franchising model implemented by al-Qaeda and Daesh is providing many of the benefits of state sponsorship to local terrorists throughout the Islamic world. The management of these diverse terrorist threats will continue to be a major diplomatic, military, law enforcement, and governance challenge for the United States and its partners for the foreseeable future.

About the Author

Dr. Thomas Searle is a retired U.S. Army Special Forces officer, a noted scholar of special operations, and the author of an influential theory of special operations. In uniform, he served in many counterterrorism joint task forces in Afghanistan, Colombia, Iraq, the Philippines, and elsewhere. He was handpicked by Admiral McRaven to write the official, classified history of how the Find, Fix, Finish, Exploit, Analyze, Disseminate (F3EAD) process was developed and how its full implementation and institutionalization transformed U.S. and partner counterterrorism operations and organizations. As a civilian war planner at U.S. Special Operations Command, Dr. Searle worked in close collaboration with the Trump and Biden Administrations' U.S. National Security Council and with U.S. allies and partners to manage and mitigate global terrorist threats in an era of strategic competition, including implementation of the concept of "over the horizon counterterrorism." Dr. Searle also helped develop, monitor, assess, and refine the U.S. Global Campaign Plan to Counter Violent Extremist Organizations (formerly the Global War on Terror) and synchronize its implementation by U.S. and partner forces around the globe. Dr. Searle is currently a Professor of Interdisciplinary Studies at the Joint Special Operations University.

Discussion Questions:

1. This chapter argues that counterterrorism (CT) is central to strategic interstate competition. Why does the author think this is true? Why do you agree or disagree? How would it change the U.S. approach to CT if the U.S. Government agreed with the author?

2. This chapter does not define terrorism or counterterrorism, but the extensive description of the challenges of defeating massed and dispersed terrorists implies a definition of terrorism and counterterrorism. How would you state the implied definition of terrorism or terrorists contained in this chapter? How would you state the implied definition of counterterrorism? In what ways do you agree or disagree with these definitions?

3. In U.S. military doctrine, mass is a principle of war, but the term "massed terrorists" is new. How do massed terrorists differ from dispersed terrorists? Is the challenge of massed terrorists an irregular warfare challenge, or is it a regular warfare challenge, like conquering a nation state and defeating its armed forces?

4. The United States has traditionally chosen not to sponsor and support terrorist groups. Should the United States consider changing that policy? If not, why not? If so, then why should the policy change, and which sorts of terrorist groups should the United States sponsor and support? (For example, if the threat from Daesh increases, should the United States facilitate counter Daesh operations by al-Qaeda as it has previously facilitated Taliban operations against IS-K)?

5. Do you think the franchising model developed by al-Qaeda and Daesh can be imitated by other terrorist causes such as white nationalism?

Recommended Reading:

- Terrorism has generated an enormous literature and the suggestions below will merely start the practitioner on a long road of study. These books will give the practitioner some basic understanding of the challenges involved in dismantling the violent extremist organizations that conduct terrorism.
- Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, (New York: Portfolio, 2006). In the terms used

by this chapter, dispersed terrorists are generally following the starfish model while massed terrorists are following the spider model. *The Starfish and the Spider* was enormously influential after the 9/11 terrorist attacks since it looked like the starfish model was nearly invincible and the spider model was doomed. However, when Daesh decided to transform itself from a starfish into a spider it forced us to consider why starfish might want to become spiders and why the spider model persists despite its vulnerabilities.

- Orrin Deforest and David Chanoff, *Slow Burn: The Rise and Bitter Fall of American Intelligence in Vietnam,* (New York: Simon and Schuster, 1990) and Stuart Herrington, *Stalking the Vietcong: Inside Operation Phoenix: A Personal Account*, (Presidio Press, 2004). These help to understand how an earlier generation identified and rolled up violent clandestine networks using filing cabinets, index cards, still photographs, and zero computers. With facial recognition, full-motion video, networked computers searching enormous databases, etc., you should be able to roll up networks twice as fast if you master the basics the way Deforest and Herrington did.
- Gen. Stanley McChrystal, *My Share of the Task*, (New York: Penguin, 2014) and Gen. Stanley McChrystal, *Team of Teams*, (New York: Penguin, 2015). In Iraq, General McChrystal recreated the Vietnam-era Phoenix Program. With better technology and a more permissive environment, McChrystal devoured enemy networks at a pace Deforest and Herrington could only dream of. In the process, McChrystal became a CT legend.
- There are a wide variety of web sites tracking terrorist activity. The sites below are good places to start if you want to monitor future developments in the terrorist threat, but they merely scratch the surface of available resources.
- The U.S. National Counterterrorism Center has a website at: https://www.dni.gov/index.php/nctc-home. Some of its resources, such as the weekly Counterterrorism Digest, are only available over government systems.
- The Critical Threats project at The Institute for the Study of War produces a "Salafi-Jihadi Movement Weekly Update". Here is a link to the one from March 22, 2023 which will help you find others. https://www.understandingwar.org/backgrounder/salafi-jihadi-movement-weekly-update-march-22-2023
- For historical data, a good place to start is the Global Terrorism Database maintained by the University of Maryland: https://www.start.umd.edu/gtd/.

China's Little Blue Men

Tuan N. Pham

ABSTRACT

Dozens of Chinese fishing boats curiously loiter for weeks in disputed or sensitive maritime areas: just offshore of Japan-administered Senkaku Islands in the East China Sea, Philippine-occupied Thitu Island in the South China Sea, Singapore-hosted U.S. Seventh Fleet Logistics Command (U.S. regional logistics hub), U.S. Naval Base Guam (U.S. regional naval base of growing operational importance) in the Marianas Islands, and/or U.S. Naval Base Pearl Harbor (U.S. Pacific Fleet Headquarters) in the Hawaiian Islands. So, are these uninvited interlopers just innocuous Chinese commercial fishermen coincidentally (and perhaps illegally) fishing in distant foreign waters? Or, perhaps more alarmingly, is China's Maritime Militia surreptitiously collecting intelligence and preparing to conduct irregular warfare actions in support of People's Liberation Army operational plans or contingency operations? Under these ambiguous gray zone conditions, and through the hazy lens of great power confrontation in the 21st century, how could and *should* local authorities respond, especially during times of increasingly high tensions and looming regional conflict? The consequences of their action or inaction underscore the political, diplomatic, legal, and military dilemmas these Chinese "little blue men" present to U.S. and allied policymakers, military commanders, and maritime constabulary forces.

Introduction

China's little blue men, formally called the People's Armed Forces Maritime Militia (PAFMM) by the U.S. Department of Defense (DoD) and intelligence community, are a Chinese government-sponsored "armed" fishing fleet under the direction and guidance of the People's Liberation Army (PLA) to conduct the "people's war at sea."[533] China's Maritime Militia (CMM) augments the more powerful PLA Navy (PLAN) and China's Coast Guard (CCG) by overwhelming the adversary with swarms of civilian fishing boats that are backed by PLAN and CCG vessels tactically positioned in escalatory concentric rings, essentially security cordons, like leaves of a cabbage (i.e., "cabbage tactics").[534] The combined maritime force collectively establishes a de facto Chinese operating presence in disputed maritime areas, legitimizing Beijing's expansive sovereignty claims while delegitimizing those of other nations through the conduct of legal warfare (lawfare). China seeks to asymmetrically change the facts on the ground in the East and South China Seas (ECS/SCS) by gaining and maintaining operational control and administrative jurisdiction over the Senkaku Islands, Spratly Islands, and other contested maritime areas. China's goal is to make counter claims moot through effective control of the international waterways (imposing a fait d'accompli). The cornerstone of this lawfare strategy consists of gray zone operations to undermine international laws and norms through: the reconstitution of the United Nations Convention on the Law of the Sea; a redefinition of freedom of navigation; land reclamation and artificial island-building efforts; instantiating a norm of bilateral resolution of maritime disputes; and a selective interpretation of, and compliance with, maritime laws and customs as well as international tribunal decisions.[535] These gray zone operations are purposely intended to "win without fighting," in accordance with Sun Tzu's core warfighting principle elucidated in his *Art of War*.

It is therefore instructive to further explore the following questions to look beyond how the Chinese Communist Party (CCP) employs the CMM as a proxy for economic and political warfare, and then predict the direction and shape of the CMM's activities in the future, both through the framework of irregular warfare and within the context of great power confrontation in the 21st century. What is the CMM and its affiliation with the Chinese state? When and why did China establish the CMM, and how did it develop over the years into its current unconventional manifestation? What does the CMM's unorthodox history suggest about its future asymmetric operations and activities? How does the CMM challenge longstanding maritime laws and customs, and what are the strategic, operational, and tactical implications thereof? How can the United States and its allies and partners deal with this ever-evolving maritime component of irregular warfare?

Nature and Character of China's Maritime Militia

Although the CMM is an open secret within China, its government affiliations, funding sources, organizational structure, administration, strategic intentions, operational plans, and tactical actions are still not well understood by foreign observers outside of the country. The CMM's strength, and therefore value, lies in its enduring nature and fluid character, shrouded in ambiguity and deniability. The CMM operates and thrives in the muddy arena that is irregular warfare. So, it is not surprising that U.S. intelligence analysts, academic researchers, legal scholars, and policy advisors view and describe the CMM through their discrete organizational prisms, cultural lens, and personal biases. Their individual analyses are akin to blind men describing different parts of an elephant.

The Defense Intelligence Agency (DIA) characterizes the CMM as a, "maritime subset of China's national militia that plays a major role in coercive activities to achieve Beijing's political goals without fighting, and part of a broader Chinese military doctrine that states confrontational operations short of war can be an effective means of accomplishing political objectives."[536] Think tank pundits from the Center for Strategic and International Studies (CSIS) describe the CMM as a, "force of vessels ostensibly engaged in commercial fishing but which in fact operate alongside Chinese law enforcement and military [PLA] to achieve Chinese political [and military] objectives in disputed waters."[537] Andrew Erickson and Conor Kennedy from the U.S. Naval War College (USNWC), who conducted the earliest, most comprehensive, and seminal academic research on the CMM, similarly define the entity as a "state-organized, -developed, and -controlled force operating under a direct military [PLA] chain of command to conduct Chinese state-sponsored activities…defend and advance China's maritime territorial claims, protect maritime rights and interests, and support the PLAN in wartime."[538] The Congressional Research Service (CRS) classifies the PLAN, CCG, and CMM as the largest maritime forces in the Indo-Pacific, and indeed the world, that regularly conduct maritime sovereignty assertion operations.[539] All in all, the CMM enables China to redefine the rules of freedom of navigation in its favor, better assert its expanding maritime territorial claims, secure more vital resources, and extend further its global economic and political reach.[540]

James Kraska and Michael Monti, also from the USNWC, who completed the first legal analysis of the CMM, astutely warn of its, "blurring beyond recognition the [legal] line between civilian fishing vessels and naval functions."[541] They further assert that the CMM conducts a "people's war at sea" by exploiting the seam in the established

law of naval warfare which shields civilian fishing boats from capture or attack unless integrated into the enemy's naval force. The legal ramifications are, therefore, quite profound. The CMM blurs the time-honored legal definitional lines between civilian vessels and warships [the principle of distinction], as laid out by the U.S. Supreme Court's ruling on *Paquete Habana* in 1900: "By an ancient usage among civilized nations, beginning centuries ago and gradually ripening into a rule of international law, coastal fishing vessels pursuing their vocation of catching and bringing in fresh fish have been recognized as exempt, with their cargoes and crews, from capture as prize of war."[542] That being said, although the established law of naval warfare protects civilian fishing boats from capture or attack during armed conflict, warships may do so if the civilian vessels engage in or support naval functions. Actions that are easier said than done. When it comes to the CMM, it is quite challenging to distinguish between legitimate civilian fishing boats and those integrated into the PLAN as an auxiliary naval force. CMM operations and activities consequently threaten to upend centuries of enduring maritime law, and afford the PLA with a cost-effective force multiplier that creates challenging legal, political, and operational dilemmas for any adversary.[543]

Taken together, the above CMM characterizations give a deeper understanding of this complex, unorthodox, and opaque paramilitary force that provides Beijing with asymmetric advantages in the contested maritime domain, with the potential to further its national goals and strategic ambitions. Hu Bo, the Director of the Center for Maritime Strategy Studies at Peking University, takes an opposing viewpoint. He contends that Chinese local governments and media wanting to highlight CMM's achievements, and certain U.S. scholars overstating the "China Threat" without substantiating academic evidence, deliberately overhype the number, role, and influence of these forces. He also asserts that the strategic significance of the CMM is in decline, with its role progressively limited.[544] Nevertheless, despite these differences of opinion, the aggregate debate provides context to, and sets the stage for, an informed discourse on when and why China created the CMM and how it developed over the years to its current unconventional manifestation.

History of China's Maritime Militia

Derek Grossman and Logan Ma of the RAND Corporation provided one of the best historical accounts of the CMM in their 2020 treatise, "Short History of CMM and What It May Tell Us." They traced the evolution of the CMM from its humble roots as revolutionary maritime militiamen, to its modern incarnation as nationalistic little

blue men conducting a "people's war at sea," answering the key questions of what, when, where, why, and how.[545]

Revolutionary Maritime Militiamen (1950-1974)

Following the end of the Chinese Civil War, and the founding of the People's Republic of China (PRC) in 1949, the fledgling CCP established the CMM to counter the frequent incursions of Chiang Kai-shek's Nationalist Forces into Chinese coastal waters from Taiwan. Although China possessed a quasi-maritime militia prior to 1949, it was the CCP that subsidized, and the PLA that professionalized, the CMM. The CCP and PLA transformed the CMM from a disparate and disorganized local coastal force into a homogenous and organized national maritime force. This force was tasked and equipped to advance China's maritime interests as the supporting "Third Sea Force" tethered to the PLAN (which was founded in 1949) and then later to the CCG (formed in 2013 from the maritime branch of the People's Armed Police Border Security Force and other maritime law enforcement agencies). The first documented involvement of the CCP in the organization, administration, and operations of the CMM was in the early 1950s, when the Chinese government collectivized local fisheries, demarcated fishing areas, imposed fish catch targets, and enforced fishing regulations. During the early 1960s, the PLAN trained the maturing CMM to conduct defensive operations against the Nationalist Forces' harassment of local Chinese commercial shipping. By 1965, Chinese state-run media formally referred to the CMM as a maritime militia supported by the PLAN, itself a brown-water navy only capable of operating closer to the coast or in interior bodies of water. The PLAN also established militia schools to train the CMM in basic navigation, communications, weapons, and engineering.[546] The interlocking administrative and operational relationships between the supported CMM and supporting PLAN aligned well with Mao Zedong's central "People's War" doctrine.

Collectivization and Soviet naval doctrine drove the rise and guided the evolution of the CMM during the height of the Cold War (1950-1970). First, as part of the country's socio-political embrace of Marxism-Leninism, Mao zealously implemented collectivization across Chinese society. He forcibly collectivized coastal fisheries as part of a national campaign to galvanize and rebuild the country after the devastating experience of the Chinese Civil War. Second, Beijing's close relationship with Moscow in formulating its early maritime strategy influenced the missions and operations of the CMM, particularly the Soviet "Young School" naval concept, which asserted that a land-centric power should nevertheless commit resources to defend its vulnerable

coastlines and project maritime power on the high seas. A focus on coastal defense made more practical sense to the then-CCP. The cost of building and maintaining a large fleet of naval combatants, such as capital ships, was simply too high for a developing nation still preoccupied with events on land.[547] Mao, therefore, directed national efforts inward to consolidate the CCP's power base, unite and indoctrinate the Chinese people in Communist ideology, rebuild and transform its devastated economy, and implement the (ultimately disastrous) Great Leap Forward campaign (1958-1962) and Cultural Revolution movement (1966-1976).

But then, in 1978, after the death of Mao, Deng Xiaoping (the "Architect of Modern China," as he came to be known) opened the country to the West, abandoned failed Soviet-style economic policies, launched a series of market-economy reforms, and set in motion China's meteoric economic rise that uplifted hundreds of millions out of poverty. This unprecedented economic prosperity, fueled by a burgeoning maritime trade, marked a turning point in Chinese national strategy. The CCP now saw the strategic imperative for a blue-water navy that could: safeguard its critical sea lines of communications; protect its expanding maritime interests; exert global influence; maintain its maritime sovereignty and territorial integrity; and, most importantly, sustain its economic growth and development, and, by extension, strengthen its political legitimacy to govern the country and ensure the survival of the state with the CCP as its sole ruling authority. The PLAN answered the strategic call and embarked on a bold arms buildup during the 1980s to become a regional naval power, and build a green-water navy that could operate in the littoral zones and surrounding marginal seas, transitioning to the supported First Sea Force tethered to the CMM and later the CCG.[548]

As China became more prosperous, its maritime interests grew along with its concomitant strategic aspirations. Under Xi Jinping, lauded as the People's Leader (a title held previously by Mao), the CCP discarded Deng's iconic "hide strengths and bide time" policy dictum and embraced "Xi's Thought on Socialism with Chinese Characteristics for a New Era" and the ambitious and expansive grand strategy for national rejuvenation (colloquially dubbed the Chinese Dream).[549] In other words, a revisionist and revanchist China seeks to displace the United States as the pre-eminent global power across the diplomatic, information, military, and economic domains, and, in effect, erase the historical and cultural stigma of the "century of humiliation" that occurred under colonialism and restore the Middle Kingdom to its rightful place in the world by 2050. The PLAN, accordingly, expanded and modernized during the 2010s

into a global naval power, becoming a blue-water navy capable of projecting maritime power worldwide, and challenging the U.S. Navy for global maritime superiority.

The PLAN is currently the largest navy in the world by size, and rapidly closing the capability gap with its rival, the U.S. Navy. The PLAN operates a battle force of about 340 ships and submarines, including approximately 125 major surface combatants, and is expected to grow to 400 ships in the next two years.[550] As for the CCG and CMM, both have become the largest coast guard and maritime militia, respectively, in the world by size. The CCG operates 225 vessels of 500+ tons, capable of operating offshore, and with another 1025 smaller vessels confined to closer waters, for a total 1275+ vessels. The CCG can conduct extended offshore naval and law enforcement operations well beyond the 200 nautical mile Exclusive Economic Zone in a number of disputed and contested maritime areas, including the enforcement of China's sovereignty claims.[551] The CMM operates 4600+ fishing boats, but this number is a conservative approximation, and could in fact be much higher considering that China boasts the world's largest fishing fleet (estimated at 564,000 fishing boats as of 2022).[552] The CMM can also "show the Chinese flag" across the globe, and conduct a wide range of naval and law enforcement missions in support of the PLAN and the CCG, including maritime sovereignty assertion operations.[553] Altogether, the PLAN [First Sea Force], CCG [Second Sea Force], and CMM [Third Sea Force] constitute the most powerful combined maritime force in the world, in terms of aggregate size, capability, and capacity.

Nationalistic Little Blue Men (1974 to present)

Through the years, CMM incrementally added on to its roles and responsibilities in the areas of maritime rescue, combat operations, anti-smuggling, and, eventually, sovereignty enforcement. In 1974, CMM played a pivotal, supporting role in the seizure of the disputed Paracel Islands from what was then South Vietnam. Chinese civilian fishing boats covertly transported PLA troops to two unoccupied islands (Duncan and Drummond), laying the groundwork for permanent occupation of the whole of the Paracel Islands. Operationally, the presence of Chinese fishing boats slowed down South Vietnamese deliberations on the use of force, as well as its response time in countering Chinese aggressive opportunism. Strategically, the employment of civilian fishing boats proved far less likely to trigger a U.S. intervention, even when the matter involved an American ally.[554] The operational and strategic lessons learned were not lost on the CCP then, and continue to be applied by it now.

The successful seizure of the Paracel Islands marked a "sea change" in Chinese maritime strategy. Beijing now routinely employs maritime irregular forces in gray

zone operations in support of the PLAN and CCG, as documented by Erickson and Kennedy. These noted academics diligently catalogued CMM's asymmetric activities since 1974. They discerned that the CMM has been involved in nearly every major PLAN and CCG operation to harass counter-claimants at disputed and contested maritime features (islands, rocks, or low-tide elevations) or to seize these features from them, especially in the South China Sea (SCS) where Beijing claims vague "historical rights" to the waters contained therein, based on its ambiguous Nine-Dash Line (NDL).[555]

In 1978, the CMM conducted maritime sovereignty assertion operations at the Japan-administered Senkaku Islands in the East China Sea (ECS). Since 2016, it has ramped up its presence and activities around these disputed and contested islands. During the 1980s, the CCP directed the CMM to maintain a "conspicuous presence" in the SCS, particularly around the Spratly Islands, under the narrative, "Develop the Spratlys, Fisheries Go First."[556] Since then, the CMM supported: the Chinese seizures of the Philippine-claimed Mischief Reef (1995) and Scarborough Shoal (2012); harassment of Vietnam's survey vessels (2011); blockades of Manila's resupply mission to Second Thomas Shoal (2014, 2021, 2022); deployments of a mobile oil rig and an oil survey ship to Vietnamese-claimed waters (2014, 2015, 2016, 2019); and oil and gas field standoffs with Malaysia (2020) and Indonesia (2021).[557]

Separately, the CCP also directed the CMM to harass, interfere with the navigation of, and disrupt the operations of U.S. naval vessels, confident that China's gray zone actions were below the threshold of any likely escalatory response. In 2002, a Chinese fishing boat struck and damaged the *USNS Bowditch's* towed array sensor while it operated in the Yellow Sea. Seven years later, Chinese fishing boats interfered with the safe navigation of the *USNS Victorious*, also operating in the Yellow Sea. Several days later, a mixed group of naval, law enforcement, and militia vessels harassed and disrupted the survey operations of the *USNS Impeccable* in the SCS. In 2014, Chinese fishing boats harassed the *USNS Howard O. Lorenzen* in the ECS.[558] In effect, Beijing was incrementally testing the waters for a U.S. response, to gauge how far it could push Washington in future contingencies.

In retrospect, the 2012 seizure of Scarborough Shoal marked a watershed event for the CMM, as the new Xi government committed more resources to modernize and professionalize the militia as part of a more assertive SCS strategy aligned with Xi's Thought and the Chinese Dream.[559] Xi saw a strategic opportunity when the United States responded ambiguously (one might even say meekly) to the seizure,

and largely accepted the Chinese fait accompli.[560] Washington did little to counter the subsequent militarization of the SCS, even after the landmark 2016 Permanent Court of Arbitration (PCA) ruling invalidated China's excessive maritime territorial claims. Xi correctly assessed that Washington would not risk the all-important bilateral economic relationship.

Since completing the controversial construction of China's artificial island outposts in 2016 (conveniently timed with the PCA ruling), Beijing shifted its focus toward exerting operational control in, and administrative jurisdiction over, the now-militarized SCS. The CMM accordingly deployed to the Spratly Islands in greater numbers, and on a more consistent and persistent basis, to assert, "China's indisputable sovereignty over the islands in the SCS and the adjacent waters thereof [NDL]."[561] Chinese fishing boats markedly increased their harassment and intimidation of other claimants' fishermen (Brunei, Indonesia, Malaysia, Philippines, and Vietnam), especially the Filipino and Vietnamese fishermen. As of 2022, hundreds of CMM fishing boats continue to operate daily in the Spratly Islands, with the Asia Maritime Transparency Initiative (AMTI) reporting increased persistent presence near the Philippine-occupied Thitu Island, the unoccupied Whitsun Reef, and the China-occupied Hughes Reef in the adjacent Union Banks.[562]

In general, China's ability to forward deploy and surge when needed—using PLAN, CCG, and CMM vessels based on Hainan Island (China's southernmost province)—throughout the SCS further changed the regional balance of power in China's favor. Moreover, the CMM's outward appearance as a commercial fishing fleet affords China with asymmetric ambiguity and deniability, allowing it to pressure other SCS claimants with maximum effect at minimal cost. Competing claimants cannot match the superior numbers and size of Chinese fishing boats, while other national powers intent on the peaceful resolution of SCS disputes, including the United States, lack the practical means to blunt this maritime coercion without appearing escalatory.[563]

Missions and Tasks of China's Maritime Militias

No official definition of the CMM has been uncovered as yet, but Erickson and Kennedy found a couple of authoritative characterizations that offered a window into Chinese thinking on the organization's missions and tasks. In 2012, the Zhoushan Garrison Commander and Mobilization Office described the CMM as an, "irreplaceable mass armed organization not released from production and a component of China's ocean defense armed forces [that enjoys] low sensitivity and great leeway in maritime

rights protection actions."[564] In 2013, the Guangdong Military Region Headquarters Mobilization Department outlined three of CMM's roles: "forms a certain embodiment of national will of the people implementing maritime administrative control; helps shape public opinion, as a group of model mariners meant to inspire both enterprises and the masses to get involved in maritime development and travel out to China's possessions (disputed islands and reefs); and is a guarantor of maritime safety, with its members often serving as the first responders in emergencies since they are already distributed out across the seas."

The first two roles speak to CMM's contribution to the political mobilization of Chinese society towards the maritime environment, a stepping stone to the Asian century, a projected *21st* century dominance of Asian (Chinese) politics, economy, and culture. The third role refers to the CMM's activities at sea as a rapid responder to crises and contingencies. Hence, the inferred primary role for the CMM is as an external maritime defense force in support of the PLAN, while serving a secondary role as an internal maritime security force in support of the CCG.[565]

The CMM has a wide gamut of assigned maritime missions, from traditional logistical support for ground forces, to more advanced maritime missions in support of naval and law enforcement. The following list of mission roles and responsibilities is not exhaustive or definitive, but rather a summary of those detailed in various Chinese sources to date:[566]

- Support the front (*zhiqian*) — The CMM provides logistical support to PLA, PLAN, and CCG operations by augmenting transport capacity, performing medical rescue, providing navigational assistance, conducting emergency repairs and refits, and conducting replenishment at sea. The CMM can also execute wartime missions including limited mining, information, electronic, and special operations warfare.
- Emergency response (*yingji*) — The CMM, in coordination with the CCG, responds to rapidly developing maritime crises, loosely defined as natural disasters, industrial accidents, public health incidents, and societal security events that threaten harm to Chinese citizens or the CCP.
- Maritime rights protection or legal warfare (*weiquan*) — The CMM asserts and enforces China's sovereignty claims in disputed and contested maritime areas. This supporting mission is meant to show national presence and manifest territorial sovereignty in conjunction with the PLAN and CCG.

- Intelligence, Surveillance, and Reconnaissance operations — The PLAN employs the CMM to fill Intelligence, Surveillance, and Reconnaissance gaps while loitering around targets of interest, or operating in the high seas.

Organization of China's Maritime Militias

The CMM follows a dual military-civilian structure, where the administrative and operational responsibilities fall on both the local maritime militia authorities and their national counterparts in Beijing. Senior CMM leaders hold multiple positions in both military organizations and concomitant civilian agencies. This parallel command system starts at the Provincial Military District-level and goes all the way down to the County/Township People's Armed Forces Department-level. The top governmental institution that brings together these interlocking military and civilian entities into a single national decision-making body is the National Defense Mobilization Committee (NDMC), responsible for organizing, directing, and coordinating national defense mobilization nationwide. The NDMC ensures that committed and allocated national resources quickly flow to the right organization, or agency, at the right time. At the national level, the Central Military Commission (CMC) and State Council, a civilian organization, lead the State NDMC. A subordinate NDMC is established at each corresponding military and civilian leadership level from the province on down. Orders to mobilize ultimately come down from the CMC or State Council, with the nature and degree of this mobilization depending on the nature and degree of response required.[567]

For the day-to-day CMM operations, the following controls govern command relations:[568]

- Units conducting Intelligence, Surveillance, and Reconnaissance operations at sea are directed by the Military District system;
- Units conducting emergency response are tasked and organized by the local government or search and rescue agencies, with Military District participation;
- Units conducting maritime rights protection report to a command organized by the local Military District and relevant civilian agencies under the unified command of local government and CCP officials;
- Units supporting law enforcement missions are commanded by the CCG, in cooperation with the local Military District, under the unified command of local government and CCP officials;

- Units supporting naval missions fall under the unified command of the PLAN in cooperation with the local Military District.

The CMM assigns its fishermen to units, or attaches them to civilian corporations, as cover, but all receive paramilitary training and political education to mobilize and promote China's maritime interests. CMM vessels are equipped with advanced electronics, including communications and radar systems, to supplement the PLAN, and enhance interoperability with other government agencies like the CCG. Many CMM vessels also have satellite navigation to track and report vessel positions to conduct maritime intelligence, which is technically a violation of the laws of naval warfare.[569]

China's Maritime Militia Challenges Maritime Law

In 2015, James Kraska and Michael Monti (USNWC) provided the first, and still one of the best, legal analyses of the CMM. They identified and described the strategic, operational, and tactical issues challenging enduring maritime laws and customs. Firstly, distinguishing between legitimate civilian fishing boats and CMM vessels supporting the PLAN and CCG during armed conflict is quite challenging due to the large numbers of vessels, the vast expanse of the maritime battlespace, and a lack of sensors to detect ships and their activities. These challenges are further exacerbated by the CMM integrating novel warfighting technology and tactics, conducting more intensive irregular warfare training, and continuing to circumvent both the meaning and intent of the laws of naval warfare to protect non-combatants through the legal principle of distinction. Secondly, China will leverage the CMM's asymmetric advantages in ambiguity and deniability to covertly conduct Intelligence, Surveillance, Reconnaissance, and Targeting in support of the maturing PLA Digital Kill Chain and greater Anti-Access/Area Denial strategy. The former seeks to enable the PLA to decide more quickly on when, where, and how it can engage targets using lethal and non-lethal fires. The latter seeks to prevent the attacker from bringing forces into the contested battlespace, or to deny freedom of movement within it. Lastly, in the case of a potential Sino-American conflict, the CMM's casualties will be core to China's political and diplomatic efforts to take the information operations "high ground" to weaken American international standing, damage the U.S. image as the "defender of global rules and norms," and undermine its commitment and resolve.[570] This prescient analysis is still relevant today. CMM operations and activities asymmetrically complicate the maritime environment, degrade decision-making, and expose decision-makers to political conundrums, and military commanders to operational dilemmas, that will make them more wary, and, perhaps, even restrained, in their actions against China during a crisis or conflict.

Opportunities to Counter China's Maritime Militia

The nature, scope, and extent of CMM irregular warfare operations call for a broad and comprehensive approach in people (force structure, training), process (policy, strategy, tactics), and things (equipment, technology) to mitigate the resultant risks across the levels of warfare.

At the strategic level, the United States and its allied partners should make it publicly known that CMM's irregular warfare activities are monitored, and that its vessels immediately become legitimate military targets should they engage in any acts of war. The goal is to strip away the CMM's masks of legal ambiguity and deniability that afford the PLAN and CCG its operational/tactical advantages, and, for the CCP, strategic gains.

At the operational level, the United States should consider several different recommendations:

- Posture U.S. forces, particularly those of the Coast Guard, to better deal with the CMM during times of both peace and war, in terms of training, tactics, and equipment. Conventional U.S. Navy forces are not well-suited to counter the unconventional CMM and its asymmetric operations and activities;
- Expand and improve the training of U.S. forces in countering gray zone operations;
- Develop appropriate rules of engagement, operating procedures, and reporting criteria for interaction with the Chinese paramilitaries on the high seas, particularly in disputed and contested maritime areas;
- Equip U.S. forces with more non-kinetic capabilities to better counter gray zone operations, and improved recording equipment to document gray zone activities for the courts of international law and public opinion;
- Do the same with U.S. allied forces, by promoting a change in domestic laws to empower their coast guards to conduct more naval functions, building up regional law enforcement capabilities and capacities to counter gray zone operations, and supporting regional maritime militias to counter the CMM with U.S. and allied navies and coast guards overwatch, similar to Chinese cabbage tactics (this can be done by leveraging Section 1202 of the National Defense Authorization Act, authorizing the United States to "partner with regional irregular maritime forces and empower their regional governments to better defend their respective maritime interests against increasing Chinese encroachments while reducing the need for

U.S. naval forces as the sole ever-present regional bulwark.")[571]

At the tactical level, civilian policymakers can direct military commanders to:

- Develop and implement better methodologies for identifying and tracking CMM vessels and detecting its irregular warfare activities to expose the organization, and diminish its effectiveness as a gray zone force;
- Formulate better tactics to counter gray zone operations, like localized electronic jamming to disrupt command, control, and communication, cyber actions to degrade positioning and navigation, and asymmetric operations to target logistics;
- Consider the tactical employment of unmanned underwater drones to covertly track the movement and activities of CMM vessels;
- Consider the tactical employment of swarms of armed unmanned aerial drones to interdict, and if necessary, neutralize a large number of CMM vessels.

These recommendations are not exhaustive, but rather represent things already being implemented or under consideration for implementation, and whose cumulative deterrent effects may also moderate future CMM operations and activities, keeping them below the threshold of escalatory response by imposing costs, denying benefits, and encouraging restraints.

China's Maritime Militia: Rise or Decline

There are two possible future scenarios for the CMM threat with rise being the more likely outcome:

"CMM Rise" — The CMM evolved and matured from a disparate and disorganized local coastal force to a homogenous and organized national maritime force, tasked and equipped to advance China's maritime interests as a critical supporting Third Sea Force tethered to the supported PLAN and CCG. The fact that the CMM not only survived, but thrived during this transition suggests that the CMM's operational role will only expand, in parallel with the PLAN and CCG, to better support their naval and law enforcement missions in furtherance of national goals and strategic ambitions. The militia's humble roots as a product of collectivization, and Soviet naval doctrine, also suggests that if China faces slowing military modernization due to economic or other circumstances, the CCP could and would rely more on the CMM as a more cost-effective and lower technology option for sovereignty disputes and territorial defense.[572]

"CMM Decline" — With the growth and development of the PLAN and CCG into the largest naval and coast guard forces in the world by size, respectively, and the CMM's subordination to them as the supporting Third Sea Force, there is lesser strategic and operational need for the declining entity moving forward. The PLAN and CCG are also catching up qualitatively with the rival U.S. Navy and Coast Guard, respectively. Therefore, the role and influence of the CMM will further decline, and operational tasks will become progressively limited as the PLAN and CCG further grow, modernize, and professionalize. Market economics make the fishing industry less and less attractive to the younger generations, resulting in an overall reduction in the fishing fleet.[573]

At the End of the Day

CMM operations (gray zone activities) steadily increased in scope and frequency since 2012, and show no signs of abatement. U.S. and regional responses have not deterred the CCP. The CCP continues to see strategic and operational value in CMM's asymmetric advantages, and remain confident that their irregular warfare actions are below the threshold of escalatory response. The CCP will ratchet up CMM's legal warfare activities to further gauge U.S. and regional tolerance, desensitize them from assertive actions, and re-baseline their behavior to new levels of forbearance. So, unless convincingly challenged, the unchecked CMM will continue to intimidate like a bully on the playground, and China will win without fighting. The CCP will also increase the CMM's irregular warfare capabilities and capacities, as well as integrate them deeper into the PLA's operational plans and contingency planning to, again, win without fighting; and when it does fight, China will fight with strategic, operational, and tactical advantages.

The asymmetric operations and activities of China's little blue men complicate U.S. and allied naval operations across the full spectrum of war: during peacetime, in the gray zone, and in armed conflict. During peacetime, the CMM conducts joint emergency response, and state-sponsored legal warfare, to assert and enforce China's expansive maritime territorial claims. In the gray zone between peace and war, the CMM tracks and reports U.S. and allied vessel positions (intelligence, surveillance, and reconnaissance) and provides logistical support to the PLAN and CCG. In armed conflict, the CMM provides intelligence, surveillance, reconnaissance, and targeting information to the

PLA Digital Kill Chain in support of Anti-Access/Area Denial defense of the Chinese mainland, and executes other supporting wartime missions. As China increasingly integrates the CMM into the PLA force structures, operational plans, and contingency planning, the legal line between civilian fishing boats and military vessels further fades, upending centuries of enduring maritime laws and customs and undermining the liberal international order that has provided global prosperity and security for over 75 years.

About the Author

Tuan N. Pham is a retired Navy Captain, maritime strategist, strategic planner, naval researcher, and China Hand with 20+ years of operational experience in the Indo-Pacific and 60+ published articles in U.S. and foreign national security journals. The views expressed here are personal and do not necessarily reflect the positions of the U.S. Government or Navy.

Discussion Questions:

1. What is the China's Maritime Militia (CMM), also known as the People's Armed Forces Maritime Militia, in the terms of irregular warfare, and in context of great power confrontation, in the 21st century?
2. What is the CMM's affiliation with the Chinese state?
3. When and why did China establish the CMM, and how did it develop over the years to its current unconventional manifestation?
4. What does the CMM's unorthodox history suggest about its future asymmetric operations and activities?
5. How does the CMM challenge longstanding maritime laws and customs, and what are the strategic, operational, and tactical implications thereof?

6. How can the United States and its allies and partners deal with this ever-evolving maritime component of irregular warfare?

Recommended Reading:

- Andrew Erickson and Conor Kennedy, "China's Maritime Militia," *Center for Naval Analyses*, February 2016. Conor Kennedy and Andrew Erickson, "China's Third Sea Force, People's Armed Forces Maritime Militia: Tethered to People's Liberation Army," *U.S. Naval War College*, March 2017. James Kraska and Michael Monti, "Law of Naval Warfare and China's Maritime Militia," *U.S. Naval War College*, 2015.
- Gregory Poling, Tabitha Grace Mallory, and Harrison Pretat, "Pulling Back Curtain on China's Maritime Militia," *Center for Strategic and International Studies*, November 2021.
- Derek Grossman and Logan Ma, "Short History of China's Maritime Militia and What It May Tell Us," *RAND Corporation*, 6 April 2020.
- Shuxian Luo and Jonathan Panther, "China's Maritime Militia and Fishing Fleet, Primer for Operational Staffs and Tactical Leaders," *Military Review*, January-February 2021.

Russia's "Special" Way of War: SOF, Spetsnaz, and Irregular Warfare

Christopher Marsh[574]

ABSTRACT

While in the United States the process of defining irregular warfare is an on-going and contentious affair, Russia does not group its mission sets–such as counterterrorism, counterinsurgency, and unconventional warfare–together in the same way. This chapter examines the development of Russian special military units over time, the evolution of these units, and the creation of their Special Operations Forces Command (KSSO). To shed light on the similarities and differences between Russian and American approaches to irregular warfare, the chapter includes four case studies, two counterterrorism operations and two unconventional warfare missions. While some similarities were identified in terms of unit mission and core activities, "similar" does not mean "the same," particularly when it comes to contrasting approaches between the West and Russia in conducting special operations.

Introduction

In the United States, and the West more broadly, defining irregular warfare (IW) has been an on-going and contentious affair.[575] Long considered "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations," the Joint Staff J7 (directorate of Joint Force Development) at the Pentagon recently released an updated official definition of irregular warfare. According to them, IW should now be considered across the Department of Defense as, "a form of warfare where states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities."[576]

In Western Europe, other definitions prevail. A leading effort was made in this regard by scholar Martijn Kitzen: "...a violent struggle involving non-state actors (including violent armed groups acting as state proxies) and states with the purpose of establishing power, control, and legitimacy over relevant populations."[577] This definition, which resembles the traditional U.S. definition of IW, can be broken down even more succinctly–as was done by James Kiras–who earlier identified terrorism and insurgency as being at the crux of irregular warfare.[578]

If terrorism and insurgency are the main modes of irregular warfare, then actions taken to counter such warfare, in the form of mission sets, can be considered irregular warfare as well. Thus, counterinsurgency and counterterrorism are at the center of the U.S. approach to IW. Foreign internal defense (which seeks to aid and support a friendly nation in its fight against terrorism and insurgency), unconventional warfare (which seeks to support a resistance movement in its fight against an occupying force or oppressive regime), and stability operations (efforts which seek to bring peace and security to a region or country, particularly in a post-conflict environment) round out the list of operations that are typically seen as comprising irregular warfare, that is, before the addition of other–mostly information-related activities–to the irregular warfare toolkit.[579]

As Sandor Fabian and Gabrielle Kennedy concluded in their study, most of the institutions they surveyed linked special operations with irregular warfare.[580] As they phrased it, this "linkage is bolstered by the idea that these forces [special operations forces: SOF] are considered as either the primary tool of irregular warfare or a major component in the practice."[581] As U.S. Army Special Forces officer LTC Stephan Bolton puts it, "in many instances, SOF tend to be the best instrument to conduct the military aspects of an IW campaign."[582] In the United States, in particular, and the West, more

generally, IW campaigns require whole-of-government efforts and various actors across the interagency play important roles. When it comes to the military aspects of irregular warfare, however, these efforts are led by SOF.

In Russia, things are a little different. The mission sets are largely the same as the traditional mission sets of U.S. SOF-led activities to counter insurgency, terrorism, and instability, with the addition of a strong emphasis on intelligence activities and covert or otherwise clandestine operations. This is due to the fact that Russia is no stranger to terrorism, insurgency, and separatism, fighting all three in combination throughout its history. Beginning with the period of the Soviet Union, the Kremlin became involved in all of the mission sets identified above, from Chile and Cuba to Angola and Vietnam. And this is without mentioning the domestic struggles with each, from terrorist cells such as the 19th century's *Narodnaya Volya* (the People's Will) to Chechen terrorists and insurgents following the collapse of the Soviet Union.

Despite its long history in fighting irregular warfare, inside Russia there is really no debate on what is or is not irregular warfare—in fact, the term itself is not used. From writings on special operations theory,[583] to Gerasimov's insights into non-linear and asymmetrical warfare,[584] the debates seem to center on how Russia can counter its adversaries rather than on fleshing out concepts that describe modes of war with which they are intricately familiar. Moreover, there is no discussion of winning over "hearts and minds" or gaining legitimacy. Rather, legitimacy is something that is constructed post-facto to preserve national interests. At other times, parsing out the type of conflict entailled does not seem to matter much to the powers that be in the Kremlin.

As for the term itself, Russians do not use the word *neregulyarnaya voina* (irregular warfare) or *neregulyarnye voiny* (irregular wars) themselves, with the term simply understood as a U.S. "doctrinal construct." In fact, they have a rather accurate understanding of our conceptual framework for IW as laid out in the unclassified annex to the 2020 National Defense Strategy, though they argue that, "events in which America is directly involved are presented in a false and distorted light."[585]

Russia views IW as a Western construct and never mentions its own operations in such a framework. Nevertheless, the country has also been faced with and engaged in activities and situations we in the United States would label IW. By this I mean insurgency, terrorism, and instability, and thus have engaged in counterinsurgency and counterterrorism, along with foreign internal defense and unconventional warfare. Russia's history with stability operations as understood by the United States is more storied, but will not be examined in detail here. The remainder of this chapter will examine

the forces that Russia employs to conduct counterinsurgency, counterterrorism, foreign internal defense, and unconventional warfare–that is primarily its SOF, *spetsnaz*, and conventional forces (including mechanized troops and artillery). The focus here is on Russia's SOF and *spetsnaz*, however, and the units that conduct some of the country's most secret and sensitive operations.

As Bolton further explains, "in many instances, SOF tend to be the best instrument to conduct the military aspects of an IW campaign."[586] This is largely true for the Russian armed forces as well, particularly when it comes to counterterrorism. But in Russia there is also the *spetsnaz* units–some of which are roughly equivalent to U.S. and Western tier 1 units–which also conduct counterterrorism and counterinsurgency. If we want to understand Russian approaches to IW, we must first begin with a solid foundational understanding of Russia's "special" way of war.

The Roots of Russian SOF

The roots of Russia's special operations forces (SOF) rest with the Soviet *spetsnaz* units. The term comes from *voiska spetsial'nogo naznacheniya*, or special designation troops. Though most *spetsnaz* units are certainly elite, and thus distinct from conventional forces, they are not the same thing as SOF despite the frequent conflation by commentators. Nor are they simply the equivalent to U.S. Army Special Forces ("Green Berets"), despite the fact that until recently they have nearly been synonymous terms. To translate *spetsnaz* as Special Forces is a gross–and misleading–oversimplification and will only lead to greater confusion since the latter are only one part of the U.S. Army SOF community (the others being psychological operations and civil affairs). Apart from the Army, each U.S. service has its own special operators (Air Commandos, Navy SEALs, MARSOC Raiders, etc.). To make the distinction simple, in Russia all SOF are *spetsnaz*, but not all *spetsnaz* are SOF.

There is even greater diversity among *spetsnaz* units, than there is within the American SOF community, because unlike in the U.S. and most NATO countries, where special operations units are limited to departments or ministries of defense, this is not the case in Russia. There, the ministry of interior, Federal Security Service (FSB, the offspring of the KGB), and other divisions have their own *spetsnaz* units, especially for intelligence collection and diplomatic security. As Lester Grau and Chuck Bartles clearly explain, "The word 'special' [in *spetsnaz*] is used in a very broad way that can indicate that the unit has a very narrow area of specialization, such as signals intelligence, engineering, reconnaissance, etc.; or the unit is experimental or temporary in nature; or the unit

conducts tasks of special importance such as sensitive political or clandestine operations. This broad usage of the term means that '*spetsnaz*' cannot be thought of as equating to the Western concept of Special Operations Forces (SOF)."[587]

This is certainly true, and I would argue that this opinion is even held by the Russian Ministry of Defense, which is why they are now developing their own SOF units, *sily spetsial'nykh operatsii*, or SSO. But this is a relatively new phenomenon and one that is only beginning to be understood, as discussed below.

Soviet Spetsnaz

Before Joseph Stalin had him executed in 1938 during the Great Purge, Russian military theorist Mikhail Svechnikov proposed the creation of a small, highly-trained military unit that could work behind the scenes to obstruct enemy operations. This idea was adopted by military officer Ilya Starinov, who became known as the "grandfather of the *Spetsnaz*."[588] The earliest actual *spetsnaz* units were formed in 1950, though it is worth mentioning the role of special-type units during the Russian Revolution (1917-1921). As John Dziak observes, while there is no "unbroken link" between such special units and later *spetsnaz*, the former are often viewed as the conceptual forerunner to the latter.[589] All Russian *spetsnaz* and SOF trace their heritage back to the *razvedchiki* (reconnaissance scouts) of the Revolutionary War. These soldiers served as behind-the-lines commando elements, providing much-needed intelligence on enemy positions and capabilities, a critical function given the nature of the civil war the Red Army was then fighting.

The most significant of the special units of the Revolutionary period was the ChON, or special purpose brigades (*Chasti osobogo naznachenya*), which by the end of the war numbered some 40,000 soldiers.[590] This was an elite unit formed from broader categories of existing specialized forces.[591] As an ideological movement, the Bolsheviks recruited from among the most loyal and "believing" Communist soldiers those to serve in the ChON. Their mission was two-fold. First, they acted as counterintelligence agents at home and in occupied territories, ensuring that those in the ranks were in fact loyal Communists. And secondly, they served as sabotage, assassination, and agitation assets behind enemy lines.[592] These were the first units to be given the label "special designation."[593]

The Russians started experimenting with elite reconnaissance and sabotage units during the Spanish Civil War (1936-1939) and employed such units in the Soviet-

Finnish "Winter War" (1939-1940), as well as in Romania, Yugoslavia, and Belarus during the Second World War.[594] But the real roots of Russia's special operators lay with the partisan fighters who fought the German forces that invaded the Soviet Union in World War II. These loosely organized units were tied to the Partisan Directorate, which officially was under the Supreme High Command (or *Stavka*). Though they did not have the label *spetsnaz*, they were resistance fighters of all types (including naval infantry and even sappers) who organized as best as they could to halt the German advance into the Soviet motherland, to support conventional forces when the opportunity arose, and to organize guerilla operations if behind enemy lines. This latter was a crucial role for the partisans during World War II, or as it is known in Russia, the Great Patriotic War.

The Russians viewed their partisan experience in the Great Patriotic War as a highly effective "unconventional" adjunct to their conventional operations. The Soviets claim that during the war partisans killed, wounded, or took prisoner, "hundreds of thousands of German troops, collaborators, and officials of the occupation administration." They also claim to have derailed more than 18,000 trains, and destroyed or damaged thousands of trains, and tens of thousands of rail cars. These operations supposedly had a devastating effect on German morale and forced the Germans to deflect much-needed resources from frontal operations.[595]

The real era of the *spetsnaz*, however, was the Cold War. The Soviets developed the first *spetsnaz* units in 1950–two years prior to the formation of U.S. Army Special Forces.[596] In the Soviet Union's attempt to keep up with U.S. military developments, the Kremlin put a tremendous amount of effort into their *spetsnaz* and special operations capabilities as they tried to outflank the West at all levels across the political-military spectrum.[597] Methods included covert and clandestine activities of all kinds, with particular emphasis on insurgencies, active measures/deception operations,[598] psychological operations, and even support for terrorist organizations around the world.[599] *Spetsnaz* squads were trained to be dispatched to reconnoiter in the enemy rear area to locate nuclear delivery systems, enemy forces, headquarters, airfields, signal sites and other important targets.[600] They were also trained for and prepared to conduct raids, ambushes, sabotage, and surgical strike operations against key enemy personnel and infrastructure, and to conduct reconnaissance/intelligence operations at the same time.[601] Moscow's capabilities were augmented by proxy forces where possible, especially when direct Soviet involvement might be imprudent.

Despite this experience, beginning in 1979 Soviet *spetsnaz* found themselves operating in a very different environment–that of Afghanistan. *Spetsnaz* were involved

from the very beginning, with Col. Vassily Kolesnik tasked with recruiting a "Moslem battalion" of *spetsnaz* of Tajik, Turkmen, or Uzbek nationality, with the idea being that its members could pass themselves off as Afghans. The unit had been assembled by June 1979 and began its training with the *spetsnaz* unit *Al'fa* (more on this unit below), though the "Moslem battalion" reportedly did not know what their mission was going to be. During the December 1979 invasion of Afghanistan their role was to penetrate the imperial palace and facilitate the infiltration of two other *spetsnaz* units–*Kaskad* (Cascade) and *Zenit* (Zenith). Together, this combined unit was the lead in conducting "Operation 333," killing President Hafizullah Amin and those loyal to his rule and setting the stage for the Soviet invasion of Afghanistan.[602]

As the war in Afghanistan dragged on, *spetsnaz* units found themselves carrying out a variety of missions, many of which were unlike those for which they had been trained for against the West. By October 1980, they were increasingly being brought in to supplement the Limited Contingent of Soviet Forces in Afghanistan (the official name of the Soviet operation in Afghanistan). There their skills for such things as reconnaissance, ambush, and rapid reaction were put to regular use. Some *spetsnaz* also became involved in so-called "Stinger hunting missions," once the U.S.-made, shoulder-fired weapon was introduced into the war zone. These "Stinger hunters" sought out Mujahedeen equipped with such weapons and did their best to destroy both the weapon and its operator.[603]

Overall, during their ten-year struggle against the Mujahideen, the Soviets deployed a significant capability based around their highly-trained *spetsnaz* units. A critical examination of their performance by Tony Balasevicius, however, reveals that Soviet *spetsnaz* were often misemployed and, as a result, were unable to make a significant contribution to the outcome of the war.[604] This misemployment, Balasevicius argues, was based on the Kremlin's desire to focus *spetsnaz* efforts on propping up their under-prepared conscript army rather than trying to identify how *spetsnaz* might contribute to a grander operational vision for success. Thus, in the end, they served as key enablers but were not tasked with the proper missions and given the correct resources, including an appropriate amount of time to meet operational and strategic demands.[605]

Spetsnaz in the Post-Soviet Era

The two wars in Chechnya were the crucible for Russia's *spetsnaz* that Afghanistan had been for their Soviet predecessors. Often employed simply as elite infantry, they were

also tasked with targeting and eliminating high value targets, in this case rebel leaders of the Chechen insurgency that sought to liberate the territory from the Russian Federation. These rebel leaders were not just untrained farmers, however, and included in their own ranks many former Soviet/Russian soldiers, and even some former *spetsnaz*. This obviously greatly problematized the Chechen wars, and their losses were considerable.

At the start of the First Chechen War (1994-1996), *spetsnaz* found themselves in their usual role of battlefield reconnaissance. But once the illusion of a quick victory disappeared, which did so very quickly, many *spetsnaz* found themselves being used as shock troops. In fact, Moscow sought capable fighting forces from wherever it could, including naval *spetsnaz*, and even the ministry of the interior's OMON counter-riot units. Moscow was greatly relieved when retired Gen. Alexander Lebed was able to negotiate a ceasefire in 1996 in the wake of the presidential elections, after he himself made a strong running for the presidency.[606]

The Second Chechen War (1999-2002) was different from the first in many ways, mostly as what had been a nationalist insurgency had developed into a Muslim religious war for independence.[607] The other difference was that Moscow's invasion of Chechnya in 1999 was well thought out and was much more successful than the first. The ground invasion was preceded by an initial air campaign, softening of targets and preparing troops for effective operations. From the fall of 1999 through 2009, Moscow directed a sustained campaign that effectively destroyed the Islamic insurgency in Chechnya, and reasserted Russian control of the region.[608] The *spetsnaz* performed their usual roles of deep reconnaissance, interdiction, intelligence gathering, and acting as a rapid reaction unit. In contrast to the First Chechen War, this time *spetsnaz* were used in their trained roles for the most part, and performed well. They were also supporting and supported heavy units, such as artillery and armor, that blasted the capital city of Grozny into rubble.

One of the most notorious of *spetsnaz* units, not just during the Chechen wars but throughout its existence, is that of the GRU, the Main Intelligence Directorate. Most direct action and reconnaissance *spetsnaz* units have historically been under the command and control of the GRU, which reports directly to the General Staff.[609] During the Cold War, their mission sets focused on deep reconnaissance, and countering weapons of mass destruction, particularly battlefield tactical nuclear weapons, especially in the event of a war in which Soviet territory was immediately overrun. These units would then act as stay-behind forces, conducting sabotage operations, diversion activities, and countering tactical nuclear weapons.

Not all *spetsnaz* fall under the military (or Ministry of Defense). Other very significant *spetsnaz* units were (and still are) found in other organs of the state. In 1974, the Soviet Union created one of its most elite tier 1 special operations units, simply known as "Group A" (later becoming known as *Al'fa*, or Alpha). *Al'fa* was the premier counterterrorist unit in the Soviet Union under the control of the KGB (Committee on State Security), as opposed to most *spetsnaz* that fall under the GRU. Today *Al'fa* still exists and is still just as elite (the "best of the best," reports *RIA Novosti*), though it is now under the reorganized and renamed KGB, known as the FSB (Federal Security Service).[610] *Al'fa* remains the premier counterterrorist (antiterror) organization in Russia, thus playing an important role in Russia's approach to irregular warfare.

Also originally falling under the KGB, and just as elite and lethal, is *Vympel* (meaning "pennant"). *Vympel*, which also has a counterterrorist role, is most well-known for its unconventional warfare and covert action skills. Again, the roots of this *spetsnaz* unit date back to the days of the Soviet Union, though in this case it was to deal with the military coup in Chile of September 1973. The socialist government of Salvador Allende, one friendly to the Soviet Union, was overthrown in a Central Intelligence Agency (CIA)-backed coup. "Group V" was created to go in and rescue the General Secretary of the Communist Party of Chile, Luis Corvalan. The special operation was not needed, in the end, as Corvalan was released in a prisoner exchange, but the incident made it clear that the Soviet Union needed such a unit that could always be on alert, and able to carry out covert operations anywhere in the world.[611] By the early 1990s the unit numbered some 300-500 persons and fell under the Ministry of Internal Affairs (MVD).[612] Highly secretive, *Vympel* plays not only a counterterrorist role, but also an unconventional warfare role, though this mission is never mentioned in connection with the unit by the Russian authorities, who publicly deny conducting such operations with the unit.[613]

By the time of the collapse of the Soviet Union, the term "*spetsnaz,*" when used in reference to the Soviet Union's elite combat units usually referred to the GRU's *Spetsnaz* Brigades and Combat Swimmer units (roughly the GRU's naval reconnaissance force with a sabotage/anti-sabotage capability), the Russian Airborne's 45th *Spetsnaz* Regiment (later brigade) or select elite anti-terrorism units (such as *Al'fa* and *Vympel* mentioned above).[614]

Russia's SOF Join the Fight

On 6 March 2013 General Valery Gerasimov, Chief of the Russian General Staff, announced the creation of Russia's own Special Operations Command and Special

Operations Forces (SOF). "Having studied the practice of the formation, training, and application of special operations by the leading foreign powers," he stated, "the leadership of the Ministry of Defense has also begun to create such forces." He continued: "We have set up a special command, which has already begun to put our plans into practice as part of the Armed Forces training program. We have also developed a set of key documents that outline the development priorities, the training program, and the modalities of using these new forces."[615] Minister of Defense Sergei Shoigu also commented on this momentous occasion in developing a Special Operations Forces Command. He said, Russia was following "the general trend [in the world] toward specialization and enhanced mobility."[616] Indeed, in their own observation of this event, one Russian news agency pointed out that the country was only 26 years behind the United States in developing such a command, in addition to being behind other Western countries, including Germany, France, and Canada.[617]

There are many reasons why Russia was so delayed in developing special operations forces, and a SOF command. The previous Minister of Defense of the Russian Federation, Anatoly Serdyukov, had apparently been supportive of the idea, but developments were kept quiet under his leadership. Once he was ousted on criminal charges and replaced by Sergei Shoigu, however, the latter picked up the ball and ran with it, quickly putting into place all the necessary components. Pieces of the puzzle began to be assembled apparently as far back as 2008, in the wake of the Russia-Georgia War, during which Russian forces did not perform as well as expected and prompted a major reorganization of the military, which came to be known as the "New Look" military reforms.[618] This major structural reorganization of the Russian Armed Forces was announced in October 2008, and began in early 2009, under Serdyukov. The stated aims of the reforms were to reorganize the structure and the chain of command of the Russian army, to reduce it in size, and build the army around a three-link system (military district–operational command–brigade). Another significant aspect of that reform initiative was the establishment of Russia's Special Operations Forces Command (*Komandovanie sil spetsial'nalnykh operatsii*, or KSSO) and Russian Special Operations Forces (or *sily spetsial'nykh operatsii*, or SSO).[619]

Russia began reforms between 2008 and 2012 that culminated in the establishment of Russia's own Special Operations Forces Command. The first step was the establishment in 2009 of the Directorate of Special Operations (*Upravlenie Spetsial'nykh Operatsii*), centered on a unit based out of a training center in Solnechnogorsk, near lake Senezh. One of its founding fathers was the then-Chief of the General Staff General of the

Army Anatoly Kvashnin. This unit had seen significant combat in Chechnya during the Second Chechen War.

The second step was the establishment of another center in Kubinka-2, also on the outskirts of the Moscow region. This center was directly under the control of the GRU, and hence it retained its *spetsnaz* designation, being named the Center of Special Designation (*Tsentr Spetsial'nogo Naznacheniya*). It came to be known as Kubinka. Shortly thereafter, on 1 April 2012, upon the initiative of Gen. Nikolay Makarov, the Directorate of Special Operations was renamed the Special Operations Forces Command (*Komandovanie sil spetsial'nalnykh operatsii*, or KSSO). Finally, on 15 March 2013, Kubinka was linked to the special operations forces.

As early as 2012, Makarov had been talking about forming a KSSO, with plans for up to nine special-purpose brigades, and an expansion of the existing system of military intelligence special forces (GRU).[620] Intensive physical plant development at both Kubinka and Senezh then began, including infrastructure for basing and military training. Senezh also houses a sniper training school, and both seem to have diver training facilities, although Kubinka apparently includes a special naval operations directorate that controls several special naval operations departments and squads. There is also a cold weather/mountaineering center at Mount Elbrus named "Terskol," in Kabardino-Balkaria, used by Russian special operators for training.[621]

As for the manning of these units, although Russia has *spetsnaz* units it could just pull from, they are not just renaming them as SOF. Rather, they are selecting the very best from their regular army, particularly their reconnaissance units, having them first serve with *spetsnaz* units and later undergoing specialized training. Only then do they get designated as Russian special operators.[622] This emphasis on quality special operators speaks to Gen. Gerasimov's comment above about the high quality of the U.S. and Western SOF they encountered in their studies.

Once selected, officers and non-commissioned officers arrive at Senezh, where they undertake a rigorous entrance examination that tests not only the physical conditioning of the SSO operators, but also the personality and, perhaps most importantly, the ability to work within a team. The basic principle of Senezh is not to prepare an individual fighter with great skills and abilities, but rather to build teams that can act as a single organism.[623] The Senezh Center is marked by the fact that it builds a culture of teamwork among its trainees, and this is increasingly a factor in recruitment.

The training of the officer recruit special operators is carried out in the Ryazan Higher Airborne Command School (RVVDKU, department of special and military

intelligence and the Department of the use of special forces) and the Novosibirsk Higher Military Command School (NVVKU, Department of Special Intelligence and the chair of the special reconnaissance and airborne training). All SOF recruits learn skydiving, mountaineering, swimming, scuba diving, and how to storm buildings and homes. Depending on the individual tasks the soldiers are being prepared for, the training is more in depth.[624]

Additionally, it should be added that unlike other *spetsnaz* units that are seen as elite forces that perform missions (reconnaissance, direct action, etc.) for the sole purpose of furthering the movement and maneuver of conventional forces,[625] the structure of Russia's new SOF units suggests that it is intended to act independently. For that purpose, the command has a dedicated special aviation brigade that directly controls combat aviation assets at Torzhok, and a squadron of the Il-72 transporters at the Migalovo airfield near Tver. The command also has supporting elements that provide Combat Support and Combat Service Support functions.[626] Additionally, Alexsey Nikolsky reports that the Senezh compound has a large helipad that can accommodate three Mi-26 heavy transport helicopters (each one capable of carrying 70 soldiers with kit). He therefore concludes that this indicates about 200 soldiers are on duty at any given time at SSO unit 92154.[627] He also calculates that between Senezh and Kubinka there are approximately between 2,000 and 2,500 total special operators.[628]

SOF Doctrine, Missions, and Activities

The KSSO is reportedly tasked with standardizing doctrine and capabilities for Russia's premiere SOF units in all military forces, and is supposed to have the capability to provide command and control for these units in wartime.[629] The Russian Ministry of Defense defines the term "special operation" as follows: "the special operation of troops (forces) is a complex of special actions of troops (forces), coordinated by objectives and tasks, time and place of execution, conducted according to a single concept and plan in order to achieve certain goals. Special actions of troops (forces) are activities carried out by specially designated, organized, trained and equipped forces, which apply methods and ways of fighting not typical for conventional forces (special reconnaissance, sabotage, counter-terrorist, counter-sabotage, counterintelligence, guerrilla, counter-guerrilla and other activities)."[630] Here we see the core activities of Russian SOF, which in many ways equates to the traditional core activities of IW in the U.S. and NATO countries.

The greatest distinctions between U.S. SOF IW activities and those of Russian SOF is the inclusion of sabotage and counter-sabotage operations. Most other missions are

similar, if only worded differently. For example, due to their experience with partisan fighters in World War II, they have retained the concept of guerilla (*partizanskie*) and counter-guerrilla (*antipartizanskie*) operations, instead of developing a concept of insurgency and counterinsurgency warfare. Likewise, their understanding of conducting guerilla warfare is very close to the U.S. concept of unconventional warfare (UW), especially when it comes to the training of foreign fighters in the conduct of guerilla warfare for the purpose of overthrowing a hostile government.

Military correspondent Alexander Sladkov, while visiting military exercises in the mountains of the North Caucasus, articulated the goals and objectives of Russia's SOF as follows:

> "Special Operations Forces (SSO) – troops intended to achieve political and economic goals in any geographical part of the world of interest to the Russian Federation.... They come in cases when diplomatic methods are no longer active. Distracting forces and the attention of certain countries by external problems, problems creating them inside, rocking the political systems of these countries, destabilizing the situation, including through a 'third hand.' Special Operations Forces create, train, and supervise foreign guerrilla movements, eliminate unwanted leaders without any sanctions on foreign soil, and so on... Russian experts' main task is the protection of our citizens abroad, the release of Russians who have fallen hostage somewhere in distant areas, and protecting the interests of our country."[631]

As Nikolsky summarizes his excellent study of Russian SOF, Moscow's units are "proper combat units themselves and can operate independently. They are ready for rapid deployment across a spectrum of counterterrorism and combat missions, on Russian territory and abroad."[632]

SOF and Spetsnaz in Action: Case Studies

Despite the fact that Russia does not label its IW activities in the same way as the United States, SOF and *spetsnaz* are employed to conduct a full range of operations and activities in order to "assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities." How similar, however, are such activities when conducted by Russia's special operations units? The remainder of this chapter will focus

on four case studies, two counterterrorism cases (both part of a larger counterinsurgency campaign), and two more recent cases of SOF and *spetsnaz* in unconventional warfare campaigns in Crimea and the Donbas. These case studies highlight the vast differences that exist between Russian employment of special operations and that of the United States.

The first case study is the tragedy at the Nord-Ost' performance in the Moscow Dubrovka theater. The Moscow theater hostage crisis (also known as the Nord-Ost' siege) was the seizure of a crowded theater by 40 to 50 armed Chechens on 23 October 2002. This siege lasted four days, and involved 850 ordinary citizens (including 75 non-Russians from some 14 countries) who were held hostage in Moscow's Dubrovka theater by Chechen insurgents who were fighting for the cause of Chechen independence from the Russian Federation, and demanded the withdrawal of Russian troops from Chechnya and an end to the war. The unit employed to end the siege by assaulting the theater was *Al'fa* – Moscow's elite tier 1 *spetsnaz* anti-terror unit, supported by *Vympel* and SOBR (Special Rapid Response Unit), a domestic rapid response unit under the Russian national guard. These special operators pumped an undisclosed chemical agent, thought to be fentanyl, into the building's ventilation system at the start of the assault, yet failed to inform anyone of the agent's use. Once inside the building, the unit shot and killed almost all of the self-proclaimed "suicide squad" terrorists. In ending the siege, the death toll reached at least 170 people (including the terrorists). The high hostage death toll was partly due to the ineptness of the special operators involved, as almost all of the 130 hostages who died did so because first responders had no idea what agent had been used, and were therefore unable to treat the victims effectively.[633]

The second case study is the Beslan tragedy. The tragedy at Beslan began on 1 September 2004, when Muslim separatists from Russia's North Caucasus seized a grammar school and held everyone hostage (except for adult males, who were taken to a back room and shot). The siege ended three days later when various military units (primarily the *spetsnaz* units *Al'fa* and *Vympel*) attacked the school. This was purportedly set off by an over-zealous sniper who shot one of the terrorists before the planned assault on the building, leading to utter chaos and the death of 330 hostages.[634] Perhaps most alarming was the failures of joint operations execution in this incident. Beslan *spetsnaz* units were under the control of one command center, while the remainder of forces were under the control of another. The response to both events, however, was universally led by *spetsnaz*, who both generated both praise and criticism for how these events unfolded.

The Beslan tragedy led to serious debate in the Russian Duma, in military circles, and in society at large.[635] Still, any criticism of the *spetsnaz*-led operations was seen as a

criticism of the regime, and Putin would not stand for that. In response, narratives were subsequently drawn up for each event that made Russian military forces heroes, brushing aside any criticism of the operations and/or the way the events unfolded. Certainly, the *spetsnaz* units that conducted these operations were motivated by the clear purpose of eliminating the terrorists that had taken hundreds of people hostage, but apparently that was their main objective above and beyond the prevention of casualties and collateral damage.

Nord-Ost' and Beslan are examples of how *spetsnaz* operated prior to the "New Look" reforms, and the creation of the KSSO. Beslan and the Nord-Ost' theater attack are two prime examples of where *spetsnaz* units, indeed the entire joint force, had failed, mostly due to breakdowns in command and control, as well as inter-service rivalry,[636] and the nonexistence of a functioning Russian interagency framework, all things the creation of the KSSO and SOF were meant to address. Much like the American catastrophe at Desert One, during Operation Eagle Claw in 1980 (when a failed attempt to rescue American hostages being held in Iran resulted in the death of eight special operators), the Beslan and Nord-Ost' tragedies provided a pretext on how Russia's elite units both functioned and also didn't function as a joint force, particularly in joint command and control and in interagency operations (a concept wholly unfamiliar to the Russian context). But unlike the United States, Russia did not draw lessons from these catastrophes. In fact, these failures were covered up, and the events heralded as successes, particularly for its *spetsnaz*.

The third and fourth case studies are more recent (post- "New Look" reforms and the creation of the KSSO), and focus on the unconventional warfare (*partizanskaya voina*) campaign in Crimea and the Donbas in Ukraine between 2014-2016. As is now well known, on 27 February 2014, the military occupation of Crimea by "little green"–and according to Russian news sources "polite"–men began. In a matter of a few days, Russian forces were able to seize power, block, disarm, and even win over significant portions of the Ukrainian military, and then to legitimize their presence, all the while conducting information operations and working to integrate the region into the Russian Federation.[637] Their campaign centered around a covert unconventional warfare operation. After identifying sympathetic locals (mostly disenfranchised ethnic Russians), they put together a proxy force comprised of a variety of groups – local hooligans, want-to-be political leaders, and even Russians from Russia. Then "unidentified men in black uniforms" seized government buildings, including the Crimean parliament, and installed Sergei Aksyonov as the new prime minister of Crimea. SOF operators seized other strategic infrastructure, including the headquarters of the Ukrainian Navy in Sevastapol,

the headquarters of the Tactical Aviation Brigade in Belbek, and the Marine Battalion in Feodosia. *Spetsnaz* personnel were also involved in several of these operations.[638] Finally, Russian forces seized all military bases and infrastructure on the peninsula. Within a few short weeks, an entire territorial objective had been seized and politically integrated into the Russian Federation, almost with no shots fired.

The final case study started immediately following the seizure of Crimea, when separatist movements emerged in eastern Ukraine, particularly Donetsk and Luhansk. The separatist forces of the Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR) began a new offensive on Ukrainian-controlled areas, claiming over 9,000 soldiers by summer 2015. From February 2014 to May 2015, *spetsnaz*, SOF, conventional forces, and Private Military Companies (PMCs) participated in the fighting in the Donbas against Ukrainian government security forces. Both *spetsnaz* units and Russian SOF (including the VDV, or Russian Airborne troops) were deployed in the region, along with conventional forces, though it is unclear exactly who was doing what. Given their mission sets, it is highly likely that both *spetsnaz* and SOF were organizing local insurgent forces, engaging in train and equip missions, and serving as military trainers in general. Additionally, it would be naïve to think that they were not also engaged in direct action missions.

One group that was intricately involved was led by Igor Girkin, who was in Ukraine under the alias Igor Strelkov (a surname derived from the Russian word for "shooter"). Strelkov made no efforts to hide the fact that he was engaged in unconventional warfare, with the goal of triggering an armed uprising and separatist movement that would ultimately allow eastern Ukraine to join Russia.[639] This retired FSB colonel led a group of more than 50 fighters, many of whom had been active in Crimea before showing up in eastern Ukraine. While not all had formidable fighting experience, the majority did, with several members even coming from the elite *spetsnaz* GRU.[640]

Juxtaposed to the quick and nearly bloodless seizure of Crimea, which can be seen as a successful special operation from Putin's point of view, the battle for eastern Ukraine is part of a protracted UW campaign that continues under a new guise even to this day as part of Putin's "special military operation" in Ukraine.

Conclusion

Irregular warfare is not the sole domain of SOF. When it comes to conducting the military aspects of an IW campaign, however, SOF are the force of choice. In Russia it is not much different where, despite not labeling the activities as IW, SOF and *spetsnaz*

are employed to conduct a full range of operations and activities in order to "assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities." Similar, however, does not mean "the same," particularly when it comes to approaches between the West and Russia to conducting special operations. While this study highlighted some of the similarities in this arena, through the examination of four case studies, it also identified significant differences. For instance, Russian special operators seem to place little value on the lives of hostages in CT missions, viewing them simply as collateral damage. And, when it comes to the effectiveness of command and control and joint operations (though improved as a result of the "New Look" reforms and the creation of the KSSO), Russian *spetsnaz* and SOF still have a way to go. Finally, the United States does not conduct UW as a means of acquiring territory as in Crimea and the Donbas.

U.S. and NATO approaches to irregular warfare therefore clearly differ from that used by Russia. In fact, when it comes to conducting even very similar activities–such as counterterrorism–the way *Al'fa* approaches the mission (think of the Nord Ost' theater attack) is very different indeed from the way U.S. SOF would conduct similar missions. In the end, an examination of the Russian approach to irregular warfare sheds light on Russia's "special" way of war.

Though the case studies here are somewhat historical, there is a clear evolution of Russian IW over the past twenty years, with the formation of the Russian Special Operations Forces Command created right at the halfway mark (2012). While it is impossible to predict the future, the course of Russia's "special military operation" in Ukraine has seen the misemployment of SOF, *spetsnaz,* and airborne forces, all of which have been used as light infantry rather than in their intended roles. This is a trend that is likely to continue, as there seems to be no institution capable of compelling commanders on the ground or Vladimir Putin back in the Kremlin to utilize these specialized units for the missions for which they were intended. But if Russia does seek to expand the war beyond the currently-occupied regions of Kherson, Zaporizhzhia, Luhansk, and Donetsk into Kharkhiv and Odesa–and perhaps Transdniestria–SOF and spetsnaz are mostly likely to be employed in their capacity as leaders of unconventional warfare. In the end, this might be the future of the Kremlin's approach to irregular warfare and Russia's "special" way of war.

About the Author

Dr. Christopher Marsh is an associate professor at the Joint Special Operations Master of Arts (JSOMA) program at Fort Liberty, a division of the College of International Security Affairs of the National Defense University. Marsh is an expert on Russian approaches to special operations, irregular warfare, military strategy, and foreign policy. Prior to joining NDU, Dr. Marsh was the Director of the Department of Strategic Research & Analysis at the Joint Special Operations University, U.S. Special Operations Command (USSOCOM). He previously held positions at the U.S. Army School of Advanced Military Studies (SAMS), U.S. Air Force Special Operations School, and Baylor University.

Discussion Questions:

1. Why did it take Russia so long to establish a SOCOM-like coordinating organization?
2. Are Russian SOF the same as U.S. SOF? What about Russian *spetsnaz*? What makes them similar and what makes them different?
3. Does Russia use the concept of irregular warfare? Why or why not?
4. What are the equivalent missions of counterterrorism and counterinsurgency in Russian doctrine?
5. What similarities and differences that exist between Russian and U.S. special operations related to irregular warfare?

Recommended Reading:

- Tor Bukhvoll, "Military Innovation under Authoritarian Government – The Case of Russian Special Operations Forces," *Journal of Strategic Studies*, Vol. 38, No. 5 (2015), 602-625.

- Tor Bukhvoll, "Russian Special Operations Forces in Crimea and Donbas," *Parameters*, Vol. 46, No. 2 (2016), 13-22.
- Christopher Marsh, *Developments in Russian Special Operations: Russia's Spetsnaz, SOF, and Special Operations Forces Command* (Kingston, ON: Canadian Special Operations Forces Command, 2016).
- Alexsey Nikolsky, "Russian Special Operations Forces – Eight Years and Three Wars," in *Elite Warriors: Special Operations Forces from Around the World*, eds. Ruslan Pukhov and Christopher Marsh (Minneapolis: East View, 2017), 20-34.

Climate Change, Conflict, and Instability: Implications for Irregular Warfare

Sam Mullins

ABSTRACT

This chapter explores the implications of climate change for potential conflict and instability, with a particular focus on irregular warfare (IW). It begins with a brief overview of the direct, physical effects of climate change before exploring key vulnerabilities and risk factors for political instability, including: 1) climate-sensitive economies; 2)a recent history of political violence; 3) the presence of "identity-based" movements; and 4) discriminatory political institutions. This is followed by a discussion of four flashpoint issues that are likely to become increasingly salient as climate change continues and which have potential to foment irregular warfare activities: 1) climate change responses; 2) geopolitical competition in climate change affected areas; 3) water security; and 4) mass migration. The chapter concludes with a discussion of the implications of climate change for the future of IW. One way or another, climate change will shape the future environment within which IW is conducted. We ignore this at our peril.

Introduction

According to the United Nations Intergovernmental Panel on Climate Change (IPCC), human-induced climate change, characterized by a rise in weather and climate

extremes, has already led to widespread adverse impacts on both natural and human systems, some of which are irreversible.[641] Even in the most optimistic future scenarios, it is believed that global warming will soon surpass the internationally agreed-upon goal of 1.5 degrees Celsius above pre-industrial levels, which would limit the worst effects of climate change.[642] As former Vice President of the United States and environmentalist Al Gore has observed, "the science is clear."[643] What is less clear, however, is what this means for the future of international security and irregular warfare (IW).

Despite predictions in the 1980s of disruptions in agriculture and rising sea levels that could cause "massive refugee problems," for example, the potential security implications of climate change were left largely unexplored until the early 2000s.[644] A report commissioned by the U.S. Department of Defense Office of Net Assessment in 2003 suggested that an "abrupt" climate change scenario—though it is "not the most likely"—could disrupt food, water, and energy supplies, with the potential to "destabilize the geo-political environment, leading to skirmishes, battles, and even war."[645] In 2007, the UN Security Council held its first debate on the security implications of climate change at which then-Secretary-General Ban Ki-Moon outlined several "alarming, though not alarmist" scenarios involving conflict around shortages of food, energy, and water, as well as increased mass migration.[646] That same year, a group of retired flag and general officers serving on the military advisory board of the CNA Corporation argued that climate change acts as a "threat multiplier" for instability, particularly in more volatile regions of the world.[647]

Since then, the number of reports produced by governments, think tanks, and academics exploring the security implications of climate change has steadily grown. There now appears to be fairly widespread consensus that climate change can indeed act as a threat multiplier, meaning that it may complicate and exacerbate existing sources of instability, even if it is not the primary cause. Nevertheless, there is continued uncertainty about the underlying causal mechanisms involved (which are likely to be highly complex and context-dependent), as well as the probability, distribution, and scale of effects. Moreover, few studies appear to have considered the implications of climate change for the future of IW specifically.[648] This chapter aims to make a modest contribution to addressing that gap.

The chapter begins with a brief overview of the direct, physical effects of climate change before exploring key vulnerabilities and risk factors for instability and conflict. This is followed by a discussion of four flashpoint issues that are likely to become increasingly salient as climate change continues and which also have the potential to

foment IW activities: 1) climate change responses; 2) geopolitical competition in climate change affected areas; 3) water security; and 4) mass migration. The chapter concludes with a discussion of implications for the future of IW, broadly defined in accordance with the Irregular Warfare Annex to the U.S. National Defense Strategy as "a struggle among state and non-state actors to influence populations and affect legitimacy."[649]

Direct Impacts of Climate Change: A Brief Overview

Climate change is characterized by long-term increases in global temperatures and shifting weather patterns.[650] Although future outcomes cannot be predicted with absolute certainty, and there will be significant geographic variability, the consequences of climate change are wide-ranging, and are expected to intensify in coming decades as global warming continues. Sea-level rise as a result of melting ice sheets, and the physical expansion of seawater volume caused by warmer temperatures, presents a direct and steadily increasing threat to low-lying coastal areas and islands.[651] Natural disasters such as floods, droughts, storms, landslides, heatwaves, and wildfires have already surged five-fold in the last fifty years and are expected to continue to increase in frequency and intensity.[652] Although associated fatalities have declined substantially, thanks to better early warning systems and disaster management, the physical damage and economic costs entailed have increased exponentially.[653] As climate change intensifies, conditions will also be ripe for the increasing spread of infectious diseases, such as malaria and dengue, and are expected to increase the risk of future pandemics.[654]

The picture looks bleak for humanity. Rising temperatures, varied and unpredictable precipitation, and changes in soil composition are predicted to result in declining output of key crops, such as corn and rice.[655] Fish stocks, already under pressure from overfishing, will also be impacted by the warming and acidification of the oceans, which is forcing fish to migrate in the short to mid-term, and raises the risk of extinction over the long-term.[656] Environmental degradation and increasing loss of biodiversity are expected to accelerate, upsetting delicate ecospheres and threatening human food, health, and economic security.[657] At the same time, the global population will continue to expand (particularly in coastal, urban areas) placing an additional strain on the ability of governments to adapt and provide for growing demand.[658] Meanwhile, both the quantity and quality of freshwater supplies will be placed at risk in a number of ways, including through the melting of glaciers, more frequent droughts, the destruction of infrastructure, and saltwater intrusion of coastlines.[659]

In the wake of these developments, which will disproportionately impact the developing world, a significant increase in human displacement is likely as more and more people are forced or otherwise feel compelled to leave their homes as a result of climate-change induced conditions. Although the majority of this trend is likely to take the form of internal displacement *within* countries, large-scale cross-border climate migration remains a distinct possibility.[660]

Even if some of these outcomes can be partially mitigated, there are likely to be wide-ranging social, political, and economic repercussions. Indeed, adapting and responding to the combination of multiple, cascading challenges that lie ahead is likely to present enormous difficulties, even for the most capable of states. Resources and capacity (including military readiness) will almost certainly come under increasing strain and governments will be faced with difficult choices.[661] The central challenge will be to find a way of effectively managing these crises and providing for the basic needs of the population, while at the same time maintaining the stability and legitimacy of the state.

From Climate Change to Political Instability and Conflict: Key Vulnerabilities

The direct impacts of climate change are destabilizing, presenting a significant threat to critical infrastructure and the well-being of populations. As noted above, developing countries, which have fewer resources available to cope with such challenges, will bear the brunt of the environmental impacts of climate change. The IPCC identified the main global hotspots of vulnerability as: East, West, and Central Africa; South Asia; South and Central America; Small Island Developing States (which are scattered across the Caribbean, Pacific, Atlantic, Indian Ocean and South China Sea); and the Arctic.[662]

Going beyond geographic and economic vulnerabilities to the physical effects of climate change, it is important to acknowledge that predicting social and political consequences is fraught with uncertainty. Nevertheless, there are several factors that are likely to amplify the adverse effects of climate change and increase the risk of political instability. The first is a high dependence on climate-sensitive livelihoods, such as agriculture and fishing.[663] If these industries are disrupted in countries where substantial proportions of the population depend on them for income—which applies to much of the developing world, including countries such as Somalia, Syria, and Afghanistan—the resultant rise in food insecurity, unemployment, and popular discontent is likely to be much greater.[664]

A second important risk factor is a recent history of violent conflict, which, as researchers John Busby of the University of Texas and Nina von Uexkull of Uppsala University argue, is probably the best predictor of outbreaks of conflict in future.[665] Related to this, Andrea Malji and colleagues at Hawaii Pacific University point to the significance of "identity-based movements," which may include militant/terrorist organizations as well as political actors, such as India's Hindu nationalists, that have a history of exploiting divisive issues and demonizing minorities.[666] Both sets of actors may try and exploit national crises caused by climate change, such as food insecurity or mass migration, to their advantage, thus contributing to worsening political instability and potential violence.

The third risk factor for climate-change related instability—one of critical importance—is weak and/or divisive governance, where states fail to provide goods and services to their population or do so in a way that systematically marginalizes certain groups or excludes them from power.[667] How states respond to crises will be key to public and international perceptions. If they are found to be inept, corrupt, or, worse still, deliberately discriminatory in the way they respond, that will give rise to a profound sense of grievance and marginalization on the part of excluded groups, running the risk of further polarizing society. Such conditions are ripe for exploitation by both state and non-state actors who wish to further undermine the legitimacy of the government.

Although any one of the above factors may significantly increase the risk of political instability and conflict, the risk is highest when they are present in combination. Using this framework, Busby and von Uexkull identified 20 countries, spread across Africa and South Asia, that exhibited a high dependence on agriculture and had bouts of recent conflict—among them, Mali, Ethiopia, Somalia, Mozambique, India, and Afghanistan.[668] They found a further nine countries where all three risk factors were present and where climate change is therefore especially likely to lead to "disastrous outcomes" in decades to come, including food crises, large-scale displacement, and violence. These countries are Angola, the Democratic Republic of Congo, Rwanda, Sudan, South Sudan, Uganda, Yemen, Pakistan, and Myanmar.

By comparison, the recent National Intelligence Estimate (NIE) on climate change identifies two regions, consisting of much of Sub-Saharan Africa and the Pacific Islands, and 11 "highly vulnerable countries of concern" where there is heightened risk of social, economic, and political instability resulting from the effects of climate change. These 11 include: Iraq, Afghanistan, Pakistan, India, Myanmar, North Korea, Colombia, Guatemala, Haiti, Honduras, and Nicaragua.[669] Notably, many of the countries

identified as being the most at-risk to climate change-related instability are also touched by, or involved in, some aspect of IW (from counterinsurgency to state-sponsorship of organized crime and terrorism) and are also of geostrategic significance. The specific types of risks and associated threats yet to emerge will, of course, vary from country to country, but in the vast majority of cases, they will most likely be irregular in nature, below the threshold of conventional war.

Flashpoint Issues Amid a Changing Climate

In addition to country-level risk factors that increase the likelihood of climate change-related instability, it is useful to identify other potential flashpoint issues that are likely to emerge as points of contention. Each of these issues are both extremely politically sensitive, and are expected to become increasingly prominent in coming decades as climate change accelerates. They include (though are not necessarily limited to): climate change responses; geostrategic competition in climate-change affected areas; water security; and mass migration.

Climate-Change Responses

Climate change itself has long been a contentious issue, subject to intense disinformation campaigns by a variety of state and non-state actors.[670] While debates about whether or not it is occurring, and whether human activity is to blame, appear to have largely disappeared from credible scientific discourse in the face of overwhelming evidence, they do persist on social media and elsewhere.[671] Meanwhile, attention is increasingly turning to climate change responses, which are fast becoming a matter of increasing geopolitical tension.[672]

The NIE identifies several ways in which climate change responses may contribute to tensions among countries, including: a perceived, or actual, lack of effort by states to reduce carbon emissions; pressure (and resistance) to transition away from fossil fuels; potentially divisive climate-related economic policies, such as the European Union's Climate Border Adjustment Mechanism, which will levy a carbon border tax on goods imported from outside the EU; competition with China over key resources and technologies needed for renewable energy, such as rare earths and minerals used in wind turbines and electric vehicle batteries; and the rising risk of unilateral attempts at geoengineering using technologies such as stratospheric aerosol injection or marine cloud brightening, which could be used to reduce climatic temperatures, but may also result in unequal disruption of weather patterns that favors some regions at the

expense of others.[673] Alluded to, but not explicitly stated in the NIE, is that these kinds of tension around climate change responses may also create opportunities for IW. For example, the document notes that, "China is the world's leading supplier of advanced grid components for ultra-high-voltage systems, [needed for utility-scale solar and wind grids], which we assess creates cyber vulnerability risks."[674]

Since the environmental and economic impacts of climate change and associated responses are unevenly distributed among state and non-state actors with competing interests and priorities, with varying capacity to be able to adapt, they are highly politicized and inherently divisive.[675] This presents ample opportunities to spread disinformation aimed at exploiting these divisions and influencing the policies of competitors. For example, a House Science, Space, and Technology Committee report found that, from 2015 to 2017, Russia made extensive use of social media to try and influence U.S. energy policy, using more than 4,000 online accounts to comment on the Dakota Access Pipeline, government efforts to curb global warming, and hydraulic fracturing, or "fracking."[676] It takes little imagination to realize that similar efforts could be made to try and drive a wedge between the United States and its allies, for instance, in relation to carbon emissions or economic policies, or to spread conspiracies about geoengineering designed to blame adversaries and distract from inept responses to climate-related natural disasters.[677]

Non-state actors are another important part of this equation. Eco-activists play a critical role in raising awareness, protesting unjust and harmful practices, and pressuring governments into taking more concerted action. Increasingly, they are victims of government oppression, targeted violence and assassination.[678] According to Global Witness, an international non-governmental organization that works to expose environmental and human rights abuses, more than 1,700 eco-activists were killed from 2012 to 2021, with more than half of those attacks occurring in Brazil, Colombia, and the Philippines.[679] However, activists have also been responsible for significant civil disorder, economic disruption, sabotage, and damage to critical infrastructure. For example, the Extinction Rebellion protests in the United Kingdom resulted in extensive damage to property, and reportedly cost London's Metropolitan Police more than £60 million from 2019-2022.[680] In the United States, climate activist Jessica Rae Reznicek was sentenced to eight years in prison for sabotaging the Dakota Access Pipeline, which the judge described as a "federal crime of terrorism."[681] As climate change becomes increasingly acute, and the perception grows that governments and corporations are not doing enough, there is concern that more violent and disruptive groups may (re)emerge on the fringes of this movement, to potentially include "eco-terrorists" motivated by

environmental concerns.[682] Not only is such a trend potentially destabilizing in itself, but again presents opportunities for further exploitation by malign state actors. Russia, for instance, has repeatedly been accused of covertly funding environmentally-focused, non-governmental organizations in Western countries. This claim was at least partially debunked by the *Washington Post*, which found no evidence to support claims made in the case of the California-based charity, Sea Change Foundation (which was at the center of allegations made in the United States), having received Russian funds.[683] However, given Russia's long history of manipulating activist movements for political gain, the possibility that the Kremlin, or other actors, would resort to such tactics in the future cannot be discounted.[684]

Geostrategic Competition

As climate change alters physical environments, it is likely to create new challenges as well as opportunities for states in particular to acquire territory and resources. As states seek to gain strategic advantage within the same, contested spaces, there will be a risk of both military and non-military clashes, particularly where institutions, rules, and norms fail to keep pace with changing operational circumstances.

Nowhere is this more apparent than in the Arctic. In the High North, global warming is happening at a faster rate than anywhere else in the world and, as the ice melts, a range of both Arctic and non-Arctic states—including the United States, Russia, and China—are already jostling to position themselves to take advantage of new economic opportunities.[685] Military activity in the region is also increasing in the form of training, exercises, deployments, missile tests, and a variety of air and naval operations.[686] According to the NIE, this will result in a "modest" risk of miscalculation by 2040, as rival military forces increasingly operate in proximity with one another in the region.[687] A more detailed report by the Center for Climate Security (CCS), in collaboration with the Norwegian Institute of International Affairs, argues that the risk of misunderstandings and potential conflict in the Arctic will depend on the future pace of climate change, with more rapid change likely to result in more intense competition.[688] The CCS report furthermore suggests that the anticipated increase in commercial shipping, fishing, and exploration of oil, gas, and minerals "expands the likelihood of states like Russia and China using civilian and commercial actors as vehicles for strategic positioning and for gray zone operations which may escalate to direct confrontation."[689] Another possible tactic that adversarial actors might use, should competition intensify in the Arctic,

would be to (mis)use bilateral and multilateral institutions, such as the Arctic Council, in order to gain unfair advantage or weaken opponents.[690] Indeed, Russia, China, and other authoritarian regimes have exploited their positions within institutions, such as the United Nations and Interpol, in order to pursue their interests in ways that undermine the very purpose of these organizations.[691] There is little reason to think that the Arctic will be different. Finally, the CCS notes that malign actor intentions to destabilize the Arctic may seek to mobilize or otherwise exploit aggrieved populations, particularly indigenous communities, whose way of life is increasingly threatened by the encroaching threats of climate change and local oil exploration.[692]

Although the Arctic is perhaps the most obvious arena for emerging geostrategic competition in the context of climate change, it is important to recognize that global warming will complicate, if not exacerbate, the situation in places that are already hotly contested. For instance, the South China Sea—an area where China already makes extensive use of irregular means, such as building artificial islands and deploying maritime militias, to further its strategic objectives—is especially vulnerable to the effects of climate change. One anticipated outcome of climate change in this region is that fish stocks, already severely stressed by overfishing and harmful environmental practices, will migrate northwards toward the East China Sea and Sea of Japan in search of cooler waters.[693] At the same time, rising ocean levels will increasingly threaten low-lying and artificial islands, imperiling the associated military and economic advantages they afford.[694] In combination, these factors will add to regional uncertainty, and potentially add to existing geopolitical tensions as countries seek alternative ways of securing increasingly scarce resources for their respective populations.

Climate change will intersect with geostrategic competition in other important regions, such as the Pacific Islands, where for some countries a rise in sea-levels presents an existential threat. Although this seems unlikely to lead to armed conflict, the increasing vulnerability of affected states might make them more susceptible to various forms of manipulation or coercion, which could in turn result in an escalation of tensions between the United States and China.

Water Security

As noted above, the threats posed by climate change to global water security are extensive, including melting glaciers, an increased risk of more extreme flooding and droughts, and the potential contamination of freshwater supplies. These phenomena pose a threat to both food and energy security, and could jeopardize the livelihoods of millions of people around the world. Moreover, as highlighted in the NIE, "nearly

half the world's 263 international river basins—encompassing about half the global population—lack cooperative management agreements to help defuse tensions in shared basins," while existing agreements lack the flexibility needed to account for climate change.[695] Without discounting the possibility that new forms of cooperation could emerge, the potential for water to become a mounting source of tension in future is high, particularly in areas of pre-existing hostility.

One area that stands out is the Tibetan Plateau—known as the "Water Tower of Asia" due to the number of major rivers that originate there, including the Brahmaputra, Yangtze, Yellow, Ganges, Indus, and Mekong—which provide water to billions of people across South and Southeast Asia.[696] China, which has the advantage of being the upstream state, has built an extensive network of dams (with more on the way), giving it "unilateral control" over these vital and dwindling water sources on which downstream nations rely.[697] Moreover, China is facing severe water shortages already, and has very limited water-related agreements in place with countries to its south. As a result, countries such as India have expressed concern that China may seek to divert, withhold, or suddenly discharge large volumes of water in the future, and potentially use this power as leverage in geopolitical disputes.[698] A broader concern is that if water levels eventually drop in China, to the extent that agriculture suffers, Beijing could be forced to import large quantities of food, thus driving up world food prices and resulting in widespread social unrest.[699]

Of course, China is not the only nation maneuvering to secure water resources with an eye on mitigating the effects of climate change. Downstream nations are building their own dams, causing similar anxiety among lower riparian states, and enflaming old rivalries. In August 2021, India's Standing Committee on Water Resources recommended to the Lok Sabha that the Indus Water Treaty (which governs its sharing of the Indus River Basin with downstream Pakistan) should be renegotiated in light of climate change, with a view to maximizing Delhi's ability to exploit the irrigation and hydropower potential of all six of the entailed rivers.[700] The response in Pakistan was decidedly negative, with one headline proclaiming, "India plans to resort to water terrorism in region."[701] India has in the past threatened to restrict water flows to Pakistan in retaliation for alleged acts of state-sponsored terrorism on its soil.[702] Meanwhile, both Pakistan and Iran have been accused of sabotaging dams located in neighboring Afghanistan, which is itself severely water-stressed, that would threaten their water security, and are highly vulnerable to climate change.[703]

The increasing scarcity and/or variability of crucial water supplies can also threaten internal state stability. One of the most oft-cited and widely accepted examples of such

issues is in the Lake Chad Basin in West Africa, which borders Nigeria, Niger, Cameroon, and Chad. Climate change, combined with overuse of water and land and aggravated by rapid population growth, has contributed to the dramatic shrinking of Lake Chad since the 1960s.[704] Although the lake has largely stabilized in size over the last two decades, increasing variability in precipitation brought on by climate change has resulted in the disruption of critical water resources, and associated livelihoods.[705] Exacerbated by weak governance, and inadequate conflict resolution mechanisms, the disruption of available water supplies has led to growing resource competition and rising levels of violence between sedentary farmers and nomadic herders, which has resulted in many hundreds of deaths and thousands more displaced.[706] Worse still, the terrorist organization Boko Haram, and its offshoot the Islamic State West Africa Province, have exploited this situation to drive recruitment, further adding to the instability of an already-stretched region.[707] Though far from being the main explanation for its rise, the Islamic State was able to capitalize on climate change-related droughts and unemployment to rise to prominence in Iraq.[708] Amid similar circumstances in Mexico, the Sinaloa drug cartel has begun siphoning off water from rivers, and hijacking water tankers, in a move to control the increasingly valuable resource.[709] As one cartel member commented, "[w]ater is now a valuable asset for us, and as it becomes more scarce, the more we will fight to make sure we have enough."[710]

Examples such as these illustrate extreme possibilities, but do not necessarily imply a significant increase in terrorism, insurgency, or organized crime as a result of rising water insecurity. Far more often, states will be faced with non-violent protest movements and occasional civil disorder, which are already on the rise in relation to water, particularly in South Asia and South America.[711] However, it is reasonable to assume that as water security becomes more salient as an issue, it will increasingly factor into the motivations and decision-making of both violent and non-violent activists. Moreover, present challenges in terms of governance may potentially be exploited by adversaries at a time when inter-state relations are already under strain. Rising water insecurity as a result of climate change will thus present myriad opportunities for IW, ranging from "weaponization" of water sources as a means of coercion, to the manipulation of legitimate protest movements to deepen the contradictions in a targeted society.

Mass Migration

While estimates vary widely, it is generally believed that global migration will increase substantially as a result of climate change, particularly after 2030.[712] According to the Institute for Economics and Peace, as many as 1.2 billion people will be at risk

of displacement by 2050 due to a combination of worsening ecological threats and low societal resilience, magnified by the realities of climate change.[713] Not all of these people will actually be displaced, and most of those that are will most likely remain within their own countries. Nevertheless, even the threat of large-scale internal displacement can still be socially, politically, and economically destabilizing. Cross-border migration, which is viewed as being more problematic, could also increase.

While migration does not necessarily result in conflict in itself, there is strong overlap between countries experiencing conflict and population displacement, and those most at risk of the effects of climate change.[714] For countries that receive large numbers of immigrants, in particular, few issues are as polarizing as migration, and it often becomes the focus of intense national debate and political upheaval, as seen recently in both the United States and Europe. In some instances, migration has resulted in widespread violence. A case in point is the state of Assam in northeast India, where an influx of migrants from Bangladesh has already resulted in intercommunal violence on several occasions, and where climate change may thus play an aggravating role in future.[715] Though climate change will not necessarily increase a propensity toward violence, it may play into local hostilities centered around issues such as access to land, and it will increasingly test local, national, and international governance mechanisms, which are currently ill-prepared for climate-induced migration of the type or scale that is projected.

From an IW perspective, it is important to recognize that migration can be exploited by a range of state and non-state actors.[716] Russia's infamous Internet Research Agency, for example, sought to exploit immigration in North America and Europe in an effort to sow political discord and weaken internal cohesion.[717] More concerning still have been moves to "weaponize" migration flows, by a variety of state and pseudo-state actors, by encouraging and facilitating migration flows toward particular countries, in an effort to gain leverage, extract concessions, or simply weaken their opponents.[718] Recently, demonstrated in the starkest of terms by Belarus which brought in thousands of Syrian, Iraqi, and Afghan migrants with the intention of pushing them into the European Union, this tactic has been surprisingly common, and successful, throughout modern history.[719] The expected climate-induced surge in migration, combined with climate change's other deleterious effects on national economies and international relations, is likely to make this tactic even more appealing.

Organized criminals and terrorists may also stand to gain from an increase in irregular migration.[720] Human smugglers, in particular, would gain financially, and as

argued in a recent White House report on climate change and migration, "smuggling operations will likely lead to a net increase in state corruption in countries of origin, transit, and destination while correspondingly contributing to the erosion of state stability."[721] Criminals and terrorists have exploited migration flows in a number of other ways, including trafficking, recruitment, propaganda, and infiltration of destination countries.[722] During the 2014-2016 migrant crisis in Europe, for instance, the Islamic State discouraged migrants from going to "the land of disbelief" in propaganda videos, while simultaneously infiltrating migration flows in order to conduct attacks.[723] Meanwhile, Mexican cartels routinely kidnap and extort Central American migrants headed to the U.S. southern border, sometimes also forcing them to act as drug mules.[724] The mutual interest that criminals and terrorists have in exploiting these flows furthermore brings them closer into contact with one another, creating additional space for convergence between the two.[725] In this way, terrorists can expand their rolodex of criminal contacts, needed for the forgery of documents and smuggling of operatives across borders, while organized criminals further increase their profits.[726]

In places where violent non-state actors are able to establish some degree of control over irregular migration flows, there will be a demand for counter-organized crime, counterterrorism (CT), and other forms of security assistance. If given the opportunity, adversarial states could exploit these governance demands in a variety of ways, not least to expand their influence using private military companies, selling invasive surveillance technology, and promoting authoritarian approaches to security, which are likely to make the situation worse.[727]

Findings and Implications for the Future of Irregular Warfare

One way or another, climate change will shape the future environment within which IW is conducted. Therefore, IW and climate change must not be viewed in isolation from one another.[728] At a minimum, this interplay between IW and climate will require building what the Department of Defense (DoD) has referred to as "climate literacy" among those involved in IW in order to better comprehend both the broad impacts of climate change, as well as specific anticipated effects in particular domains.[729] A climate literacy effort must extend from the strategic, down through operational and tactical levels, from understanding which countries or regions may be most at-risk for climate-change related instability, to adapting plans, policies, training, and equipment to be able to operate under more extreme environmental conditions.

A related, and equally important point, is that climate change both shapes and will be shaped by strategic competition. Competitors such as China and allies such as India

will have vital roles to play in curbing global warming. Key battlegrounds for strategic influence—including the Arctic, the Pacific Islands, and the South China Sea—are also among the most vulnerable to climate change. And, as discussed, climate change will present myriad opportunities for states to exert strategic influence, including by irregular means. In this respect, climate change should be looked at as both a challenge and an opportunity. Whereas adversaries may seek to take advantage of climate change-related vulnerabilities to advance their interests at the expense of others, the United States and its allies have an opportunity to counter—or better yet preempt—such efforts, while advancing principles of good governance and security. Where IW capabilities are employed (from CT to military information support operations), they must be assessed not as standalone missions that are mutually exclusive of broader strategic efforts, but with the interplay between climate change, IW, and strategic competition in mind.[730]

A third observation that emerges from this discussion is that while conventional conflict between states resulting from the effects of climate change remains a possibility, it seems far more likely that the majority of adversarial actions will take place within the irregular domain. Conceivably, all of the "traditional" IW mission sets–CT, counterinsurgency, unconventional warfare, stabilization operations, and foreign internal defense—could be called upon. In particular, however, the circumstances created by climate change will probably be contested most readily in the information space.

Besides information operations, other tactics that adversaries might employ include cyberattacks, deception, economic coercion, lawfare, sabotage, the weaponization of water or migration, and the use of proxies—potentially ranging from unwitting climate change protestors to criminal gangs and terrorist organizations. This is important because much of the literature until now has tended to focus on the implications of climate change for more traditional forms of security and has largely ignored IW.[731] This is a gap in existing research that must be addressed. On a more practical note, a "no-holds barred" approach to IW likely to be employed by authoritarian competitors, who are not bound by legal or ethical constraints, suggests the need for a more comprehensive response. DoD has already argued for a "revised understanding" of IW that dispels the perception that IW is the sole responsibility of special operations forces and furthermore encompasses the non-military side of adversarial competition.[732] However, it is unclear that this message is gaining traction. Yet, if IW is to proliferate in response to climate change as this analysis suggests it could, it will be important to develop a more coordinated, interagency approach.

Concluding Remarks

The future effects of climate change are both complex and uncertain. How exactly it will impact global security and irregular warfare is unknown. Accordingly, the U.S. intelligence community has expressed, "low to moderate confidence in how physical climate impacts will affect U.S. national security interests and the nature of geopolitical conflict, given the complex dimensions of human and state decisionmaking."[733] Nevertheless, analyses dating back to the early 2000s have repeatedly shown that climate change has significant potential to foment political instability. This chapter has sought to add to this discussion by highlighting the implications for IW. While more research is undoubtedly needed, the analysis suggests that climate change could indeed shape the future of IW in important ways. We ignore this at our peril.

About the Author

Dr. Sam Mullins is a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI APCSS) in Hawaii. Previously, he was a professor of counter-terrorism at the George C. Marshall European Center for Security Studies in Germany where he was awarded the Superior Civilian Service Award in March 2019. Dr. Mullins has spoken at numerous international conferences around the globe and has presented his work for a variety of government agencies including the FBI, the NYPD, the Canadian Security Intelligence Service, the Australian Federal Police, the International Special Training Centre in Germany, the NATO Centre of Excellence - Defence Against Terrorism institution in Turkey, the Chinese Ministry of Public Security and the Indonesian National Armed Forces, among many others. He holds an MA (Hons) in Psychology from the University of Glasgow, Scotland; an MSc in Investigative Psychology, with distinction, from the University of Liverpool, UK; and a PhD from the University of Wollongong, Australia. He is the author of two books: *'Home-Grown' Jihad: Understanding Islamist Terrorism in the US and UK,* and *Jihadist Infiltration of Migrant Flows to Europe: Perpetrators, Modus Operandi and Policy Implications.*

Discussion Questions

1. Of the countries and regions which are most vulnerable to climate change, which of these is particularly at risk of political instability and conflict? In what ways might IW be relevant?

2. Which particular IW missions or activities do you think might be most relevant as climate change intensifies?

3. Four flashpoint issues that may lead to political instability discussed in this chapter include: climate change responses; geostrategic competition in climate change affected areas; water security; and mass migration. What other issues do you think are important, with particular relevance to IW?

4. Some of the tactics that adversaries might employ to take advantage of climate change include disinformation, cyberattacks, deception, economic coercion, lawfare or legal warfare, sabotage, the "weaponization" of water or migration, and use of proxies—potentially ranging from unwitting climate change protestors to criminal gangs and terrorist organizations. How can the United States and its allies best respond to such tactics?

Recommended Readings

- Chad Briggs, (2020) "Climate Change and Hybrid Warfare Strategies" *Journal of Strategic Security*, 13(4), 45-57.
- International Military Council on Climate and Security, *The World Climate and Security Report 2021* (Washington, DC: The Center for Climate and Security, 2021).
- National Intelligence Council, *National Intelligence Estimate: Climate Change and International Responses Increasing Challenges to US National Security Through 2040* (Washington, DC: Office of the Director of National Intelligence, 2021).
- *Report on the Impact of Climate Change on Migration: A Report by the White House* (Washington, DC: The White House, 2021).

The opinions expressed in this article are the author's alone and do not necessarily represent the official position of the Daniel K. Inouye Asia-Pacific Center for Security Studies or the U.S. Department of Defense.

Total Defence: Nordic and Baltic Perspectives on Irregular Warfare

Ulrica Pettersson and Col (R) Hans Ilis-Alm

ABSTRACT

A constantly and rapidly changing threat environment, not least in times short of war, demands a realistic perception of what the future may hold in terms of new threats as well as new opportunities. A prerequisite to being able to adapt is, however, to recognize and understand the need for adaptation.

In this chapter, we seek to illuminate challenges for a small state with limited resources in the contemporary and future security environment. We have chosen to focus on special operations forces (SOF) as one of a nation's strategic resources. We discuss three conceptual ways of utilizing special operating forces in a Total Defense concept: 1) domestic security; 2) resilience and resistance; and 3) preparations for war. These serve as examples of how small states could enhance their capacity to both conduct and counter irregular warfare. The eternal challenge for a small state is how to achieve maximum effect from its limited resources. We argue that SOF will thus be invaluable irregular warfare assets to small states in the context of their comprehensive security and Total Defense.

Introduction

Irregular warfare (IW) is far from a new phenomenon; nevertheless, it has to some extent changed in character over time. Charles Black and David Ellis argue that a modern IW consortium needs to move beyond existing doctrines and paradigms of

power in order to develop knowledge networks and promote creativity and innovation. There seems to be some confusion, and little common understanding or definitions, regarding irregular, hybrid, and asymmetric warfare.[734] However, in hierarchical and control-oriented organizations, such as armed forces, IW is repeatedly defined in a manner similar to the United States Department of Defense joint publication which defines it as: *"A violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. 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 present it is applied in all domains and during the entire conflict scale."*[735]

For small states, the doctrinal approach of a great power, such as the United States, is not always fully appropriate. Despite that, the essence of the traditional definition above can be applied to IW in general, regardless of the size of state engaging in it. States that aspire to build a resilient and comprehensive defense should apply a whole-of-society approach to national security. Consequently, building Total Defense requires the coordinated participation of the military, paramilitaries, police forces, all branches of government, the private sector, and last but not least, the general population.[736] Small states, by nature, have limited resources to counter a multi-faceted array of threats, and therefore, they need to choose wisely to find the synergies within their toolbox of comprehensive capabilities. In this chapter, we have chosen to focus on one of a nation's strategic resources and aim to highlight how special operations forces (SOF) could be utilized both to conduct IW and to counter an adversary's IW. We argue that SOF will be an invaluable asset in the IW context of Comprehensive Security and Total Defence in the Nordic-Baltic High North. In order to exemplify a small state perspective, we will primarily use Sweden as an example in this chapter. However, what will be discussed also relates to other small states in the Baltic Sea region (BSR). Due to the geostrategic conditions in the Nordic-Baltic High North, Russia is assessed to constitute the primary threat and is therefore perceived as the potential aggressor.

Ever since the end of the Cold War, and influenced by the cognitive views presented by, for example, Francis Fukuyama, the notion of a major war in Europe was for a long time seen as surreal.[737] Consequently, Defense Force expenditure in most European countries fell and the focus almost entirely shifted to expeditionary crisis management. In civil society, reductions in spending were even more dramatic. For example, prior to 1991, Sweden had a very solid and well-functioning preparedness in civil society framework, within the comprehensive whole-of-society concept of Total Defense.[738] This concept aimed at securing a strong resilience in the country in case of a deteriorating

security situation in the BSR. In Finland and Norway, comprehensive security concepts can also be found, even if neither of the concepts are identical to one another.[739] Total Defense is, as its name indicates, an inclusive concept aimed at resilience. From a cost/benefit perspective, it also aims at serving as a means to deter a potential aggressor from attacking.[740]

The Russian war against Ukraine, which started in 2014 and massively intensified in 2022, has served as a brutal wake up call for the rest of the world. It has proven the importance of societal resilience, and the strong interconnections that are necessary between civil society and its military forces. It is rather obvious that the Russian plan of attack in February 2022 was based on speed: a direct attack aimed at decapitating the Ukrainian leadership, taking control of vital infrastructure, then eliminating any resistance, before finally taking full control of the country.[741] Using Dr. Ivan Arreguin-Toft´s terms, a strong aggressor can either choose to use a direct attack or barbarism.[742] As we have seen, the direct attack concept failed and, as of this writing, the war has morphed into more of a protracted war utilizing all means possible. Russia has, in short, reverted to barbarism. According to Lt Gen (retired) Dennis Gyllensporre, "[w]eak and defensive actors can choose between two strategic options, a direct defense or guerilla warfare strategy."[743] In this war, Ukraine is utilizing a combination of direct defense and guerilla warfare. The approach chosen is related to the status of different parts of the country, namely, whether the area is occupied by Russia or controlled by Ukraine.[744]

A common historical error among nations, and their militaries, is to resist change and prepare for the last war.[745] Nevertheless, trends from the war in Ukraine, together with some relevant lessons learned from the major wars in our time, can give us indications of what and how nations need to prepare for the next war. Such a perspective should be valid stretching from now, to five to eight years hence. The interdependency between civil society and its military, when defending against an aggressor that is utilizing all means of power, is one important aspect. Another is that in asymmetric warfare, the weaker side needs to be innovative and utilize all resources that a nation has at its disposal. In Ukraine, this has been proven in many ways, not least in how civilian drone enthusiasts have been employed for targeting purposes.[746] A third observation is how the Ukrainian defense industry has worked in close connection with its military, modifying and improving existing weapons as well as developing new weapons with incredible speed.[747] In other words, it is of the utmost importance for a small state to utilize a whole-of-society approach to create the necessary resilience.

If the assumption is correct that the Western world, for a long time, has been in a conflict or competition just short of war with Russia (and China), a definite sense of urgency must now be applied.[748] The demands Russia made in its December 2021 letter, and the subsequent attack on Ukraine, have proven that Europe, not least the BSR countries, needs to prepare for a deteriorating security environment.[749] The actions taken during the phases short of war can serve dual purposes. They can act as deterrence and, in the case of aggression, can optimize the ability to resist. Furthermore, they can also be applied in countering any ongoing hybrid threats short of war.[750]

The period since 9/11, mainly characterized by counterinsurgency (COIN) and counter terrorism (CT) operations, has been what could be described as a boom for SOF. Two of Professor Colin Gray's master claims of strategic utility for special operations, *economy of force* and *expansion of choice*, make SOF a highly appealing asset to policy makers.[751] Further, Professor James Kiras argued that SOF was less about epic raids than they were about the combined effects they created during a campaign or series of campaigns. He claims that "special operations are not decisive, independent acts of war devoid of context."[752] Kiras also stresses that attrition also contains a moral dimension, which this chapter considers to be a vital part of resilience in a modern Total Defense concept. As most countries are now preparing for their national defense in a potential major conflict, SOF could constitute one important tool in a comprehensive toolbox.

Throughout history, SOF have been significantly susceptible to changes following periods where their strategic utility has been held in high regard.[753] There is a risk that the current and increasing competition for resources between the services may once again lead to the decline of SOF. The recipe to avoid that, and to continue to be of strategic utility, is for SOF to adapt to change and stay relevant in the context of a comprehensive Total Defense concept. The utility of SOF for small states is somewhat different from that of larger military powers for a variety of reasons, including the divergence in geostrategic conditions and the political willingness to use military force as a strategic tool.[754] However, one thing most states have in common is that SOF are normally a comparatively small resource to build and maintain, especially in terms of numbers.

Contextual Factors

In the BSR and the European High North, there are several contextual dimensions that constitute the strategic security environment of this region. The Baltic Sea, with

the Danish straits, is one of the busiest shipping areas in the world and is, therefore, of vital interest to all the BSR countries, including Russia.[755] The Arctic and subarctic areas of the Nordic countries border the Kola Peninsula, one of the most important Russian strategic basing areas. Military resources stationed on the Kola Peninsula are part of Russia's *Bastion concept* which aims to assert sea control and denial activities in the North Atlantic and beyond.[756] This strategy constitutes a Russian long-term interest in ensuring control of the region and, consequently, deny it to other actors. In an environment short of war, BSR countries should be prepared for Russian shaping activities within the concept of New Generation Warfare (NGW) to take place. These NGW activities aim at creating chaos throughout the country that is nevertheless carefully targeted, thereby facilitating the ensuing phases of conflict. In addition to different types of subversive methods, information operations will be one of the multiple tools used and it will play a significant role.[757] Proxy forces are another tool that can be used for sabotage, intelligence operations, and to support useful groups, such as criminal organizations and private military companies (PMC). Furthermore, Russian SOF could also be employed in such activities.[758]

The initial analysis of the contemporary war in Ukraine has shown that Russia planned for a quick decapitation of the political leadership through *kill-or-capture* missions with the use of its airborne forces.[759] Due to the efficient countermeasures deployed by the Ukrainian Security Services, this tactic failed. Logistics is an important and eternal factor that is always significant, and important in preparation as well as in the conduct of actual war. The Russian dependence on fixed railway infrastructure for their logistics system presented opportunities for sabotage, and Ukrainian deep precision strikes have proven to be highly effective.[760]

In a future deteriorating security environment, there are many situations in which SOF could be of strategic utility. In the following sections, we will discuss three conceptual ways of using SOF within a Total Defense approach: support to other agencies in domestic security, resistance operations (both internal and external), and preparations for war. Short of war, the above categories are generic settings in which small state SOF could be utilized to create strategic and operational effects, in both the contemporary and future BSR security environment.

During the competition phase, short of war, the security situation will probably not be isolated to the territory of a specific nation.[761] Furthermore, the situation will contain a wide spectrum of blurry fragments where conventional and unconventional methods are mixed and utilized by a number of quite divergent actors.[762] In order to

achieve the desired operational and strategic effects, the use of SOF should be seen from a highly collaborative perspective, including cooperation with both domestic interagencies and partner nations.

Domestic Security

Due to the changing and evolving nature of threats in contemporary conflict, including the use of multiple methods and actors, the traditional division between war and peace has become blurred. Nothing indicates that such developments will decrease in the future. Traditionally, there has been a tendency to illustrate a conflict in a linear way (i.e., peace followed by crisis leading to combat). However, an increasing understanding of the non-linearity between these phases is growing. The traditional and sharp division, in most states, between the roles of different government agencies in war, and during times short of war, constitutes a challenge as the nature of conflict itself changes. Domestic security is, in times short of war, normally mandated by law through government agencies other than the armed forces. The police and security services are those mainly responsible for dealing with the majority of domestic threats.

However, with an understanding NGW, it is apparent that several other agencies within sectors such as finance, infrastructure, energy, and information, also will play important roles in countering an adversary´s IW activities.[763] The domestic use of the armed forces pre-war, however, is quite constrained by legislation. Several small states in Europe have, as a result of several decades largely defined by counter-terrorism, developed new legislation increasing the ability for military support to civilian agencies. For example, Sweden passed a new law in 2006, allowing the police authorities to request support from the armed forces when needed. This law aims at dealing with terrorism, and it is primarily resources Swedish Special Operations Forces (SWESOF).[764]

Legislation differs between countries. The Netherlands, for example, has a Special Interventions Service (DSI) where police and military units are integrated and tasked with domestic counter-terrorism and hostage rescue operations.[765] New insights into the nature of future war will most likely influence developments towards extended possibilities for the military to support civilian society as the line between what is terrorism, crime, subversion, and sabotage is increasingly blurred. In a 2012 speech, President Putin described *controlled chaos* as the nature of coercion aiming at destabilizing an opponent.[766]

So, within a Total Defense concept, how could the armed forces generally and SOF in particular play a domestic role in phases short of war? Countering IW threats against, for example, energy infrastructure is one important task in order to maintain societal resilience. A small and highly qualified resource, such as SOF should, however, not be spent on static tasks such as guarding critical structures. SOF could support civilian agencies and organizations in developing their own capabilities, as well as being a resource on high readiness alert in cases of emergency such as violent attacks on infrastructure and hostage situations.[767] With reference to an adversary's strategy to use a wide spectrum of actors to conduct IW activities—such as reconnaissance, sabotage, and to create civil unrest through separatist movements —SOF would be an instrument that could add much value to a whole-of-society effort. Tasks could be to support other agencies in shaping and understanding the environment. Furthermore, they could conduct joint operations with civilian agencies or partners to neutralize specific threats.[768] Acting in a domestic role is mainly defined by reacting to, rather than anticipating, the actions of an adversary. However, countering an adversary in a peer-on-peer environment is of the utmost importance, in terms of the ability to understand and anticipate the adversary's actions.[769]

Resilience and Resistance

Modern war in the twenty-first century appears to be in line with the Gerasimov doctrine. In Ukraine, Russia has demonstrated how brutal kinetic attacks, alongside non-kinetic tactics, can be interwoven.[770] Russia has embraced a much wider array of attack methods than before, including the targeting of civilians.[771] New technology, which is remote from conventional armed forces expertise, is utilized over the entire conflict scale. To counter and resist such attacks, a nation needs a modernized Total Defense, as defined in the introduction. The willingness to defend among the population is central, and fostering that is a long process, built on societal cohesion and a strong trust in the capabilities of the state. People also need to be educated, and prepared for a possible crisis or a war situation. In Sweden, the government has published videos through a range of channels, including YouTube, explaining how the population can prepare for various dangerous situations. They have also sent brochures to all the households with the very same message. To further improve this concept, additional measures need to be implemented.

One important aspect for small states in a deteriorating security environment is to partner with other states where shared interests exist. One example of such a common

effort between nations in the BSR and U.S. Special Operations Command Europe (SOCEUR) resulted in the production of the *Resistance Operating Concept* (ROC).[772] The ROC aims at facilitating interoperability between nations if they were to become occupied. The ROC defense concept effectively aligns with Total Defense and encompasses digital technologies, as it highlights the necessity of converging military power with civilian counterparts.[773]

In Total Defense, IW concepts need to be developed top-down as well as bottom-up. Companies in the private sector are often less hierarchical than governmental organizations. They are also profit driven, and consequently, constantly forced to adapt and be innovative. Several private companies have the ability to develop and sustain resources that could be of dual use, that is commercially viable in peacetime with the ability to deliver capabilities to the government and the military when necessary. For example, there a Swedish company that sells services to the forestry industry, such as flying drones with cameras to aid in forest inventory. That branch of the company is also tailored to be a part of the military reserve and hence able to deliver the surveillance services in times of crisis, but with other useful commercial purposes in peacetime. The same company has also developed other dual-use capabilities, and serves as a great example of cooperation between the armed forces and the private sector.[774]

Considering the context of great and emerging power competition short of war, the threshold effect as used in the doctrinal context needs to be adjusted or developed to also include the entirety of today's Multi-Domain Battle (MDB). Resilience also includes a significant psychological component as, "resilience often describes military personnel's mental preparedness for warfare operations or other engagements in contexts shaped by uncertainty, complexity, and physically as well as mentally demanding tasks."[775] Small states need to acknowledge the importance of fostering digital, cyber, and informational resilience and resistance. Both to reject propaganda and lies, but also to be proactive in strategic communication.

A small state attacked by a superior aggressor will probably be forced into conducting defense and resistance operations in parallel, depending on the aggressor's territorial gains in different regions of its territory.[776] This complex environment demands flexible leadership, along with agile command and control (C2) systems. Due to threat levels on the battlefield, seamless transition between well-coordinated joint defense operations with centralized command, and more self-synchronized resistance operations led by mission command is required. Dr. Sandor Fabian stresses the necessity of pre-conflict preparation in almost all sectors of society ranging from urban development, all the

way to purpose-built resistance forces, which are quite different from the traditional role models.[777]

In resistance operations, local defense units, such as the Home Guard and Territorial Defense, would naturally be key elements. SOF would most likely primarily be involved in other strategic operations in the early phases of a war, and might be a quite scarce resource at this stage. However, SOF could still play an important role by using their human capital in new ways, for instance, by utilizing former operators, retired from active duty, to form the backbone of a reserve organization. The mission would be to work with the local Home Guard and Territorial Defense units in the area in which they live, building local resistance networks and providing their professional expertise in a wide range of fields. As new technology has developed, the digital footprint of almost everyone in society creates risks that previously did not exist. The awareness within the SOF community regarding threats from digital footprints, would in that sense contribute to risk mitigation related to the individual histories of citizens, and their exposure on social media. The war in Ukraine has shown several examples of new types of capabilities that have developed during the conflict from rather unexpected sources.[778] SOF are recognized for their innovative mindset, and could be a dynamic multiplier constituting the glue between some important resources across society.

Preparations for War

Past wars have taught us that pre-conflict preparations optimize the conditions for achieving the desired effects with minimized risks. When an armed conflict begins, the risks and complexities increase exponentially. Pre-conflict activities must truly be a part of a comprehensive effort, including preparations for deep operations and resistance operations. This implies the necessity for close cooperation with other agencies, such as the intelligence services. It would also imply cooperation and collaboration with neighboring countries where shared interests exist. The sensitive nature of such operations, and the levels of risk connected to them, apply throughout the preparations and conduct of them. A high level of secrecy is therefore critical. As we have seen in Ukraine, during the early phases of a war, SOF are an ideal instrument in supporting and facilitating the effects of conventional forces. Striking enemy high-value targets throughout the operational depth, including deep in enemy territory, creates opportunities for conventional kinetic and non-kinetic measures and also creates psychological impacts on the adversary.[779] Professor Gray claims that *humiliation of the enemy* is one of the strategic utilities of SOF.[780] Enhanced by information warfare, measures embarrassing the enemy can be a powerful weapon.

In times short of war, SOF could, through special reconnaissance and in collaboration with the intelligence services and partners, prepare the future battlefield. If one compares phases short of war with what U.S. doctrine labels *competition,* SOF are one of the crucial instruments for understanding the adversary, anticipating its actions, and shaping the environment.[781]

Preparations in times short of war, should also include facilitating physical as well as cognitive and moral access to future areas of operation.[782] In the later stages of a conflict, when an aggressor has turned to overt action, SOF are suitable for guerrilla warfare and ultimately, in occupied territory, for the support of resistance movements.[783] The war in Ukraine has proven that traditional small unit tactics, such as ambushes and guerrilla-type operations against enemy forces in canalizing terrain, still generate operational effects.[784] The ancient ways of defensive guerrilla warfare, Byzantine-style, are still applicable when adapted to the new challenges and opportunities of the modern battlefield.[785]

Discussion

Most small states have limited redundancy, in terms of resources, to deal with high-impact, long-term contingencies. The risk is, therefore, apparent that limited resources could be misused and, as a result, not deliver the desired effects. SOF has roles to play within this concept. In an anticipatory role, SOF can work in concert with other agencies and partners, to contribute to shaping and understanding the environment domestically and abroad. In a reactive role, SOF can deal with contingencies that demand capabilities outside of what other Total Defense instruments can deliver.

In crisis, whether caused by natural disasters or armed conflict, contemporary history has shown that only a few states, if any, have the resources to deal with the challenges alone. Domestic and multinational interoperability are crucial factors to create the necessary synergies between the instruments at hand. When creating a holistic Total Defense, this philosophy is essential. For a small state, which almost by default would be the weaker side in an asymmetric conflict, it is an existential question to use its scarce resources in ways that are optimizing the desired effects. Such an approach to resource allocation is not to be taken for granted, or perceived as being something that will happen by default. On the contrary, it takes prudence in times of low tension to make sure that interoperability and trust are built between Total Defense actors, as well as with international partners. Domestically, this process would necessitate

the development of new attitudes and holistic approaches in order to facilitate such a transition.

The competition for resources and power between different agencies has always been a major disruptive factor in both the interagency and intra-agency relations. A clear and deep understanding of what Total Defense is aiming at, by all actors involved, is one way of reducing traditional interagency competition. During the decades of COIN and CT, SOF has been an instrument proven to be successful, but at the same time has been rather spoiled in terms of getting most of the resources on their wish list. There is an apparent risk that this has created an attitude, formed by tactical success and the perception of always being the supported effort rather than the supporting one, which could be an obstacle to overcome. Adapting to a new reality in a Total Defense context includes, among many things, that SOF adapt to a new normal characterized by the demand of seamless transition between serving in supported and supporting roles.

The Total Defense understanding of the contemporary world includes the insight that it is hard, bordering on impossible, to distinguish what constitutes a clear act of aggression, or an act of war. The traditional notion of conflict as categorical, and acts of war marking a transition from war to peace being clearly discernable, is no longer valid. Consequently, legislation in many countries is written for a reality that no longer exists, if it ever truly did. A review of the legal dimension, facilitated by legislative institutions, is therefore fundamental in creating a balanced and well-functioning Total Defense concept. This is particularly true concerning the use of SOF during times short of war, which would require a reevaluation of existing legislation, as well as policy. This is particularly relevant internally in countering an aggressor's initial IW actions, as well as when conducting external shaping activities in the same domain. Two decades of expeditionary warfare have formed perceptions and habits that need to be adjusted and adapted to a new environment, and to face new challenges. If this is not done effectively, SOF cannot be utilized to its maximum capacity. It is important to have a tool such as SOF in the toolbox, but not being able to use it properly is something small states cannot afford.

The importance of anticipation, and preparations for potential future developments and security challenges, cannot be stressed enough. If deterrence and defense eventually fail, and an aggressor is controlling parts or the entirety of a country´s territory, the whole of society will need to engage in resistance operations. SOF, in this context, are one of several instruments that, if properly utilized, could have a disproportional impact on the occupying force. This is, as earlier stated, an instrument that is quite limited

in numbers, and most probably quite operationally stretched in the later stages of a conflict. One way of circumventing this particular resource conflict, is to utilize former (non-active) special operators to build the backbone of local resistance networks. With such an initiative, the connections to active SOF are already established, and could also facilitate a transition of latent resources into resistance operations. Furthermore, proper preparations will have created the necessary networks in local civil society, on which any resistance movement will be heavily reliant.

In terms of offensive operations, SOF can enable the delivery of effects by conventional means that otherwise would not be able to affect the desired targets. SOF can, of course, deliver effects on their own, preferably with strategic implications for an enemy state. However, these actions also demand preparations, and shaping efforts, in times short of war. Ideally, such efforts should be undertaken in close collaboration with other agencies and international partners.

Conclusion

Much has changed in the contemporary and future conflict environment, and this demands adaptation to new realities. States must accept that the forms of IW have moved beyond existing doctrines and paradigms of power. Current threats are exceptionally non-linear, and the distinctions between criminality, terrorism, and acts of war have become blurred. Consequently, defense resources, as well as attitudes and perceptions, need to adjust in order to match these challenges. Due to decades of dismantling military and civilian defense resources, all states, especially small states, need to choose wisely in order to make the most of their limited defense resources. In Total Defense, an extensive toolbox is needed and all sectors of society must be involved, from the individual to the government. The interconnectivity between all these actors, and a deep understanding of overarching national aims, are vital components in this concept.

Total Defense should, therefore, be perceived as an ecosystem consisting of several different sub-systems and communities that are all important and interdependent. SOF constitutes just one of these communities, and is heavily reliant on the other parts of the system. The last two decades have illustrated the fact that no matter how tactically-successful SOF has been, the strategic objectives of the campaigns in question have not been achieved. Without being integrated into a strategic context where all instruments are supporting the overarching objectives in concert, defeat will likely be the eventual result.

However, if utilized properly, within a strategic concept, one should not disregard the additional value of what ultimately is an exclusive resource. In line with Professor Kiras, we stress that special operations can affect both the enemy's physical and moral vulnerabilities. Operations at the tactical level, therefore, should not be seen as independent acts of war, or purely regarded in terms of enabling conventional forces or other agencies. On the contrary, since SOF are effectively linked to the strategic level, they also have a unique potential to empower a small state´s Total Defense strategic efforts in phases short of war.

Realizing this, and accepting the need to find new and better ways of interacting, SOF could, if properly utilized, be an instrument that can punch above its weight and truly make a difference of strategic significance. Characterized by their extraordinary human capital, and having capabilities outside those of most other resources, they can, in conjunction with the other elements of Total Defense, be a decisive factor in many situations. To manage that, prudence and preparation in times of peace are important factors. However, prudence and preparation only by the performers is not enough. To facilitate maximum effect of the resources at hand, legislation needs to be adapted to this new reality. Changed policies, and new ways of employing SOF as a vital instrument at home and abroad, and in times short of war, are essential factors in shaping the environment. This would also enable the transfer from an almost purely reactive stance, to a posture that includes proactiveness. To make this happen in time, a sense of urgency as well as courage from political leadership is required.

About the Authors

Dr. Ulrica Pettersson is Director for Centre of Special Operations Research at the Swedish Defence University. She holds a PhD in Risk Management and Safety Engineering from Lund University. She worked in the Swedish Armed Forces for 20 years, and has been a faculty member at Joint Special Operations University. Her publications include *Special Operations from a Small State Perspective: Future Security Challenges* (Palgrave), "Resilience and Resistance in the Digital Age: Revisiting the Threshold Effect in Total Defence" (*Journal of Baltic Security*), and "ROC (K) Solid Preparedness Resistance Operations Concept in the Shadow of Russia" (*Prism*).

Colonel (R) Hans Ilis-Alm is serving as a Lecturer at the Swedish Defence University. He served in the Swedish Special Forces during the majority of his career. Col Ilis-Alm has operational experience from several continents, and has also served in the EU Military staff as well as in U.S. CENTCOM and U.S. EUCOM/AFRICOM. His publications include "Resistance Operations: Challenges and Opportunities for Special Operations Forces" (*Journal of Baltic Security*), *Special Operations from a Small State Perspective: Future Security Challenges* (Palgrave), and "Coalition Warfare: Going into Battle Together is the Rule Rather than the Exception" (*Handlingar och tidskrift: The Royal Academy of War Sciences*). Col Ilis-Alm holds an MSc from the National War College in Washington, D.C..

Discussion Questions

1. What is New Generation Warfare, and how well-understood is this concept by Western political and military leaders? How much do they realize, and accept, the cognitive challenges of modern irregular warfare?
2. Given the realities of New Generation Warfare and Total Defense, what measures are necessary to implement to address the challenges inherent in both?
3. How should the limited resources inherent in SOF be used most effectively and efficiently in Total Defence?
4. What opportunities and challenges exist for conducting and countering irregular warfare challenges in the Baltic and Nordic regions? How similar or distinct are they, and why?

Recommended Readings

- Otto C. Fiala, *Resistance Operating Concept* (Stockholm: Swedish Defence University, 2019 & MacDill AFB, FL: JSOU, 2021).
- Gunilla Eriksson & Ulrica Petterson, *Special Operations from a Small State Perspective: Future Security Challenge*s (New York, NY: Palgrave Macmillan, 2017).

- Andrew Molnar et al., *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare,* (Washington DC: Special Operations Research Office, American University, November 1963). (n.b., a revised, updated second edition is available online from the US Army Special Operations Command in audiobook, eBook or PDF form from https://www.soc.mil/ARIS/books/arisbooks.html)
- Hans von Dach, *Total Resistance: Swiss Army Guide to Guerilla Warfare and Underground Operations* (Boulder, CO: Paladin Press, 1965).

The views expressed are those of the authors and do not necessarily reflect the official position of the Swedish Ministry of Defence, Swedish Defence University, the U.S. Department of Defense, Defense Security Cooperation Agency, or the Irregular Warfare Center.

The United States' Maginot Mentality

Sean McFate

ABSTRACT

The United States is preparing for the only kind of war it will most likely never face: a conventional one. Nothing is more unconventional today than a "conventional war," and only 6% of armed conflicts since 1945 were fought using this kind of warfare. Also, the Cold War teaches us conventional wars between nuclear powers are either very short or non-existent because it can escalate to a strategic nuclear exchange in minutes. Consequently, the Cold War was fought covertly with unconventional warfare: political warfare, covert operations, and proxy wars. The United States frequently won, yet avoided conventional battle, and China can do the same. Incredibly, the U.S. national security establishment has forgotten Cold War lessons—an extremely dangerous situation—because it suffers from the "Maginot Mentality:" expecting future wars to look like past victorious ones, but with better technology. It is investing heavily in conventional warfare capabilities, while ignoring how the character of warfare has changed, leaving itself vulnerable to modern warfare. The French got *"blitzkrieged"* while sitting behind the false security of their Maginot Line, and something similar could happen to the United States. Concepts matter more than weapons systems, as the Maginot Line evidences.

Currently, Washington's strategic concepts are stuck in the early 20th century, as it prepares to fight China using an outmoded form of armed conflict. This chapter will explain the source of this dangerous ignorance, what modern warfare looks like, and briefly how it could be won.

Introduction

Imagine a group of former Pentagon officials, retired senior military officers, and think tank experts gathered around a table and staring at a hexagonal map of Taiwan. Quietly they move pieces around the board—F-35 fighter jets, aircraft carriers, Marine Corps units—followed by sagacious nodding. Then, shock, as two carriers get blown out of the water by a swarm of Chinese hypersonic missiles. After several iterations, they lose more than they win. Often the simulation ends in nuclear war. War gaming has become a cottage industry inside the Beltway, led by the Pentagon and think tanks, to develop "evidence-based" strategies. Rightly, the Defense Department must study how to win against China and/or Russia in "strategic competition," should it become a shooting war.

But here's the key problem: it will not happen, at least not like it is usually simulated, and thus we are learning the wrong lessons. The wargamers view ultimate "competition" settled in a conventional battle, and tend to recreate the Battle of Midway with Ford-class carriers and F-35s. Such a conflict probably would go nuclear in hours or days, and the gamers' artificially-prolonged conventional war phase is fantasy. Worse, it reinforces the wrong lessons. Strategic leaders have a moral obligation to be competent, because mistakes are paid for in American blood and treasure.

As the Cold War teaches, conventional wars between nuclear powers are very short or non-existent because they can go nuclear in minutes. It's why the United States and Soviet Union (USSR) avoided putting their troops into direct conflict, and what made the Cuban Missile Crisis a "crisis." Instead, the Cold War was won unconventionally through nuclear deterrence, unconventional war, covert operations, coercive diplomacy, economic superiority, and offering a better way of life. The most important lesson: the United States won, avoided conventional battle, and adversaries like China can learn to do the same by 1 October 2049, their self-imposed deadline. However, today's defense community remains recklessly ignorant of these clear lessons.

In terms of the military, nuclear strategic competition is an unconventional fight, not a conventional one. The imperative to avoid a mushroom-cloud apocalypse drives

armed conflict into the shadows of plausible deniability, using stratagems such as political warfare, covert operations, and proxy wars. It's why Army Special Forces, or "Green Berets," were founded, how Stinger missiles broke the USSR's back in Afghanistan, and how Javelin anti-tank missiles blunted Russia's invasion of Ukraine.

Meanwhile, the U.S. national security establishment is planning for a conventional war against China. The dangerous truth is: the United States has forgotten how to win wars. Like the French and their Maginot Line, the United States assumes the next war will look like the last one we won but with better technology. The last big war America won was World War II (WWII), the archetypical conventional war (albeit one that ended with the first use of nuclear weapons), and Washington's fixation on this style of combat proves the adage "generals always fight the last war they won." This kind of strategic thinking will likely kill us. When it comes to war, concepts matter more than weapons systems, and we urgently need to improve our strategic intelligence quotient (IQ).

Victor's Curse

The United States has stopped winning wars because it has a bad case of the "Victor's Curse." In some ways, the nation is a victim of its own success. The Victor's Curse occurs when the strong get complacent and dangerously view warfare as static, while the weak innovate past the strong and succeed. It does not matter who has superior technology, or more firepower. If your concept of war is outdated, and you don't know how to deploy your military for victory, you are lost. This is how David beats Goliath, not with firepower but with smarts.

There is a difference between war and warfare. War's essential nature never changes, whether it's 1000 BC or now; war is armed politics. However, warfare is always changing. Warfare refers to how wars are fought, and its tactics, technologies, leadership, geopolitics and so forth are forever metamorphosing. The Victor's Curse erroneously assumes warfare is static. More precisely, it presupposes future wars will look like the last successful one, but with better technology, given its march of progress seems never denied. The Victor's Curse is how superpowers can get blindsided by the future, and why high-tech militaries can still lose to "weaker" foes. The weak transform their warfare, while the strong remain in their cocoon.

World War I provides a stunning example of the Victor's Curse. After it ended, victorious France assumed the next war would look like the last one, namely defense-

dominant trench warfare. Accordingly, they built the Maginot Line, the most sophisticated fixed fortification system in history. Named for André Maginot, the French war minister who pressed the government to spend vast sums on defense, this 280-mile-long network of concrete bunkers, retractable turrets, and underground casemates was designed to repel any direct German invasion.

The Maginot Line, however, failed. Warfare had moved on, while France did not. As the French slept soundly in the false security of the Maginot Line, defeated Germany innovated. German strategists devised a new strategy called the blitzkrieg that easily bypassed the fortification system, albeit using the same pathway through neutral Belgium they had less than 30 years before, essentially bypassing the Maginot defenses which mostly held until the French surrender. What the Germans could not achieve in four bloody years of World War I, they accomplished in only 46 days, driving panzers around the *Arc de Triomphe* in 1940. The French high command was flummoxed and swirling in cognitive dissonance, as German tanks went through the "impassible" Ardennes Forest, around the Maginot Line, and advanced on Paris. One eyewitness lamented how, "our leaders...were incapable of thinking in terms of new war...[Their] minds were too inelastic."[786]

The Maginot Line example teaches us that warfare changes before warriors do, and this is a major cause of defeat regardless of military strength and technology. The French possessed an impressive army, and state of the art equipment, but they lacked the strategic IQ to wield it. They were undone by their success, and leaders like Maginot suffered from the Victor's Curse. Blinded by past victory, they were too busy refighting the last successful war rather than preparing for the next one, leading to their easy defeat.

Cassandra's Curse

Unlike Maginot, true war prophets exist but are seldom believed. This is the "Cassandra's Curse." In Greek mythology, Cassandra was given the power of prophecy but cursed that no one believed her. Cassandras can be found in every profession and personal life, but when it comes to war, their unheeded warnings are often paid for in needless blood and squandered treasure.

General William "Billy" Mitchell was an American aviator during World War I, and suffered from the Cassandra's Curse. He saw the future of war, and it was air power. When he returned to Washington, he proselytized his message, "[i]f a nation ambitious

for universal conquest gets off to a 'flying start' in a war of the future," he said, "it may be able to control the whole world more easily than a nation has controlled a continent in the past."[787] Mitchell was derided. The defense establishment of his day believed the dominant arena of the next war would look like the past one: trenches.

Dauntless, Mitchell raised the volume. In the future, he claimed, aircraft carriers would replace battleships, the long-reigning king of the sea. Everyone laughed, especially those in the Navy. Then he spoke heresy; airplanes could *sink* battleships. Back then, planes were little more than motorized kites in the era of the superdreadnought. People howled. Yet, Mitchell had grit and convinced the Navy to haul out a captured German battleship into the Chesapeake Bay, where he sank it using airplanes. Rather than spark a strategic conversation about the potential of airpower, his demonstration did the opposite. The Navy dismissed the experiment as a sham, because it did not simulate war time conditions, while Mitchell literally stuck to his guns. The row escalated, erupting into national newspapers and Congressional politics.

Perhaps to keep Mitchell out of further trouble, General John J. Pershing, Chief of Staff of the Army, sent him on an inspection tour of the Pacific. The furor died down. Months later, Mitchell returned with a 525-page report that predicted Pearl Harbor, in 1924. He warned that Japan would launch a sneak attack against the American Navy base in Hawaii using airplanes, and this would start a war between the two nations. The, "attack will be launched as follows: Bombardment, attack to be made on Ford Island (in Pearl Harbor) at 7:30 a.m. ... Attack to be made on Clark Field (Philippines) at 10:40 a.m."

The top brass already thought Mitchell was crazy, but this new assertion went too far. For this and other sins, Mitchell was deemed insubordinate and court martialed. But it was not just any trial; it was a Kim Kardashian-style spectacle, replete with paparazzi, corrupt judges, and unconventionalities. After thirty minutes of deliberation, the jury found Mitchell guilty, and he was suspended from the Army without pay for five years. In disgust, he resigned.

For the next decade, Mitchell preached tirelessly about the coming age of air war, when battles would be fought in the sky, over who would rule continents. Many thought him an entertaining fruitcake. He died a bitter man in 1936, declining to be buried at Arlington National Cemetery.

Five years later, the Japanese attacked Pearl Harbor as Mitchell had prophesied. Within two hours, they sunk or damaged eight American warships, including the famed USS *Arizona*, destroyed 188 aircraft, and killed 2,403 people. Washington claimed it

had been caught "completely by surprise," even though one of its own generals foretold the attack seventeen years earlier. Instead, the War Department blamed an unscrupulous enemy for its failure. In reality, the 2,403 casualties were killed as much by the Victor's and Cassandra's Curses as Japanese bombs, because Pearl Harbor was avoidable.

The United States and Japan went on to fight one of the largest naval engagements in history, the Battle of Midway. Never did the two fleets directly see each other, because it was fought entirely with aviation. The battleship was already obsolete in 1940, but it took until Midway to prove it to those with the Victor's Curse. When the war was over, aircraft carriers replaced battleships as king of the ocean, just as Mitchell had predicted twenty years earlier. This legacy endures today.

Mitchell had the Cassandra's Curse; he saw the future, but no one believed him. Sometimes it is easier to court martial the truth than listen to it. Years after he died, the military did apologize, in its own way, and named a bomber (a supporting, or "medium" B-25, vice main "heavy" one) after him, which he surely appreciated.

Today's Mitchell Moment

We are facing a Billy Mitchell moment today. Like the French between the World Wars, warfare has moved on while the United States has stood still, and it's why it no longer wins, even against weaker adversaries. Having the best military and most advanced technology is not enough if you are stuck in the past, as the Maginot Line evidences. Concepts matter most.

The American Victor's Curse looks back to the glory days of WWII, the last time the United States won decisively. The frustrations that followed 1945, from Korea to Afghanistan, are either forgotten or dismissed as quagmires. Rather than face reality, America remains spellbound by WWII. The U.S. Army recently adopted "new" dress uniforms that are WWII cosplay. Military education remains conventional war at its core, from basic training to war college. Experts strangely describe this style of combat using normative language such as "conventional war," "regular war," and "symmetrical war" (I use the term "conventional war," but they all mean the same thing).

Conventional war coincides with a military-centric view of international relations, and is why militaries remain smitten with its call. Nation-states battle for destiny using big militaries as gladiators. Victory is determined by whoever seizes more territory, kills more of the enemy, and flies their flag over the opponent's capital. It is Carl von Clausewitz's way of war, and why the 19th century Prussian is beatified in war colleges,

and his tome *On War* quoted like scripture. Honor matters, as do the laws of war, and citizens are expected to serve their country in uniform with patriotic zeal and self-sacrifice. It is why Americans say "thank you for your service" to veterans in the airport.

Civilians are also prisoners of the WWII paradigm. Many call it the "good war" fought by the "greatest generation." Nearly seventy years on, the demand for WWII movies appears unstoppable, and the supply inexhaustible. Like a handsome man in uniform, these films never really go out of style. There are over six hundred unique WWII movies, and more are released each year.[788] That's more than films about the Korean, Vietnam, Iraq and Afghanistan wars combined. The *American Heroes Channel* is a television (TV) network that carries programs on the military, warfare, and military history. Tellingly, it showcases WWII. Novelists such as Tom Clancy, and his successors, often depict armed conflict as conventional war, as do movies. It is what people have come to expect and want.

To show how deep-rooted the conventional war bias goes, take the Russian War in Ukraine. Most Americans, from military experts to Joe the Plumber, believe it's conventional simply because they see tanks and artillery and associate them with the Battle of the Bulge. Astonishingly, they overlook the conflict's larger unconventional features: Ukraine's guerilla warfare campaign, the Wagner Group mercenary army, Russia's deliberate bombing of civilians to inflict terror, and the wily disinformation campaigns waged by both sides. Other than a traditional state-on-state conflict, little about the war is "conventional."

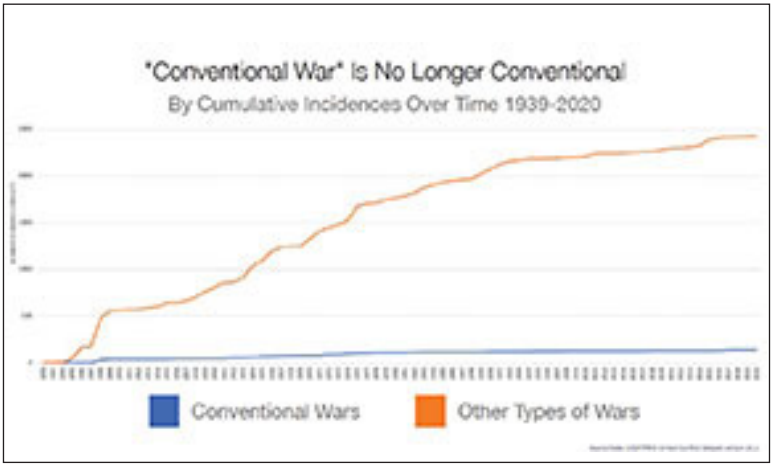

Figure 1. Instances of Conventional vs. Other Types of War (Source: UCDP/PRIO Armed Conflict Database)

There is just one problem with conventional war: no one fights this way anymore, if they ever did. Nothing is more unconventional today than a "conventional war." Only 6 percent of armed conflicts since WWII were conventional, which has nearly flatlined since 1945 (see Figure 1).[789]

However, organized violence has not waned. The International Institute for Strategic Studies, a British think tank, releases an annual report detailing the deadliest conflicts in the world, and they are always topped by unconventional conflicts like Syria, Mexico, Iraq, Afghanistan, and Yemen. There are no more conventional wars, yet astonishingly many still believe this style of warfare is predominate, timeless, and universal. It is not. "Conventional war" reigned from Napoleon to Hiroshima, according to the bounds imposed by this data, a mere 150 years. What came after, was the nuclear age and civil conflict quagmires.

Warfare has moved beyond conventional war, which is as obsolete today as trench warfare was during the blitzkrieg. Yet despite the bitter lessons of Vietnam, Somalia, Balkans, Iraq, Afghanistan, and Syria, Washington still spends billions on a military predominantly designed to thwart enemies who fight conventionally, even though no one predominantly battles this way anymore. The United States fights in the past, while its enemies wage war in the present. No wonder Afghanistan was the longest war in American history.

The American Maginot Line

The United States has struggled against low level foes like terrorists and insurgents for nearly twenty years. What will happen if it confronts weightier threats posed by great powers like Russia or China? Nothing good. With an eye towards this risk, the United States' 2018 National Defense Strategy reorients the military away from counterterrorism and counterinsurgency, and towards "great power competition" (read: Russia and China). This is smart, but what kind of war is the Pentagon expecting? Its shopping list reveals all. Budgets are moral documents because they do not lie. Weapon systems built for conventional wars are both obsolete and heinously expensive, yet the United States is investing heavily in them. Dear Taxpayer, welcome to America's Maginot Line.

The F-35 fighter jet program costs taxpayers $1.7 trillion. That's more than Russia's GDP, spent on a single seat airplane. If the F-35 were a country, it would rank 11th in the world in terms of GDP. Buying one costs around $100 million, almost double the price of a Boeing 737-600. They are also expensive to fly. Each flight hour costs $42,000,

more than twice that of the F-16 fighter jet and nearly the salary of the mechanic fixing it.[790] For the past 20 years, the United States has been at war somewhere, yet the F-35 has zero combat missions. As we say in the airborne infantry "that dog don't hunt." The F-35 was designed to win last century's wars, not this one's. Nevertheless, we're buying hundreds more, and pressing allies like Germany, the United Kingdom, and Finland to do the same.

A Ford-class aircraft carrier costs $13.3 billion per ship, and that's before you add sailors and aircraft. Imagine it as Spain's defense budget, wrapped up in a hunk of steel. Carriers are worthless today. They did not help win the War on Terror, and are not deterring China or Russia. If a shooting war starts in the Straits of Taiwan, sailors—5000 per carrier—know they will be on the bottom in 20 minutes. And they are correct, according to multiple Pentagon wargame simulations. The United States has nevertheless bought five of them.

The defense budget for 2023 is a whopping $868 billion, exceeding Saudi Arabia's GDP. It's more than the next fourteen biggest militaries in the world combined, and greater than all other federal departments combined. If you want to know what kind of war Washington thinks we will face, looks at what we're buying. The top weapon systems acquisitions are all conventional war weapons: fighter jets, submarines, aircraft carriers, armored battle vehicles, and so forth. Washington's military-industrial complex retorts that these weapons can also contribute to victory in unconventional wars, and hence, not a total waste of money. However, they did not win in Iraq or Afghanistan, which turned out to be unconventional fights much like Vietnam.

Triumphant nations get lazy and want the latest technology to fight the last war, rather than weapons that work for the next one. Experts turn to the past, and imagine conventional wars fought by robots commanded by artificial intelligence. Washington invests heavily in "combat overmatch" and "battlefield lethality" to shorten the "kill chain" at the tactical level, even though the nation already possesses superior capabilities on this score compared to potential enemies. Why are more needed? Even America's enemies know a military-on-military confrontation would be suicidal, and that's why they avoid it. Chinese strategic ideas like "Unrestricted Warfare" and "The Three Warfares" are designed to win against the United States while avoiding conventional war, as is Russia's Primakov doctrine and concept of "active measures."[791] Additionally, America's tactical and operational prowess does not deter China from expanding in the South China Sea and Russia from invading Ukraine, Georgia, or Syria. Conventional deterrence fails because with live in a post-conventional war era.

Like André Maginot, American strategic leadership has the Victor's Curse. They assert a big conventional force is needed to deter Chinese and Russian aggression, but avert their eyes from the obvious, namely that China and Russia continue to expand, undeterred. The Pentagon spends trillions on weapons designed to win conventional fights at the tactical level, like F-35s, while ignoring how warfare has changed at the strategic level. The defense establishment prioritizes technology-centric solutions, like the Revolution in Military Affairs and the Third Offset Strategy, but ignores history. Since 1945, Luddites have routinely bested high-tech militaries, from Indochina to Afghanistan. If there is a single lesson of modern war, it is this: frontline technology is not decisive. Nor is battlefield victory (who remembers "Mission Accomplished"?). You can win every battle, yet lose the war, something Washington should have learned decades ago but has not. Instead, it suffers the Victor's Curse and spends astronomical sums to fight conventional wars, then struggles in the more frequent unconventional ones. Rather than learn, it buys F-35s and Ford-class carriers: the definition of insanity, just like the Maginot Line.

Conventional warfare is obsolete, and has been for a long time, as Putin learned in 2022. At first, Russia tried a conventional war *blitzkrieg* and failed. A 40-mile-long armor column was stuck on the road to Kyiv, the perfect symbol for conventional warfare in modernity. After a month of humiliation, Putin went unconventional. In April, he replaced the failed general with General Aleksandr Dvornikov, by all accounts a uniformed sociopath. Known as the "Butcher of Syria," he is infamous for bombing civilians wholesale in Syria and Chechnya. Russia nevertheless won those fights. They used "conventional" weapons and units for unconventional, not conventional, war. In more recent examples, Russia carpet-bombed civilian centers, like Mariupol and Bakmut, with conventional artillery shells and rockets. Regular military units massacred civilians in Bucha, some with their hands tied behind their backs. Civilian mass graves were found outside Izium, some with signs of torture. For the United States, unconventional warfare implies winning hearts and minds. But for Russia, it means massacring civilians, and flattening cities. Wanton destruction is a feature—not a bug—of Russian unconventional warfare. Americans cannot comprehend it.

Future War

Forget what you know, wars of the future will look nothing like those of the past, just as the French learned during the blitzkrieg. If there will be a major conflict between great powers, why does Washington assume it will be fought conventionally? Those

afflicted with the Victor's Curse will probably not recognize future conflicts as wars at all, until it is too late, just like the French. The United States may already be at war with Russia or China and not know it, which is part of their strategy. Warfare has changed, but America remains mired in the past, dangerously unprepared for the future. Below are a few ways the character of war has transformed. More exist, but here are four significant ones.

First, war is getting sneakier. Armed conflict is going underground, into the shadows. Occasionally, it will bubble up into mainstream media and may look "conventional" for a brief time, before returning to the shadows. Russia has mastered this new way if war. During the Cold War, when the Kremlin wanted to put its boot on someone's neck, it rolled in the tanks. Brute force squashed uprisings in Hungary in 1956, and Czechoslovakia in 1968.

That was the twentieth century, when raw military might represented power. Now it is a liability. Moscow blew it in 2022, using conventional war *blitzkrieg* tactics to storm Ukraine, and got beaten back by guerilla fighters firing handheld anti-tank weapons. Russia enjoyed more success when fighting in the shadows, just as they did in 2014. They flooded the countryside with a ghost occupation force comprised of Spetsnaz special forces, mercenaries like the Wagner Group, "little green men," and astroturf proxies like the Donbass People's Militia. Dense propaganda, along with "active measures," further distorted the world's perception of reality, making the conflict disappear from the global stage. Many outside the region did not know it was a shooting war, and still don't. By the time the international community figured things out, Moscow's conquest of Crimea was a *fait accompli*. Only then did the tanks, destroyers, and other conventional war weapons arrive. Strategic deception rather than brute force won.

In the information age, weapons that bestow plausible deniability are more effective than firepower, and this is driving war underground. Russia waged a shadow war in Ukraine, manufacturing the fog of war and exploiting it for victory. If the basic facts of the conflict are in question, how can the United States or the United Nations rally the world to fight a war that may not exist? They can't. It's an effective strategic offense by Russia, and it's an example of what's to come.

Second, war or peace no longer exists; now, it is war *and* peace. However, this is not how the West thinks about warfare. War versus peace is enshrined in the Laws of Armed Conflict, the writings of Clausewitz, and conventional war theory. Each views conflict in black and white terms: war occurs when peace fails. In WWII, Japan broke the peace when it attacked Pearl Harbor. Then, war was declared and battle was the great decider.

In war, ethical standards lapse and atrocities are committed. Conventional warriors justify these things as "collateral damage" and "military necessity." War ended when the defeated Japanese surrendered aboard the battleship USS *Missouri*, signed a peace treaty, and honored it. Then peace resumed. You behave differently in war versus peace, making the distinction between them crucial.

The Western construction of war versus peace, however, is a false dichotomy, one that cunning adversaries exploit. China can get away with almost anything in the space between war and peace, and they do. As any American admiral will tell you, in private: "Give us the order, and we can take care of the South China Sea in one afternoon." Beijing knows this too. But they also know Washington has a light bulb vision of war: it is either on or off. The trick is to maneuver, while keeping America's war switch flipped to "off," so the superpower remains docile and at "peace." China accomplishes this through a dangerous game of brinksmanship, going right up to the edge of war, or what the West thinks is war, and then stopping. China escalates to deescalate, but keeps everything it captures (or creates). Done enough times, this gradual incrementalism will eventually win the South China Sea, one island and ally at a time.

China leverages the space between war and peace for advantage. They throttle their actions so they remain just below the United States' threshold for "war," when it will flip the light switch to "on" and unleash fire. To conventional warriors, the South China Sea looks frustratingly like a "non-war war," and that's how China wants it. They pull a strategic jiujitsu move on the United States, using Washington's paradigm of warfare against it, and this strategy is proving more effective than a fleet of aircraft carriers. The trick is to do it slowly, akin to boiling frogs, so as to not alarm the United States. If successful, Washington will realize the gravity of the situation too late, like French during the blitzkrieg.

Third, the use of conventional weapons, but in unconventional ways, can befuddle conventionally-minded adversaries. For the past 100 years, the Kremlin has had the same objective: a disunited Europe. During the Cold War, the Soviets staged massive military exercises on the border, designed to strike mortal dread into NATO, which it did. Operation Zapad-81 ("West-81") was an eight-day show of force involving 100,000 to 150,000 troops, arrayed in battle formation, and ready to invade. Moscow assured NATO it was just an exercise, but NATO could never be sure. Nothing stresses alliances like the threat of total annihilation.

Today, when Russia wants to destabilize Europe, it does not threaten military action, as the USSR did. Instead, it bombs Syrian civilians. This helped create a tidal

wave of refugees that crashed onto the shores of Europe, resulting in Brexit, and the rise of right-wing parties across the continent that want to leave the European Union. It became a crisis for NATO. General Philip Breedlove, the supreme allied commander of NATO and the head of the U.S. European Command, said Russia and Syria had turned migration into a weapon by systematically bombarding civilian centers. "Together, Russia and the Assad regime are deliberately weaponizing migration in an attempt to overwhelm European structures and break European resolve," Breedlove told the Senate Armed Services Committee.[792] The Soviets would have dreamed for such outcomes. Putin achieved what the politburo could not, by weaponizing refugees rather than threatening conventional force.

Fourth, war is becoming epistemological, and this changes how you win. In conventional war, big battles determined winners and losers: Waterloo, Gettysburg, Stalingrad, and Midway. In modern war, battlefield victory is irrelevant. In 2003, the U.S. military easily defeated the Iraqi army, and President George W. Bush stood on the deck of an aircraft carrier declaring "Mission Accomplished." But destroying the enemy's conventional forces proved unimportant, and the war waged on for years. The phrase "Mission Accomplished" has devolved into a meme denoting clueless failure. Winning battles no longer wins wars, a trend since 1945: the Vietnam War, the USSR's and the United States' wars in Afghanistan, and Israel's 2006 war in Lebanon. Those who think ISIS was defeated, simply because they ceded the field in Raqqa and Mosul, were mistaken. ISIS and related groups will rise again, as long as their virulent ideology exists, and F-35s cannot prevent that.

Today, discerning truth from lies determines winners, rendering the armed forces secondary in modern war. Influence is now the strategic weapon of choice, supplanting firepower, and the logic is compelling: who cares about the sword, when you can manipulate the arm that wields it? Moscow has prioritized what it calls "information confrontation" to guarantee information superiority in peacetime and wartime. RT News is not a media company, but an intelligence operation, funded by the Kremlin, and its purpose is not information, it's disinformation. The "Troll Factory" is a cyber army that manipulates public opinion to serve Russia's interests, and it is owned by war oligarch Yevgeny Prigozhin, who also owns the Wagner Group. Both are powerful, because they weaponize information in an information age.

Russia has become a disinformation superpower, employing a "kill 'em with confusion" strategy. And it's working. The evidence is everywhere: making the 2014 war in Ukraine invisible, stoking the Brexit vote, and spinning Russia's dubious role

in the Middle East and Africa. The main threat is hacking democratic elections across the United States and European Union and choosing pro-Russian leaders. However, their recent conventional war blunders in Ukraine have cost them significant influence gains.

China also prioritizes deception, a key feature of Chinese strategic culture since Sun Tzu's *Art of War* and the ancient Thirty-Six Stratagems. Beijing's grand strategy is called the "Three Warfares," and it relies on subversion, not firepower, to become regional hegemon by October 1, 2049, the centenary of the founding of the People's Republic of China. The warfares are ways of fighting and they are influence, lawfare, and economic power. Conspicuously absent is a fourth military warfare. Like Russia, China knows conventional war is antiquated, and armed force wins in "ever decreasing scenarios."[793] The Three Warfares succeeds because it disguises war as peace, fooling conventional warriors who can only think about war in terms of military action. By using nonmilitary tools, China effectively masks its conquest. War colleges in the United States do not take economic and political warfare seriously, and almost no flag officers have a background in economics.

China's First Warfare is strategic information operations, and they go beyond Russia's cyber trolls and state-spun "news." When was the last time you saw a Hollywood movie with a Chinese villain? It seems an obvious choice, given all the bad guys with Russian and Middle Eastern accents. The reason is because China bought Hollywood. They green light films that matter to them, and ban "un-Chinese" movies from their domestic market, the second largest in the world. Hollywood kowtows to Beijing's market power, and studios will even create and alter content to appeal to Chinese consumers and avoid censorship by the Communist Party. In a remake of the 1984 cult classic *Red Dawn*, the studio swapped out Chinese villains for North Korean ones at the last minute to appease Beijing. In the disaster movie *2012*, humanity is saved because the Chinese government had the foresight to build life-saving arcs. In *Gravity*, Sandra Bullock survives by getting herself to the Chinese Space Station. Such examples are ubiquitous. China always casts itself as the hero, subtly influencing the world's upcoming generation, as Hollywood did in the past.

In an era of epistemological warfare, Hollywood is a weapon of mass destruction and is increasingly speaking Mandarin. China can shape its own strategic narrative, while denigrating those of rivals. Who needs battlefield victory, when you can sap your enemy's will to fight in the first place? Or, make their children cheer on Beijing? It is winning hearts and minds on a global scale. To this end, China is building its own

Hollywood back home, changing movies from "Made in China" to "Made for the World." The recent Chinese blockbuster *Wolf Warrior 2*, a patriotic movie about a Chinese soldier rescuing Chinese nationals from conflict in Africa, broke records by bringing in $874 million. China is quietly building an arsenal of soft power.

In future war, victory goes to the cunning, and not necessarily the strong. Subversion will be everything, because it turns the adversary into a sock puppet. Who cares how many nuclear weapons you have, if you do not know where to point them? Russia, China, Iran, and others are honing the dark arts, while the United States is buying more tank rounds. It *is* the Maginot problem.

Here are some examples of future war that will make the conventional warrior's head explode. What good is a high-tech military, if your microchips are made by the enemy? The West's global supply chains may already be compromised by China, and why Congress passed the CHIPS and Science Act (2022) with rare bipartisan support. Or, what if Russian active measures corrupted U.S. intelligence databases, analysis, and conclusions. Why invade a country when you can trick the United States (or someone else) into doing it for you? Or, we all know America is in the middle of a culture war, perhaps the biggest since the 1850s. Democracies are messy, and it is okay if the nation is enduring a family quarrel. What if foreign powers are fanning the flames of discord, in sophisticated and targeted ways? Is it war? Is it peace? It is the future.

Adapt or Perish

"Culture eats strategy for breakfast," according to Peter Drucker, a management expert. Washington's strategic culture has the Maginot Mentality. It possesses the best military in the world, but is stuck in the fantasy of yesteryear, and that is why it has stopped winning wars. It yearns to fight "conventionally," like it is 1945, and then wonders why it struggles against vastly weaker foes. Conventional warriors gnash their teeth in cognitive dissonance. Experts have forgotten what war is. Buzzwords have replaced ideas, as authorities argue over the "gray zone" and "war by other means"—bizarre Pentagon jargon for wars that don't prioritize bombs. The national security establishment does not know how to win post-conventional wars, leaving us all vulnerable.

Warfare has moved on, and America must catch up. Like the French in 1940, the United States thinks itself secure when it is, in fact, dangerously exposed. It believes whiz-bang battlefield technology, and superior firepower, will win the future, while

its enemies outflank it in the present. The United States should not scrap its peerless conventional forces, because sadly there will always be a need for organized violence in war. However, it must learn how to use force differently for modern warfare, and not waste billions of dollars purchasing more conventional weapons. Instead, it should buy weapons that work. For a few F-35 squadrons, the United States could develop capabilities for winning 21st century wars, and dominate great power rivals. Conventional warriors be warned: not all of these weapons will reside in the DoD.

As dire as the future sounds, the United States and its democratic allies are not helpless. It is true that modern warfare favors autocracies because they can control the media, subvert the rule of law, manipulate elections, and other dark arts. This is why autocracies are on the rise everywhere. However, they have a major weakness: autocracies are brittle. They centralize power among the elite, led by a dictator paranoid about job security. A cunning strategist could exploit this, as long as he or she were not a conventional thinker. There are myriad ways to hobble autocracies, for those with the strategic IQ to think beyond brute force. Curiously, the United States used to fight this way during the Cold War but has forgotten how in the interceding years.

To win, the United States must follow warfare into the complicated shadows, and punch back. It should not mirror the Russian, Chinese, or Iranian ways of unconventional warfare because those are tailored to subvert democracies. Instead, the United States must develop its own methods to undermine autocracies, which are easier prey in an era of epistemological warfare because they centralize power. In other words, they may be easier to manipulate. Some may cavil that this will violate the laws of armed conflict. However, these so-called "laws" were established to govern conventional warfare, not contemporary conflict, and they also suffer from the Victor's Curse. When one thinks about the character of warfare since 1945, rarely do the laws of armed conflict come to mind. To prepare for tomorrow, we must embrace war as it is, not as we wish it to be.

The bigger challenge is that warfare is getting sneakier, but secrets and democracy are incompatible, as the findings of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, or Church Committee (1975), remind us. This means democracies will be disadvantaged in an age of shadow warfare, a fact Russia and China already exploit. This is the real conversation America should be having about its defenses, not how many F-35s and killer robots are needed, or how to shorten kill chains. Should this foolishness continue, the United

States will eventually be tested and will fail. However, this can be averted if we act now, before the crisis. If we do not, those who do not fight conventionally will inherit the world.

About the Author

Dr. Sean McFate is a professor at Georgetown University, Syracuse University, and the National Defense University. His career began as a paratrooper and officer in the U.S. Army's 82nd Airborne Division, and then he became a global private military contractor. He authored *The New Rules of War: How America Can Win—Against Russia, China, and Other Threats*, named a "Book of the Year" by *The Economist.* He also wrote *The Modern Mercenary: Private Armies and What They Mean for World Order* which *Foreign Affairs* called "essential reading." McFate holds a BA from Brown University, MPP from the Harvard Kennedy School of Government, and a Ph.D. in international relations from the London School of Economics and Political Science (LSE).

Discussion Questions

1. Is conventional war obsolete? How conventional is Russia's 2022 war in Ukraine? When was the last time a country started a conventional war and won?

2. What is "war" now? Can you win without firepower? Can China win and avoid major battle, as the United States did in the Cold War?

3. For the past 70 years, luddites have routinely overcome technologically advanced militaries. How decisive is technology in modern war?

4. How does a democracy defend itself against disinformation, yet not lose its democratic soul? Censorship and other illiberal measures lead to autocracy. But what happens if democracies do not try?

5. Some consider unconventional warfare illegal, dirty, and dishonorable. Is it somehow better to lose honorably, than win dishonorably? When was the last time a conventional warrior won a war "honorably"?

- Qiao Liang & Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).
- Stefan Halper, *China: The Three Warfares* (New York : University of Cambridge, 2013) , pp. 9-27 and skim the rest.
- Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action," Carnegie Endowment for International Peace, June 5, 2019.
- Eran Ortal, "The Fly on the Elephant's Back: The Campaign between Wars in Israel's Security Doctrine," *Strategic Assessment: A Multidisciplinary Journal on National Security* 24, no. 2 (April 2021).
- Sean McFate, *The New Rules of War: How America Can Win—Against Russia, China, and Other Threats* (New York: Morrow, 2019).

Great Power Confrontation in the 21st Century for the Baltic States

Lt Col Karl Salum

ABSTRACT

This article describes the constant pressure, and aggressive behavior, that the Russian Federation has been conducting toward the Baltic states. The Baltic states have reduced their vulnerabilities in multiple domains and are conducting an active battle against Russian disinformation efforts both in the Baltic states and in the wider West.

Membership in the European Union (EU) and NATO is the most vital guarantee of continuing stability, security, and sovereignty of the Baltic states. The Russian minority population in Estonia and Latvia are a significant factor that Russia seeks to exploit. The main vulnerability of the Baltic states continues to be their military inferiority when compared to Russia. This has been partially alleviated by the deployment of allied units in accordance with the decisions taken at NATO Wales Summit of 2014, and enhanced by the decisions taken at the Warsaw Summit in 2016.

Nevertheless, the significant escalation of the Russian aggression against Ukraine in February 2022 has shown that it takes far larger forces to halt, and push back, a conventional military campaign. If Russia decides to engineer a rebellion against the Baltic governments similar to the events that unfolded in eastern Ukraine in 2014, and enhance it with aggressive military posturing around the Baltic states land and sea borders, NATO will face an escalation and reinforcement challenge which requires very quick decisions and implementation. The Baltic states have little operational depth, and the lines of communication to the rest of Europe can be cut off far easier than in Ukraine. Despite losses incurred in Ukraine, Russia maintains sufficient resources to reconstitute its military to the level of executing a limited land-grab style, *fait accompli* in one or several Baltic states. Under the umbrella of possible Russian nuclear blackmailing, the end results of such events are unpredictable with one exception: the people in areas targeted and occupied by Russia will suffer a similar fate as Ukrainians have since 2014.

Introduction

The Baltic states have been subjected to pressure from Russia across the whole PMESII (political, military, economy, social, information, infrastructure) spectrum since regaining their independence in 1991. Russia's focus on a particular Baltic state, or a specific domain, has been shifting throughout the decades depending on:

1) Russia's own needs regarding its national interests;
2) the dynamics of Russian relations with the larger West; and
3) how Russia views some Baltic states' policy choices, and whether it can seize opportunities from them.

The general trend of Russian malign pressure has, however, remained constant. The Baltic governments, as well as some local governments with sizable Russian minorities, have had to keep this pressure in mind when considering policy options. Russia continues to view the independence of Baltic states, which it conquered during

history from various Western kingdoms, as an anomaly grounded in a temporary lapse in great power politics. What irritates Moscow even more, is that among the Western nations, the Baltic states have often been at the forefront of pointing out how Russia's policies and actions violate basic human rights and freedoms, thus partially contributing to the increased tensions between Russia and the West.

The Baltic states have now been independent for longer than the first period of independence after World War I (1918-1940). Throughout both periods, Russia's attempts to subvert and erode the Baltic states' independence and sovereignty have continued in a relatively uninterrupted manner. Whether these attempts are called irregular, hybrid, or unrestricted warfare, "gray zone threats," great power politics, or "competition below the threshold of armed conflict" is a subject for academic or policy-level debates. The label applied to the Kremlin's activities holds little relevance for those in the Baltic states whose jobs are to deal with Russian pressure and its effects. However, these attempts and lessons learned must be shared among allies and partners, to better prepare our societies for Russian pressure. Smaller neighbors have witnessed the ultimate manifestation of Russian pressure in Ukraine, especially since the significantly expanded invasion on February 24, 2022. The governments and societies in Russian neighboring countries must get ready for the possibility that the aggression against Ukraine will not be the last war Russia may seek to conduct against its neighbors.

In the 1990s, Russian action was generally restricted to the economic domain and consisted mostly of varying the access of Baltic products to the its market by, for example, citing various quality and sanitation reasons for banning agricultural products. When opportunities or need arose, Moscow also played the Russian minority card, especially against Latvia and Estonia, usually complaining about citizenship and language policies and consequently, the alleged secondary status of local ethnic Russians. At the same time, Russia has until very recent years benefited from practically unlimited transit options for import goods through Baltic ports and rail lines, given the very limited capacity of its own ports and rail transit network in the Gulf of Finland. During this period, there were no notable incidents of military pressure, with the exception of limited air border violations.

The following essay will look at examples of Russia's aggression toward the Baltic states, and describe the various aspects across all domains related to this pressure. The essay will also look at the countermeasures, or mitigating factors, that the Baltic states utilize and highlight the key trends that are likely to continue in the future as well.

EU and NATO Membership as a Significant Boost to the Comprehensive Security of Baltic States

The Baltic states became significantly more stable and secure in the economic and military domains upon joining the European Union (EU) and the North Atlantic Treaty Organization (NATO) in 2004. For a brief period, it seemed that they had finally come in from the proverbial cold. However, in the first decade of the 21st century, Russia's foreign policy became increasingly assertive. President Putin's well-known speech at the Munich Security Conference in 2007 can be considered as Russia's first public declaration of fighting back against Western influence. In retrospect, the window of opportunity for the Baltic states to join the Euro-Atlantic international organizations, and acquire enhanced security guarantees, was very narrow, comprising roughly from the invitation to join NATO in 2002 to Putin's speech and the Bronze Soldier riots in Estonia in 2007.[794]

As a part of such an assertive foreign policy, Russia began to view the Baltic states as a soft spot through which to launch attacks against both NATO and the EU. Russia's aim was to take advantage of the different perceptions towards Moscow within these organizations, and prevent them from adopting policies not suitable for Russia. Thus, Russia's focus shifted onto the social and information domains which seemed far more promising for success. The two factors benefiting Russia are the close proximity of the Baltics, and the sizable Russian minorities in Estonia and Latvia. Consequently, the political pressure on the Baltic states also increased, combined with frequent information offensives on traditional subjects such as the treatment of Russian minorities. Russia has sought to demonstrate to the EU and to NATO that the Baltic states were dysfunctional, harmful to the organizations' interests, and not worthy of membership and protection.

In the social domain, Estonia and Latvia have been, and continue to be, easier targets due to the Russian minority populations living near their borders as well as in the national capitals. For various reasons, ethnic Russians in Estonia and Latvia have historically had a lower level of income, which presented an easy opportunity for information operations.[795] It has to be noted that the aforementioned levels of income and living standards were, and continue to be, considerably higher than that of their compatriots in Russia proper—a fact that Moscow has always chosen to conveniently ignore, but which has in practical terms reduced the influence of their messages at the grassroots level.

Russia's pressure has been most steady and comprehensive in the information domain, targeted at domestic audiences, those in the Baltic states, and in other Western states beyond. In the Baltic states, there have been some efforts to control Russian activities in the information domain, especially since the annexation of Crimea in 2014. Namely, the regulatory focus has been on containing the spread of Russian messages in public media and online information channels. In the past, Baltic governmental information efforts have been directed towards promoting the benefits of being in the European Union, and demonstrating the adversity of Russian government actions. The main message for the internal and external audiences is to not fall prey to Russian propaganda or direct influence. These efforts in the information domain are mutually supportive of activities by Baltic internal security services, who track specific Russian individuals of interest and monitor possible networks.

Baltic government-mandated information efforts have been further intensified since February 2022. For example, Russian TV channels are no longer offered by Baltic cable television providers. In Estonia, local Russians have found a way around the ban by purchasing satellite dishes, or simply viewing these channels via internet as the Estonian government has not restricted online access to such media. To compete with these, in 2015, Estonian and Latvian governments stood up their own state-funded TV channels which offer various content, including news and entertainment in the Russian language. However, these channels are less popular, compared to the major Russian channels that are much better funded and deliver much more entertainment, not to mention other content that better appeals to the worldview of their ethnic kindred.

Since 2007, cyber-attacks originating from Russia have become a regular occurrence in the Baltic states. Their intensity has increased, especially after the annexation of Crimea and the subsequent sanctions implemented by the European Union. According to the Estonian Information System Authority, another notable rise occurred after February 24, 2022. In 2022, notable targets in Estonia included all larger private media companies.[796] Cyber-attacks seem to be supporting wider efforts in the information and social domains, spreading Russian messages, and denying the people the use of various information systems in the public and private sectors.

In the political domain, Russia has not enjoyed any significant successes in influencing either local- or national-level political processes. In Estonia, Russian efforts over the last 30 years have not produced a stable and well-represented political party with a clearly Russian-friendly agenda. This situation has caused ethnic Russian politicians to join other political parties, and try to work their way up. During this process, they

usually have had to tread carefully and avoid overt pro-Russian perceptions in order to avoid being sidelined by party leadership. This posture does not mean that these politicians are not necessarily standing up for their kin. Rather, they must be more cautious in their rhetoric and activities. In Latvia, Russian-friendly political parties have been more successful, but the end result is the same: no major influence in national-level politics. Due to differences in their approaches, ethnic Russian politicians in the Baltic states rarely present a unified front across party lines, when vouching for a pro-Russian agenda. Their influence on national and local level policies is therefore diluted.

As a positive trend, vulnerability and susceptibility to Russian influence is ameliorated by a generally low level of political activism in the Baltic states. There is no regular habit of political violence. Protests occur in small sizes and intensity, and there is very rarely rioting.[797]

The Baltic states' economic dependence on Russian trade has been dwindling over time. Further, the Baltic states do not possess any significant industry that would be of interest for Russian investments, or where such investments would even be welcome. As a result, the amount of Russian money in the Baltic economies is relatively small, and thus incapable of having a significant effect on local- or state-level policies.

The last two decades have shown that, in general, Russian hostile efforts towards the Baltic states across the PMESII spectrum are focused on increasing domestic discontent and dissatisfaction with the governments, using any possible topic or trend. Russia's goal is to create political turbulence and cleavages within the Baltic societies, resulting in reduced societal resilience. This requires very good knowledge of the local intricacies, as well as skilled middlemen, or agents, whose behavior would not rise suspicion of acting on behalf of Russia. Such personnel can successfully operate in a permissible human terrain, that is, in areas with significant Russian population. Needless to say, such areas are under heavy scrutiny by the internal security services. For example, the efficiency and effectiveness of the Estonian counterintelligence has been demonstrated by the high number of Russian spies and collaborators captured and sentenced.[798] As a result, Russia has had to resort to "economy agents" who focus on more insignificant targets, are of lesser quality, and can be captured more easily.

In Estonia, counterintelligence efforts are also directed at shrinking the pool of support for Russia by identifying and tracking individuals who may be prone to influence and recruitment by Russia's Federal Security Service (FSB, the successor of the Soviet KGB) and Russian Military Intelligence (GRU). These individuals, usually ethnic Russians living in Estonia, fall into two broad categories: those with business

or family connections to Russia, including low-level criminals such as smugglers, and those susceptible to blackmailing or other pressure.

Despite setbacks, Russia's special services, mostly FSB and GRU, continue their efforts in the Baltic states to establish and maintain networks for collecting information. Additionally, it is highly likely that the FSB and GRU also see these networks having a more active role in preparation of the environment. FSB and GRU preparations for the expansion of aggression against Ukraine are gradually being publicized, and serve as a rich field for lessons learned for the consideration of Baltic internal security services.[799]

How Does it all Fit Together?

According to the United States' 2020 *Irregular Warfare Annex to the National Defense Strategy*, irregular warfare is a, "struggle among state and non-state actors to influence populations and affect legitimacy."[800] In a broad sense, this is applicable for Russia's activities in, and concerning, Baltic states. However, the main concern for small states is to predict whether and when the struggle might become violent. The key challenge here is resources: small states have to choose wisely when and how to employ their finite resources, in order to maintain sovereignty and independence. The margin of error in early warning, and responding appropriately to a looming crisis, is rather narrow for small states. As Dr. David Ucko and Dr. Tom Marks emphasize, "violence in irregular warfare is often deliberately ambiguous or even implicit—until suddenly it is not. [...] This ambiguity makes it difficult to delineate where strategic competition ends, and irregular warfare begins."[801]

However, if we look at Russia's activities and messages from the strategic perspective, it would appear that Moscow is conducting irregular warfare against the West as a whole. At the strategic level, Russia's targets for influence, which, according to definitions, is the nucleus of irregular warfare, are thus in Washington, London, Paris, and Berlin, not in Tallinn, Riga, or Vilnius. At the same time, the Baltic states remain important for the West as allies, especially in light of their geopolitical location and consequent security issues, which former Swedish Prime Minister Carl Bildt described in 1994 as "The Baltic Litmus Test" for wider European security.[802] This presents Russia with a dilemma: too much direct pressure on the Baltic states can invoke an unwanted reaction from major powers, such as reinforcements or other reassurance measures.

In terms of the strategic competition between Russia and the West, the Baltic states are just a convenient location where Moscow wishes to remain the main actor controlling the intensity of the competition. There are similar locations of interest along

Russia's periphery, in the form of frozen conflicts and Russian "peacekeeping" forces and also in the Middle East. While Russia focuses on competition along its periphery mostly for security reasons, it also seeks to maintain its influence and importance in the global competition for resources elsewhere, especially in the Middle East.

Russia's center of gravity for implementing hybrid threats against Estonia and Latvia continues to be their ethnic minorities in these states. The state-driven integration of Russian minorities into the Baltic nations has not been very successful. The affinity towards Russia continues to be obvious, especially among those 40 years of age and older, who have some recollection of life in the Soviet Union. These are also the hardest groups to shift, in terms of their orientation towards Russia. One option for Estonia and Latvia would be to simply "wait it out." The new generations, those younger than 30, are focused more on Europe, and the options of prosperity it offers vis-à-vis Russia. Education at school, and how they are raised by their parents at home, are the critical factors or linchpins.

Thus, Russia's desire to maintain some sort of influence over its center of gravity in the Baltic states—their local ethnic kin—has been and continues to be a long game. It is becoming more challenging, as the living standards in the Baltic states continue to rise and the benefits of EU membership are beginning to surpass the effect of Russia's sweet talk and ethnic connections. As one example of this shift in attitudes, the number of Russian citizens living or residing in Estonia acquiring Estonian passports significantly grew in 2022, mainly due to the risk of getting drafted or mobilized into the Russian military otherwise.[803]

Gazing into the Future: Potential Russian Kinetic Risks

In order to assess the potential dynamics of Russia's pressure on the Baltic states, one option is to view these dynamics through the broad categories of hybrid warfare identified in Dr. Andrew Radin's RAND report, *Hybrid Warfare in the Baltics*: 1) nonviolent subversion, 2) covert violent action, and 3) conventional aggression supported by political subversion.[804] For the Baltic states, the third category is the most dangerous one, which will be elaborated upon more below.

Unless there are serious shortcomings in the work of Baltic states' internal security agencies, or if the Estonian and Latvian governments for some reason decide to enact extremely antagonistic policies towards their Russian minorities, Moscow's potential for realizing decisive success in the first two categories does not seem very plausible in

the near future. Another factor contributing to the reduced Russian potential is the ongoing war in Ukraine, which ties up valuable resources and forces. The FSB and Russian *Rosgvardiya*, an internal security-focused military organization, have likely had to contribute a considerable share of their attention also to the domestic front to guarantee regime stability.

The same optimistic outlook cannot be extended to the possibility of conventional warfare. In light of losses in the ongoing aggression against Ukraine, and the difficulties encountered in reconstituting conventional forces, the force ratio between Russia and Baltic states is slated to be less in Moscow's favor. Nevertheless, Russia will maintain its supremacy in military industry capacity, and reinforcement speed and scale, compared to Baltic states and NATO. For the conventional military, the scale of the task, and the geography of the Baltics, is much more favorable for invasion than Ukraine and if the ambitions and missions are narrowed. They are also easier to execute, especially in case of a *fait accompli.*

Regarding support to conventional war efforts, it is likely that the Russian intelligence and special services would improve their operational practices for the Baltic states. The FSB and GRU have almost certainly learned significant lessons from Crimea and Eastern Ukraine since 2014-2015, especially from the preparation and conduct of the wide-scale aggression of 2022. Their main failures in Ukraine were operational security, as proven by capture of numerous Russian special services' teams, and faulty interpretation of intelligence collected.[805] Both of these can be mitigated by improving operational practices, and reducing the number of key targets in terms of personnel and critical infrastructure that must be hit to have a significant influence on the Baltic states ability to organize, lead, and conduct operations to counter the Russian aggression.

All Russian hybrid threats occur against the backdrop of conventional military superiority vis-à-vis Baltic states. The first example of this could be observed in 2008 in Georgia, where Russia enjoyed conventional military supremacy, and was thus able to conduct various hostile activities in preparation for the invasion in August. After the aggression, Russia continued hybrid pressure with creeping borderization and seizing control over all spheres of life in South Ossetia, officially Georgian territory. The Georgian military, defeated in the short conflict, and wary of the potential resumption of expanded Russian aggression further into its territory, could not resist such activities. A similar situation arose in Eastern Ukraine, in 2014, after the commencement of a Russian-facilitated unconventional warfare campaign, during which significant parts of the Luhansk and Donetsk oblasts were captured by Russian proxy forces. Ukrainian

forces were unable to conduct a conventional campaign to reestablish control over these areas, as they were very likely concerned about a massive Russian conventional operation to prevent this from happening. This resulted in a stalemate, with neither side having sufficient potential to achieve victory.

In terms of predicting and resisting Russian aggression, the main challenge for the Baltic states continues to be a potential miscalculation by the Kremlin of the Baltic and Western allies' resolve to fight back. When its hybrid/irregular activities didn't deliver the desired outcome/effects in Ukraine, both towards the end of years 2013 and 2021, Russia conducted military operations to achieve its goals. The Baltic states have been very successful in fending off Russian pressure in all non-military domains. Would Russia again resort to conventional warfare, especially when it has an overwhelming supremacy in the military domain as the Baltic states are significantly smaller, have less forces and capabilities, and are thus easier to attack? The Baltic states became more keenly aware of this possibility because of the 2008 war in Georgia, but the real wake-up call was the 2014 aggression in Ukraine. Especially since the February 2022 expanded invasion of Ukraine, the Baltic states have embarked on a crash course for preparing for a possible Russian aggression, by acquiring significant combat capabilities and increasing the number of trained troops on high readiness.

Regarding manpower, all Baltic states have now realized that conscription is the most efficient method, in terms of resources and time, to increase the number of troops ready to defend the homeland. Estonia has maintained conscription since regaining independence, Lithuania reintroduced it in 2014, and Latvia is slated to bring it back in the summer of 2023. The main idea behind conscription is to have trained units in reserve, and bring them back periodically for mobilization exercises and refresher training, thus reducing the burden of having a large permanent force on active duty and away from the civilian labor force. Conscription also serves as a vital connection between the military and the rest of society, benefits recruitment to the professional service, and acts as a pool for recruiting into the National Guard which all three Baltic states possess.

In addition to acting as a reserve for the military, former conscripts can also be retrained for internal security, rescue service, border guard, and even auxiliary police functions. The aforementioned services do not have their own designated reserve forces. The war in Ukraine has shown that they are just as vital in providing comprehensive security as the military forces. The number of active personnel providing such services

will likely be insufficient, as demonstrated by the relentless Russian attacks against the civilian population. Previous groups of reserve forces could be a suitable source for internal security and protection functions. For example, in Estonia there have been discussions within the government of allocating some parts of the general military reserve for such tasks. However, it does come with a significant price tag and, so far, there has been no government approval for funding such an initiative.[806]

Forward-Looking Perspective: Finding a Balance Between Acquiring Hard Power and Societal Resilience

Regardless of losses in Ukraine, the balance of power in terms of manpower and combat equipment along the Baltic states' borders, will continue to be in Russia's favor. The Baltic states are unable to purchase the necessary amount of equipment to achieve even some sort of parity, as Russian redeployment potential from the Western Military District alone, not to mention the "donor" Central Military District, is far greater than the Baltic states or even Poland. Another issue with raising the level of military capabilities is that the Baltic states need to spend resources on other parts of the whole-of-government defense approach, while also maintaining the basic living standards for their societies.

The war in Ukraine has shown that it is possible to capture and control territory the size of the Baltic states with conventional forces augmented by *Rosgvardiya*, FSB, and private military companies. With proper intelligence preparation of the battlefield, it is possible to erode resistance capacity by reducing the number of personnel most suitable for organizing and conducting such resistance. In the example of Ukraine, Russian forces had lists of military affiliated personnel and others who could hinder and resist the occupation process.[807] Given the size of the Russian minority, and consequent potential for collaboration in Estonia and Latvia, it is highly likely that similar lists have been crafted in these two countries as well. The success rate of implementing them depends on several factors, but the permissive local environment (i.e., the percentage of ethnic Russians among the population) is likely to play a significant role.

In case of Russian aggression, outnumbered Baltic and in-place allied conventional defense forces would likely gradually trade space for time, while attriting the enemy as much as possible. The conduct of war in Ukraine since February 2022 offers a glimpse of how conventional operations could play out in the territories of Baltic states. Ukraine also offers an example of the importance of resistance capabilities that are meant to

operate in enemy-controlled territory for an unknown period of time with two missions: first, to prevent the enemy from having complete control and, second, to establish the conditions for launching a liberation campaign. Ultimately, it will become a game of numbers where the Baltic states' capabilities are clearly inferior to Ukraine's.

Ceding control of territory, in order to sustain combat capabilities and the ability to continue fighting, will likely be a difficult challenge for Baltic and allied units. The Soviets and the Russians have always conducted civilian targeting as part of their conventional operations. Unlike the Western approach for counterinsurgency, Russians have not shied away from completely destroying infrastructure and deliberately targeting civilians in order to reduce resistance potential. This presents ideological and operational challenges for both conventional forces and resistance forces; they do not have much power to protect civilians, and prevent destruction in areas under enemy control.

Since the annexation of Crimea and occupation of Eastern Ukraine, the Baltic states have paid more attention to societal resilience, especially in terms of defending their societies against Russian propaganda. After Russia significantly expanded its invasion of Ukraine in February 2022, the Baltic governments, and other concerned entities, began focusing additional attention on physical protection of the people, critical infrastructure, and services. These efforts compete against conventional armament programs, economic support measures, and other requirements for state funds. For small economies where national income is largely based on services, and thus dependent on energy prices, it is a challenging task to balance the funding of all of these competing, very important, lines of effort. Throughout the last 15 years, the Baltic states have been reducing their vulnerability to Russian energy blackmail by establishing new connections, such as gas pipelines and electricity cables, to Finland and other Western states. The last remaining connection, a common electric grid with northwestern Russia and Belarus, will be severed by 2025.

The tensions between Russia and the West can be expected to last into the foreseeable future, despite the outcome of the war in Ukraine. While the possibility of regime change in Russia has been discussed in vain for years, Putin's demise would very likely have little to no significant effect on Russian-Western relations. Regardless of the nature and extent of the hypothetical regime change, Russia's nature will not change, and definitely not the way previous aggressor powers of similar scale have in the past, for example, Nazi Germany and Japan.

The main reason behind such pessimism is that it is highly unlikely for any political actor other than the current ruling class of former or current members of force structures, mostly FSB—in Russian referred to as *siloviki*—to seize power and establish governance in the post-Putin era. The new government may even denounce Putin and his acts, much along the lines of Khruschev and the de-Stalinization campaign in the 1950s, for the sake of the West to resume some form of economic cooperation and flow of capital. But in the longer term, probably for the next two generations, this reconciliation will in all likelihood be irrelevant. A post-Putin Russia will likely be governed by a generation that remembers both the era of allegedly Western-caused turbulence in the 1990s, and the new humiliation of the oil and gas-funded and subsequently "newly awakened mighty Russia" by Ukraine and the West. Even when the war in Ukraine ends, and Russia remains economically and conventional-militarily inferior to the collective West, the imperial ideas and desire of being one of the global power centers will not die.

About the Author

LtCol Karl Salum is a lecturer at the Baltic Defence College in Tartu, Estonia. He has served in the Estonian Defence Forces since 1998, mostly in staff and professional military education assignments. In 2006, he deployed to Iraq as a staff officer in the Coalition headquarters. LtCol Salum holds a master's degree from Georgetown University's Security Studies Program, and is a graduate of the US Marine Corps Command and Staff College Blended Seminar Program.

Discussion Questions

1. What are the key vulnerabilities of small states in irregular warfare?
2. What benefits does membership in international organizations provide to small states in defending against irregular warfare?

3. What protective or preventive measures can be undertaken to increase societal resilience against irregular warfare?

4. What are the considerations in resource allocation for different capabilities, and programs, for defending against irregular warfare?

Recommended Readings

- *Societal Security in the Baltic Sea Region: Expertise Mapping and Raising Policy Relevance*, ed. Mika Aatola et al., (Riga: Latvian Institute of International Affairs, 2018). Available at https://liia.lv/en/publications/societal-security-in-the-baltic-sea-region-expertise-mapping-and-raising-policy-relevance-716.
- Alina Polyakova & Mathieu Boulègue, "The Evolution of Russian Hybrid Warfare: Executive Summary," CEPA, January 29, 2021, https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-executive-summary/.
- Eero Epner, "Human Life Has No Value There:" Baltic Counterintelligence Officers Speak Candidly About Russian Cruelty," *Eesti Ekspress,* translated by Adam Cullen, originally published in Estonian October 5, 2022, https://ekspress.delfi.ee/artikkel/120083694/human-life-has-no-value-there-baltic-counterintelligence-officers-speak-candidly-about-russian-cruelty.

National Security Challenges and Irregular Warfare in the 21st Century

F. Dennis Walters and Michael C. McMahon

What's next? What is the way forward? The Irregular Warfare Center's (IWC) first book produced excellent assessments and perspectives on irregular warfare (IW) in the contemporary international security environment. We are confident the results will help the nation's security enterprise be better prepared to incorporate IW concepts into planning processes and operations. The academic and educational research communities are key audiences: domestic, international, civilian, and military. We are certain this publication raised many difficult and challenging questions requiring additional research to formulate cogent responses to contemporary and future IW requirements.

Forecasting, calculating the future, is nearly impossible beyond a year or two out, but organizations must nevertheless plan for that future. The challenge is how? Future projections must not be based solely on what is currently happening, but they must also have a solid foundation in historical experience. The greatest challenges facing national security planners regard the difficulty in understanding what adversaries want, or need to do to achieve them. Comprehending past and present events, as well as potential competitor desires, is a complex task but a critical approach to planning processes.

This book is one of IWC's initial forays into the national IW dialogue. Enabling this valuable dialogue to address perspectives on appropriate national security structures, strategies, and policies also helps the Center respond to its Congressional mandate. Congress established the Center to foster increased discourse into the role of IW across the nation's security enterprises to better prepare the United States, its allies, and its partners for the challenges in pursuing it. Tasked to "amplify, illuminate, and address" the nation's IW threats, we hope we met our goal and the reader understands that "IW is neither new nor irregular."

Irregular Warfare and International Security

Tensions are increasing within the international system. Although these risks may appear novel, there are historical perspectives and trends that can guide in assessing IW's role in current and future security environments. A historical example is the post-World War II (WWII) "Cold War" period. As the name indicates, conflicts and wars during this period were different than the preceding, hot, "world wars." In hindsight, the Cold War's significant difference was major power reticence to conduct large-scale, conventional war directly against one another. Of course, conflict and tension continued within the international order and conventional war occurred frequently, but not, except with the partial exception of the early-phase Korean War, directly between major powers.

These tensions continued despite efforts to create an international organization designed to ensure peace and stability between nation-states. The United Nations (UN) was created to be a more inclusive and powerful supranational organization than its predecessor, the League of Nations. Unfortunately, both transnational and internal conflicts remained. Although major powers avoided catastrophic conventional and nuclear conflicts, they routinely engaged in IW. Using this historical paradigm today, the world's major powers are already engaging in IW, and almost certainly entering into another cold war phase. A renewed cold war paradigm is therefore appropriate to evaluate challenges from global and regional state adversaries such as Russia, China, Iran, and North Korea. However, the rise of para-state, near-state, and non-state actors during the last quarter of the 20th Century continues to present major challenges to international order and stability.[808]

Cold War as a Recurring International Security Paradigm

This mix of state and non-state actors and adversaries continues a pattern found in the 20th Century's two post-world war eras. Following World War I (WWI), the major powers created the League of Nations, and managed to avoid direct conflict with each

other during the 1920s and most of the 1930s. Although containing postwar Germany was a primary motivation, interwar conflicts were limited to major power aggression against weaker states, and proxy wars between major powers. Examples of the former are Japan's invasion of China, and Italy's conquest of Ethiopia.[809] A proxy war example was the Spanish Civil War when fascist powers, Germany and Italy, supported the nationalists. Communist Russia supported the republicans directly and sponsored the "International Brigade," a non-state proxy force of 50,000 international volunteers.[810] During this first "Cold War," the League of Nations could not maintain, nor create, peace and failed to become an international collective security organization. The European WWI victors would not risk another major war under League of Nations auspices, while isolationist policies precluded United States involvement.[811]

After WWII, the UN was established as an ostensibly more inclusive and powerful supranational collective security framework. Once again, major powers generally avoided direct conflict, and proxy wars reemerged as a common form of international security conflict.[812] A major difference during this second Cold War was the existence of strategic nuclear weapons. The Korean War started as a proxy war, much like the Spanish Civil War, with Russia and China supporting the north and the United States and its allies the south. North Korea's invasion almost succeeded, but following its military collapse, China's intervention turned a limited proxy war into a protracted and stalemated Sino-American war.[813] The United States, the world's only nuclear power, nevertheless chose not to use nuclear weapons to break this impasse.[814]

Although the United States and its allies sought to contain, and avoid direct conflict with, Russia and China, the UN also failed to create an effective collective security system, and was only marginally effective in cases peripheral to great power interests.[815] This created a schism with the "West," led by the United States, opposed by a "Communist" bloc, led by Russia and China. Eventually, a third group of "non-aligned" states emerged, choosing to remain outside these two competing blocs.[816] This state of international affairs remained until the collapse of the "Soviet" Russian Empire in the early 1990s. The "West" believed it won this cold war and a newly empowered liberal international system.

End of the Cold War: the "End of History" or "A Clash of Civilizations"?

Francis Fukuyama argued Russia's collapse represented the victory of Western liberal democracies over totalitarian communist regimes. The rise of a neoliberal international

order indicated realist balance of power frameworks had been overcome by events.[817] However, Samuel Huntington's response to the optimistic euphoria, and the rise of democratic governments, was "The Clash of Civilizations?" article published in *Foreign Affairs*. Huntington proposed an alternative, pessimistic, perspective of a world released from the constraints of geopolitical competition. The Cold War throttled cultural and ethnic tensions, Huntington argued, and when released, he predicted increased "inter-civilizational" conflict.[818]

During the 1990s, Russia appeared to be transitioning to a democratic form of governance, and China, after a particularly nasty suppression of the Tiananmen Square uprising 1989, continued to integrate its economy and society into the international system.[819] Even in late 1990s, the Iranian Islamic Republic appeared to initiate reforms opening more inclusive processes, with both secular and theocratic relevant political structures.[820] In North Korea, the autocratic dictatorship seemed amenable to reaching an international agreement to halt its nuclear weapons program.[821] However, as the century came to a close, all four states chose not to pursue moderate, or collaborative, policies with the broader international community. Huntington's prediction appeared to come true, with a burst of conflicts and wars associated with the rise of powerful non-state actors. The three "communist" states that "lost" the Cold War (Russia, China, and North Korea), along with Iran, reacted negatively to the "unipolar world" dominated by the United States, the remaining superpower.

A Potential Eurasian Coalition: Authoritarian, Anti-democratic, and Anti-west

The millennium saw our Eurasian adversaries take increasingly aggressive, and confrontational, policies towards regional neighbors and the international community. Vladimir Putin's assumption of power in Russia in 2000 marked the rise of "Putinism," and a return to a more traditional Russian imperialism similar to that of both Tsarist and Soviet policies. China increasingly evidenced a conservative approach to governance, and under Xi Jinping took more domestically authoritarian, and internationally confrontational, turns. Following the 2003 invasion of Iraq, Iran became increasingly hostile and confrontational towards the United States and its allies and partners. Iran spent decades creating a network of allied states, para-states, and non-state organizations to serve as proxies throughout the Middle East. Finally, North Korea repudiated its international non-proliferation agreements, and became a declared nuclear state with weapons systems capable of striking beyond the Korean Peninsula.

By 2023, it appears Fukuyama's prediction of liberal Western democracy's success was premature. To be fair, he admitted to still believe in western-style liberal success, only that it likely will take a long time.[822] On the other hand, Huntington's controversial "Clash" thesis currently appears to offer a more accurate international security assessment following the second Cold War to some. These trends indicate the United States will almost certainly continue to be engaged in IW.

Irregular Warfare and the Viability of Containment in the 21st Century

Will this trend of four autocratic adversarial states executing increasingly combative foreign and military policies continue? The Ukrainian War, the first major Western Eurasian interstate war since WWII, indicates this is possible. What should the United States along with its allies and partners do? The United States must adapt its national security enterprise to reestablish a viable IW capability, similar to that possessed from 1947 to 1991, in order to contain Eurasian adversaries, and avoid catastrophic conventional, or nuclear, war.

Containment as a National Strategy

There is precedent for this course of action. In the late 1940s, George Kennan argued for a new approach to counter "Soviet" Russia's efforts to restore its old Empire. Kennan argued for a containment policy, because he assessed the Russian state was inherently weaker, and more fragile, than many observers thought. Therefore, a strategic containment strategy was enacted, emphasizing patience, diplomacy, and deterrence, rather than overt military conflict.[823] Grudgingly, the United States accepted that WWII did not set the stage for an era of enduring peace, and reevaluated its national security enterprise and historical isolationist policies. The resulting National Security Act of 1947, and National Security Council Paper (NSC-68) of 1950, institutionalized many core WWII security policies: joint military operations, regional commands, increased intelligence capacity, the forward basing of military forces, and the need for strong and formal alliances. However, it is important to note that containment planning acknowledged diplomatic, economic, and psychological capabilities that were also critical.[824]

Although, in previous IW environments, the primary goal was similarly to avoid direct major power conflict, the circumstances and key factors were not the same. The current security environment differs from previous periods in three key areas. First,

there are more nuclear powers, and these countries are more widely distributed across Eurasia. Second, the information technology domain is drastically more complex, and yet is a critical component of a globalized economic system. [825] The internet lowered entrance barriers into mediums with large audiences, creating an increasingly anarchic and chaotic information environment. In addition, liberal democracies and autocratic countries have radically-different governmental approaches to managing this information domain.[826] Lastly, non-state organizations are relatively much more powerful than in previous eras and, potentially, more autonomous from their patron states. These factors indicate managing adversarial coalitions in an increasingly interconnected and complex environment will be more challenging than in previous IW periods.

Containment and the Relationship between Irregular, Conventional, and Strategic Warfare

Irregular, conventional, and strategic (nuclear) types of warfare are distinct, interrelated, and equally important. Of the three types, IW is the least understood, and typically the least resourced, capability. The United States military services traditionally favor large-scale, industrial-type, conventional forces emphasizing technology, mass, and firepower. In addition, America maintains a technologically robust strategic nuclear weapons triad.[827] IW seems to be an afterthought.

The contemporary international security environment inhibits conventional, and strategic, warfare between major powers. Competition, tension, and conflict exist between major powers, usually exhibited via irregular activities in the gray zone.[828] Therefore, it is critical the United States accepts IW as an essential, and primary, type of conflict occurring below the threshold of conventional and strategic war. The challenge facing the United States, its allies, and its partners is how to maintain an effective security enterprise operating across all three types of warfare while overcoming budget, authority, bureaucratic, and cultural challenges that create institutional and governmental biases towards outdated industrial forms of warfare.[829]

The Irregular Warfare Center and A Way Forward

In 2022, Congress identified IW challenges within the Department of Defense (DoD), and the need to increase research and education to help IW capabilities move forward across the national security enterprise. Congress authorized and appropriated

funding to create the IWC to assist the DoD in adapting and creating dedicated forces trained and empowered to conduct complex IW operational activities. The center is to facilitate research and educational programs to foster collaboration and coordination among the government, academia, and industry, both domestic and international. These varied security partners have essential roles and responsibilities necessary for success in an IW security environment.

Is this the next "revolution in military affairs?" Perhaps, but the need for change is much broader. Our nation tends to perceive technological innovation as revolutionary; the same disruptive perspective must be applied to our strategic thinking. We have to change the way we think about competition and conflict, and learn new ways to conceptualize solutions. We are at an inflection point where we must adapt and expand the national security enterprise beyond traditional military responses to challenges, and this is more of a revolution in *national security affairs*. The IWC will take the lead in charting a path forward. The ride will be bumpy, but disruptive thinking usually is.

Acknowledgments

This book is the product of a collective group of intriguing minds who put their heads together and began to imagine how the Irregular Warfare Center (IWC) can contribute to filling the gap in existing literature on irregular warfare, specifically a primer on the subject for professional military education. We, the editors, have many people to thank for helping the Center materialize this extraordinary vision.

Nothing would have been possible without the talented slate of authors who eagerly stepped up to contribute their expertise to the IWC's inaugural work.

To all of our authors—David Ucko, Thomas Marks, Jonathan Odom, Lumpy Lumbaca, Christopher Paul, Mike Schwille, Christian Ramthun, Maurice "Duc" Duclos, DeVan Shannon, Tuan Pham, Christopher Marsh, Ulrica Petterson, Hans Ilis-Alim, Sean McFate, James Sullivan, Parsley Ong, Greg Rattray, Tom Searle, Jenn Walters, and Karl Salum—we appreciate your continuous support and contributions immensely. And to LTG (R) Nagata, who so graciously agreed to pen the foreword and is one of the IWC's earliest supporters: we sincerely appreciate everything.

The editors would also like to express extreme gratitude to all IWC personnel—thank you for your expertise and assistance in copy editing, proofreading, designing, and assisting with every phase of publishing this book from start to finish. Your support and encouragement are truly appreciated.

Endnotes

1 Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, (Washington, DC: The Joint Staff, Nov 2022), p. 104.

2 Summary of the Irregular Warfare Annex to the National Defense Strategy, (Washington, DC: Office of the Secretary of Defense, 2020), p. 2.

3 Nadine Dories, DCMS Secretary of State speech at the Summit for Democracy, 8 Dec 2021, accessed at https://www.gov.uk/government/speeches/dcms-secretary-of-state-speech-at-the-summit-for-democracy on 27 Jan 2023.

4 Lloyd J. Austin, "Establishment of a Functional Center for Security Studies in Irregular Warfare," Secretary of Defense Memorandum, (28 Jul 2022).

5 10 USC § 345, Section 1204, "Modification of Existing Authorities to Provide for an Irregular Warfare Center and a Regional Defense Fellowship Program," James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, (3 Jan 2022), p. 434.

6 Summary of the Irregular Warfare Annex to the National Defense Strategy, (Washington, DC: Secretary of Defense, 2020), p. 1.

7 Robert W. Komer, Bureaucracy Does Its Thing: Institutional Constraints on U.S.-GVN Performance in Vietnam, Report R-967-ARPA (Santa Monica, CA: RAND, August 1972), p. ix.

8 Dennis M. Drew, "U.S. Airpower Theory and the Insurgent Challenge: A Short Journey to Con fusion," The Journal of Military History 62, no. 4 (October 1998): 809–32.

9 Colin Gray, "The Changing Nature of Warfare?" Naval War College Review, vol. 49, no. 2, (Spring 1996), p. 12.

10 Joint Publication 1, Volume 1, Joint Warfighting, (Washington, DC: Joint Staff, 12 Jul 2019), II-15.

11 National Defense Strategy of the United States of America, (Washington, DC: Secretary of Defense, Oct 2022), p. 2.

12 https://study.com/academy/lesson/janus-roman-god-origin-mythology-family.html

13 Gray, p. 10.

14 This chapter draws on David H. Ucko and Thomas A. Marks, Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action, 2nd edition (Washington DC: National Defense University Press, September 2022), and David H. Ucko and Thomas A. Marks, "Redefining Irregular Warfare: Legitimacy, Coercion, and Power," Modern War Institute, October 18, 2022, https://mwi.usma.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/.

15 The term "political opportunity structure" highlights that the structure of society, as implemented through its politics, either enables or hinders individual and group opportunity. Opportunity, in turn, seeks realization of the fundamental troika for existence: sustenance, security, and meaning. The use of "the POS" emerged from academic and systemic efforts to explain the profound alienation of "the Sixties," which had exploded in widespread violence. For a benchmark academic discussion see Peter K. Eisinger, "The Conditions of Protest Behavior in American Cities," The American Political Science Review 67, no.1 (March 1973), 11-28, which in turn was informed by efforts to explain the societal explosion as assessed in The Kerner Report: The National Advisory Commission on Civil Disorders, 1968 report by U.S. Government (Princeton, NJ: Princeton University Press, 2016).

16 Original formulation in Michel Wieviorka, "Terrorism in the Context of Academic Research," in ed. Martha Crenshaw, Terrorism in Context (University Park, PA: The Pennsylvania State University Press, 1995), 597-606. An early treatment of the same subject, using different terminology, appeared in Tom Marks, "Terrorism vs. Terror: The Case of Peru," The Journal of Counterterrorism & Homeland Security International 2, no. 2 (July-August 1990), 26-33.

17 This has been highlighted most recently by Stephen Biddle, Nonstate Warfare: The Military Methods of Guerrillas, Warlords, and Militias (Princeton, NJ: Princeton University Press, 2021).

18 For regular warfare, Warren Wilkins, Grab Their Belts to Fight Them: The Viet Cong's Big Unit-War Against the U.S. 1965-1966 (Annapolis, MD: Naval Institute Press, 2011). For nuclear, "Dien Bien Phu: Did the US offer France an A-bomb?", BBC, May 5, 2014, https://www.bbc.com/news/magazine-27243803. For chemical, David Biggs, "Vietnam: The Chemical War," The New York Times, November 24, 2017, https://www.nytimes.com/2017/11/24/opinion/vietnam-the-chemical-war.html.

19 For an explanation of terminology and categories, among a host of possibilities, particularly useful is an older

doctrinal publication, Air Force Doctrine Document 2-3 Irregular Warfare (August 1, 2007), https://fas.org/irp/doddir/usaf/afdd2-3.pdf. Individual services, notably the army, add further categories to IW, but these are but an extension of mission sets.

20 On this point, "peace" or "stability operations" typically share the same political complexity as counterinsurgency, something often wished away in the official literature. See David H. Ucko, "Peacebuilding after Afghanistan: Between Promise and Peril," Contemporary Security Review 31, no. 3 (2010), 465-485; also, Carlos Ospina, Thomas A. Marks, and David H. Ucko, "Colombia and the War-to-Peace Transition: Cautionary Lessons from Other Cases," Military Review 96, no. 4 (July/August 2016), 40-52.

21 Still unmatched in its laying out of this reality is Dale Andrade, "Westmoreland was Right: Learning the Wrong Lessons from the Vietnam War," Small Wars & Insurgencies 19, no. 2 (June 2008), 145–181. For the relationship between the southern and northern efforts, as now understood based on examination of post-war documentation, Ed O'Dowd, "'What Kind of War is This'?" The Journal of Strategic Studies 37, nos. 6-7 (2014), 1027-1049.

22 A helpful definition of legitimacy points to the "beliefs and attitudes of the affected actors regarding the normative status of a rule, government, political system or governance regime." See Cord Schmelzle, Evaluating Governance: Effectiveness and Legitimacy in Areas of Limited Statehood (Rochester, NY: Social Science Research Network, January 16, 2012), 7, available at <https://papers.ssrn.com/abstract=1986017>.

23 Useful past treatment is Rod Paschall, "Low-Intensity Conflict Doctrine: Who Needs It?" Parameters 15, no. 3 (Autumn 1985), 33-45; also, Wray R. Johnson, "Doctrine for Irregular Warfare: Déjà vu All Over Again?", Marine Corps University Journal 2, no. 1 (Spring 2011), 35-64.

24 Summary of the Irregular Warfare Annex to the National Defense Strategy (Washington, DC: Department of Defense, 2020), 1.

25 The present working definition of Irregular Warfare is "a form of warfare where states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities" (Joint Publication 1, Vol. 1: Joint Warfighting (CJCS, August 2023), as disseminated at Irregular Warfare Forum, 5-7 December 2023.

26 Irregular Warfare Joint Operating Concept (JOC) 1.0 (September 11, 2007), 10, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v1.pdf?ver=2017-12-28-162020-260.

27 George F. Kennan, "The Inauguration of Organized Political Warfare [Redacted Version]," April 30, 1948, 1, Wilson Center Digital Archive, https://digitalarchive.wilsoncenter.org/document/114320.

28 Draws on David H. Ucko, "The Right Force for the Right Mission: Assessing the Role of Special Operations in Strategic Competition," Statement before the Subcommittee on Intelligence and Special Operations, House Armed Services Committee, 118th Congress, Washington DC, February 8, 2023, https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Testimony%20Role%20of%20SOF%20in%20GPC%5B68%5D.pdf, 4. For specific treatment of political warfare, Thomas A. Marks, Counterrevolution in China: Wang Sheng and the Kuomintang (London: Frank Cass, 1998).

29 Excellent treatment, Paul B. Rich, "People's War Antithesis: Che Guevara and the Mythology of Focismo," in People's War: Variants and Responses, eds. Thomas A. Marks and Paul B. Rich (London: Routledge, 2018), 43-79.

30 David H. Ucko and Thomas A. Marks, "Redefining Irregular Warfare: Legitimacy, Coercion, and Power," Modern War Institute, October 18, 2022, https://mwi.usma.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/.

31 Maxwell, D. (2020b). "Resistance and Resilience in Asia – Political Warfare of Revisionist and Rogue Powers." Presentation given to the students and faculty of the US Naval Postgraduate School's Department of Defense Analysis, February 4, 2020.

32 Clausewitz, C.v. (1827). "Two Letters on Strategy." Edited and translated by Peter Paret and Daniel Moran. 1984. US Army Command and General Staff College. Ft. Leavenworth, KS.

33 Jones, R. (2022). "Strategic Influence." Presentation given as part of the Counter-Terrorism and Irregular Warfare (CTIW) concentration, Comprehensive Security Cooperation (CSC) Course 22-3, at the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI APCSS) in Honolulu, Hawaii on 18 October 2022.

34 Dunford, J. (2016). "Implications of Today's Threats on Tomorrow's Strategy." Speech given to the National Defense University. Washington, DC. Accessed on July 2, 2021, at https://www.defense.gov/Explore/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy/

35 US Congress. (2022). "H. R. 6452 To require the Director of National Intelligence to produce a National Intelligence Estimate on escalation and de-escalation of gray zone activities in great power competition, and for other purposes." Washington, DC. https://www.congress.gov/bill/117th-congress/house-bill/6452?s=1&r=79 ; US Congress. 2021a. Strategic Competition Act of 2021. Bill number S.1169. Washington, DC. https://www.congress.gov/bill/117th-congress/senate-bill/1169/text

36 Lin, B., Garafola, C., Mcclintock, B., Blank, J., Hornung, J., Schwindt, K., Moroney, J.D.P., Orner, P., Borrman, D., Denton, S.W., Chambers, J. (2022). "Competition in the Gray Zone: Countering China's Coercion against US Allies and Partners in the Indo-Pacific." Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA594-1.html.

37 Rodgers, M. & Schneider, J. (2021). "Cyberspace as a Battlespace: Irregular Warfare through Bits and Bytes." Podcast time stamp quote at 40:20 minutes. Irregular Warfare Podcast moderated by Kyle Atwell and Shawna Sinnott. West Point, NY: Modern War Institute. https://mwi.usma.edu/cyberspace-as-a-battlespace-irregular-warfare-through-bits-and-bytes/

38 Ibid.

39 Starling, C., Iyer, A., and Giesler, R. (2022). "Today's wars are fought in the 'gray zone.' Here's everything you need to know about it." The Atlantic Council's Hybrid Conflict Project. https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/

40 McMaster, H.R. (2020). Battlegrounds: The Fight to Defend the Free World. (New York, NY: Harper Collins Publishing).

41 Rajah, R., A. Dayant, and J. Pryke. (2019). "Ocean of debt? Belt and Road and debt diplomacy in the Pacific." Lowy Institute for International Policy. https://think-asia.org/handle/11540/11721

42 Priestap, B. (2018). "China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses." Federal Bureau of Investigation. Washington, DC https://www.fbi.gov/news/testimony/chinas-non-traditional-espionage-against-the-united-states.; Wray, C. 2020. "Responding Effectively to the Chinese Economic Espionage Threat." Department of Justice China Initiative Conference, Center for Strategic and International Studies, Washington, DC, February 6, 2020. https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

43 Morris, L.J., M. Mazarr, J. Hornung, S. Pezard, A. Binnendijk, & M. Kepe. (2019). "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War." Pp 30–39. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR2942.html

44 De Wit, D. (2019). "Competing through Cooperation Leveraging Security Cooperation to Counter Chinese and Russian Influence in Africa." Marine Corps University Journal, vol. 10, no. 2, Fall 2019. Pp 162. https://www.usmcu.edu/Portals/218/MCUJ_10_2_Competing%20through%20Competition_Leveraging%20Security%20Cooperation%20to%20Counter%20Chinese%20and%20Russian%20Influence%20in%20Africa_Daniel%20De%20Wit.pdf

45 Kennedy, S. (2021). "Beijing Suffers Major Loss from Its Hostage Diplomacy." CSIS Report. https://www.csis.org/analysis/beijing-suffers-major-loss-its-hostage-diplomacy

46 Kiessling, E. K. (2021). “Gray Zone Tactics and the Principle of Non-Intervention: Can ‘One of the Vaguest Branches of International Law’ Solve the Gray Zone Problem?” Harvard National Security Journal, Volume 12, pp 127.

47 Finley, J. (2021). "Why Scholars and Activists Increasingly Fear a Uyghur Genocide in Xinjiang.” Journal of Genocide Research. 23:3, pp. 348–370. DOI: 10.1080/14623528.2020.1848109; Stern, J. 2021. "Genocide in China: Uighur Re-education Camps and International Response." Immigration and Human Rights Law Review, Vol. 3, Issue 1, Article 2. https://scholarship.law.uc.edu/ihrlr/vol3/iss1/2

48 Gershaneck, K.K. (2020). Political Warfare, Marine Corps University Press. Pp 71–71. https://www.usmcu.edu/Portals/218/Political%20Warfare_web.pdf

49 Doesher, T. (2018). "How China Is Taking Control of Hollywood." Heritage Foundation. https://www.heritage.org/asia/heritage-explains/how-china-taking-control-hollywood

50 Rácz A. (2020). “Band of Brothers: The Wagner Group and the Russian State.” USCIS. https://www.csis.org/blogs/post-soviet-post/band-brothers-wagner-group-and-russian-state

51 Harris, K. (2018). "Russia's Fifth Column: The Influence of the Night Wolves Motorcycle Club." Studies in Conflict & Terrorism, 43:4, 259–273, DOI: 10.1080/1057610X.2018.1455373; Harris, K. 2021. "Russia’s Night Wolves in Australia, Journal of Policing.” Intelligence and Counter Terrorism, DOI: 10.1080/18335330.2021.2014549; Lauder, M. 2018. “Wolves of the Russian Spring: An Examination of the Night Wolves as a Proxy for the Russian Government.” Canadian Military Journal, Vol. 18, No. 3. Pp 6–16. http://www.journal.forces.gc.ca/vol18/no3/page5-eng.asp?utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_the_night_wolves_a_russian_biker_gang_are_a_tool_of_russian_intelligence&utm_term=2018-08-19

52 Brown, A. (2020). "An Enduring Relationship – From Russia, With Love." USCIS. https://www.csis.org/blogs/post-soviet-post/enduring-relationship-russia-love

53 Morris, L.J., M. Mazarr, J. Hornung, S. Pezard, A. Binnendijk, & M. Kepe. (2019). "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War." Pp

48–70. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR2942.html

54 Callamard A. & I. Khan. (2021). "Russia responsible for Navalny poisoning, rights experts say." United Nations News. https://news.un.org/en/story/2021/03/1086012

55 Michaels D. & M. Coker. (2009). "Arms Seized by Thailand Were Iran-Bound." Wall Street Journal. https://www.wsj.com/articles/SB126134401523799287

56 Kiessling, E. K. (2021). "Gray Zone Tactics and the Principle of Non-Intervention: Can 'One of the Vaguest Branches of International Law' Solve the Gray Zone Problem?" Harvard National Security Journal, Volume 12, pp 129.

57 Department of State. (2022). "State Sponsors of Terrorism." Bureau of Counterterrorism. Washington, DC. https://www.state.gov/state-sponsors-of-terrorism/; Byman, D. (2017). "Putting the North Korea terrorism designation in context." The Brookings Institution. https://www.brookings.edu/blog/order-from-chaos/2017/11/21/putting-the-north-korea-terrorism-designation-in-context/

58 Chin, J. U. (2017). "Killing Kim: Political sanctuary, assassination, and why Kim Jong-nam's death won't be the last." Asia and the Pacific Policy Society (APPS). Canberra, Australia. http://ecite.utas.edu.au/121986/

59 Teichmann, F.M. (2019). "Recent trends in money laundering and terrorism financing." Journal of Financial Regulation and Compliance, Vol. 27 No. 1, pp. 2-2. https://doi.org/10.1108/JFRC-03-2018-0042

60 Mullins, S. "Twenty-Five Years of Terrorism and Insurgency in Southeast Asia" in A. Vuving (Ed.) Hindsight, Insight, Foresight: Thinking about Security in the Indo-Pacific. Pp 112–113. Daniel K. Inouye Asia-Pacific Center for Security Studies. https://apcss.org/wp-content/uploads/2020/09/07-mullins-25thA.pdf; Singh, B. (2018). "Crime-Terror Nexus in Southeast Asia: Case Study of the Abu Sayyaf Group." Counter Terrorist Trends and Analyses, 10(9), 6–10. https://www.jstor.org/stable/26487539

61 Tekwani, S. (2020). "Political Violence in South Asia: 1995-2020" in A. Vuving (Ed.) Hindsight, Insight, Foresight: Thinking about Security in the Indo-Pacific. Pp 91. Daniel K. Inouye Asia-Pacific Center for Security Studies. https://apcss.org/wp-content/uploads/2020/09/06-tekwani-25A.pdf

62 Zuberi, KJ (2018). "Use of cyber space by terrorist organizations." International Journal for Electronic Crime Investigation, 2(1), 6–6. http://ojs.lgu.edu.pk/index.php/ijeci/article/view/258

63 Wilson III, I., and Smitson, S. (2016). "Are Our Strategic Models Flawed? Solving America's Gray-Zone Puzzle." Parameters 46, no. 4 (2016–2017). https://press.armywarcollege.edu/parameters/vol46/iss4/; Bhatia, K. 2018. "Coercive Gradualism Through Gray Zone Statecraft in the South China Seas. China's Strategy and Potential US Options." Joint Forces Quarterly, JFQ 91, 4th Quarter, p. 6. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-91/jfq-91_24-33_Bhatia.pdf

64 Mead, W.R., (2013). "The End of History Ends." The American Interest, December 2, 2013. https://www.the-american-interest.com/2013/12/02/2013-the-end-of-history-ends-2/

65 Burgers, T, & Romaniuk, S. (2022). "China's Real Takeaway From the War in Ukraine: Grey Zone Conflict Is Best." The Diplomat. https://thediplomat.com/2022/10/chinas-real-takeaway-from-the-war-in-ukraine-grey-zone-conflict-is-best/

66 Jones, S.G. (2021b). Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare. P. 193. New York, NY: Norton.

67 Babbage, R. (2019b). "Stealing a March Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners, Volume II Case Studies." Center for Strategic and Budgetary Assessments (CSBA), p. 7.

68 Bhatia, K. (2018). "Coercive Gradualism Through Gray Zone Statecraft in the South China Seas. China's Strategy and Potential US Options." Joint Forces Quarterly, JFQ 91, 4th Quarter, p. 29. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-91/jfq-91_24-33_Bhatia.pdf

69 Ibid. 196.

70 Ibid. 189.

71 Nagata, M. (2020). Interview with Jones, S.G, 2021b, in Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare, p 191. New York, NY: Norton.

72 Carment, D. and Belo, D. (2020). "Gray-zone Conflict Management: Theory, Evidence, and Challenges." Air University, US Air Force. https://www.airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zone-conflict-management-theory-evidence-and-challenges/

73 Frialde, M. (2016). "Duterte Says Unknown Donor Paid for His Pre-Campaign Ads." PhilStar. https://www.philstar.com/headlines/2016/03/10/1561872/duterte-says-unknown-donor-paid-his-pre-campaign-ads

74 Ibid. 186-8.

75 Ibid. 199.

76 Layton, P. (2022). "China's Grey–Zone Activities: Concepts and Possible Responses." Journal of the Royal New Zealand Air Force, Volume 7 – Number 1 – 2022, p. 113.

77 Ibid.

78 Mahnken, T., Sharp, T., & Kim. GB (2020). "Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition." Center for Strategic and Budgetary Assessments (CSBA). https://csbaonline.org/uploads/documents/CSBA8209_(Deterrence_by_Detection_Report)_FINAL.pdf

79 Layton, P. (2022). "China's Grey–Zone Activities: Concepts and Possible Responses." Journal of the Royal New Zealand Air Force, Volume 7 – Number 1 – 2022, p. 113.

80 Ibid.

81 Gould, J., & Pomerleau, M. (2022). "Why the US should fight Russia, China in the 'gray zone.'" C4ISR net. https://www.c4isrnet.com/information-warfare/2022/01/04/why-the-us-should-fight-russia-china-in-the-gray-zone/

82 Brook, D.A. (2012). "Budgeting for National Security: A whole of Government Perspective." Journal of Public Budgeting, Accounting, and Financial Management, 24 (1), 34. https://calhoun.nps.edu/handle/10945/57698

83 Swinsburg, P. (2001). "The Strategic Planning Process And The Need For Grand Strategy." P. 7. School of Advanced Military Studies. Kansas Fort Leavenworth, Kansas: United States Army Command and General Staff College Press.

84 Brook, D.A. (2012). "Budgeting for National Security: A whole of Government Perspective." Journal of Public Budgeting, Accounting, and Financial Management, 24 (1), 35. https://calhoun.nps.edu/handle/10945/57698

85 Stoker, D. (2022). Why America Loses Wars: Limited War and US Strategy from the Korean War to the Present. P. 171. New York, NY: Cambridge University Press.

86 Winger, G. & Amador, J. (2022). "Aim Higher: The U.S.-Philippine Alliance Can Do More." War on the Rocks. https://warontherocks.com/2022/08/aim-higher-the-u-s-philippine-alliance-can-do-more/

87 Ibid.

88 Lin, B., Garafola, C., Mcclintock, B., Blank, J., Hornung, J., Schwindt, K., Moroney, J.D.P., Orner, P., Borrman, D., Denton, S.W., Chambers, J. (2022). "Competition in the Gray Zone: Countering China's Coercion against US Allies and Partners in the Indo-Pacific." P. vi. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA594-1.html.

89 Lopez, C.T. (2022). "Building Asymmetric Advantage in Indo-Pacific Part of DOD Approach to Chinese Aggression." US Department of Defense News. https://www.defense.gov/News/News-Stories/Article/Article/3107197/building-asymmetric-advantage-in-indo-pacific-part-of-dod-approach-to-chinese-a/

90 Ibid.

91 Ibid.

92 Manwaring, M. G. (2010). Gangs, pseudo-militaries, and other modern mercenaries: New dynamics in uncomfortable wars. Pp. 164. University of Oklahoma Press.

93 Rehberg, C. (2019). "Overview of US Grand Strategy." Liberty University presentation given for course NSEC 504. Lynchburg, VA.

94 Manwaring, M. G. (2010). Gangs, pseudo-militaries, and other modern mercenaries: New dynamics in uncomfortable wars. Pp. 160. University of Oklahoma Press.

95 Smith, P. A. (1989). On Political War. Pp. 3, 7. Washington, DC: National Defense University Press.

96 Ibid.

97 Kennan, G. (1948). CIA Policy Planning Staff Memorandum. Washington, DC. https://digitalarchive.wilsoncenter.org/document/208714.pdf?v=0dcd3b6b5638d93857f6ba75cee7c0cf

98 Ibid.

99 Codevilla, A. (2009). "Political Warfare: A Set of Means for Achieving Political Ends," in Waller, ed., Strategic Influence: Public Diplomacy, Counterpropaganda and Political Warfare. Pp. 206. IWP Press.

100 Department of Defense. 2020a. Summary of the Irregular Warfare Annex to the National Defense Strategy. Washington, DC. https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF

101 Smith 1989

102 Creswell, J. & Creswell J.D. (2018). Research design: Qualitative, Quantitative, And Mixed Methods Approaches (5th ed.). Pp. 181. Thousand Oaks, CA: Sage Publishing.

103 Yin, R. (2018). Case Study Research and Applications, 6th ed., p.169. CA: Sage Publishing.

104 Hicks, K., Dalton, M., Donahoe, M., Sheppard, L., Friend, A.H., Matlaga, M., Federici, J., Conklin, M., & Kiernan, J. (2019). "By Other Means Part Ii: Adapting To Compete In The Gray Zone." Center for Strategic and International Studies. https://www.jstor.org/stable/resrep22608.1

105 National Security Council. (1950). "National Security Council Report, NSC 68, 'United States Objectives and Programs for National Security.'" Washington, DC: History and Public Policy Program Digital Archive, US National Archives. http://digitalarchive.wilsoncenter.org/document/116191; Department of State. n.d.1. "NSC-68, 1950." Office of the Historian. Washington, DC. https://history.state.gov/milestones/1945-1952/NSC68

106 Huntington, S. P. (1961). The Common Defense: Strategic Programs in National Politics. P. 49. New York: Columbia University Press.

107 Ibid.

108 Larson, E.V., Eaton, D., Nichiporuk, B., & Szayna, T.S. (2008). "Assessing Irregular Warfare: A Framework for Intelligence Analysis." Rand Arroyo Center Report. https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG668.pdf.

109 Ibid.

110 Stringer, K. and Urban, M. (2022). "Irregular Warfare Campaigning and the Irregular Warfare Center." Department of Defense Irregular Warfare Center Press. https://irregularwarfarecenter.org/2022/12/irregular-warfare-campaigning-and-the-irregular-warfare-center/

111 Ibid.

112 Manwaring 155.

113 Furst, A. (1988). Night Soldiers: A Novel. Boston, MA: Houghton Mifflin

114 Clarke, R. & L. Robinson. (2021). “Special Operations Forces and Great Power Competition,” 5 November 2021, in Irregular Warfare Podcast, produced by the Irregular Warfare Initiative. https://mwi.usma.edu/ special-operations-forces-and-great-power-competition/.

115 Sean McFate, The New Rules of War: Victory in the Age of Durable Disorder, (New York, NY: William Morrow, 2019).

116 Harlan K. Ullman, Anatomy of Failure: Why America Loses Every War It Starts, (Annapolis, MD: Naval Institute Press, 2017).

117 David H. Ucko and Thomas A. Marks, Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action, (Washington, D.C.: National Defense University Press, September 2022). https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/Crafting-Strategy-for-Irregular-Warfare_2ndEd.pdf?ver=mFY-dJC9aRGKfjz0E0KK5Q%3d%3d

118 Seth G Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare, (New York: Norton, 2021).

119 Anthony H. Cordesman, “Chronology of Possible Russian Gray Area and Hybrid Warfare Operations”, Center for Strategic and International Studies, December 8, 2020. https://www.csis.org/analysis/chronology-possible-russian-gray-area-and-hybrid-warfare-operations

120 Eugene Rumer, “The Primakov (Not Gerasimov) Doctrine in Action”, Carnegie Endowment for International Peace, June 05, 2019. https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254

121 John R. Haines, “How, Why, and When Russia Will Deploy Little Green Men – and Why the US Cannot,” Foreign Policy Research Institute, March 9, 2016. https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot/

122 Ankit Panda, “Is the Trump administration about to take on China’s Belt and Road Initiative?” The Diplomat, October 19, 2017. https://thediplomat.com/2017/10/is-the-trump-administration-about-to-take-on-chinas-belt-and-road-initiative/

123 Arwa Mahdawi, “China has fully militarized three islands in South China Sea”, The Guardian, 20 Mar 2022. https://www.theguardian.com/world/2022/mar/21/china-has-fully-militarized-three-islands-in-south-china-sea-us-admiral-says

124 Owen L. Sirrs, Iran's Qods Force: Proxy Wars, Terrorism, and the War on America, (Annapolis, MD: Naval Institute Press, 2022).

125 A. Trevor Thrall and Erik Goepner, “Step Back: Lessons for U.S. Foreign Policy from the Failed War on Terror”, POLICY ANALYSIS NO. 814, CATO Institute, June 26, 2017. https://www.cato.org/policy-analysis/step-back-lessons-us-foreign-policy-failed-war-terror and Julia Gledhill, “The Failures of the War on Terror”, Issue Paper, Friends Committee on National Legislation, August 2022. https://www.fcnl.org/sites/default/files/2022-08/FailuresOfTheWarOnTerror.14.pdf

126 Dan De Luce, “After 9/11, China grew into a superpower as a distracted U.S. fixated on terrorism, experts say”, NBC News, Oct. 17, 2021. https://www.nbcnews.com/politics/national-security/after-9-11-china-grew-superpower-distracted-u-s-fixated-n1278671

127 Official NATO homepage. https://www.nato.int/

128 David Ignatius, “Putin warned the West 15 years ago. Now, in Ukraine, he’s poised to wage war”, Washington Post, February 20, 2022. https://www.washingtonpost.com/opinions/2022/02/20/putin-ukraine-nato-2007-munich-conference/

129 Global Times, “GT Investigates: US wages global color revolutions to topple govts for the sake of American control,” December 2, 2021. https://www.globaltimes.cn/page/202112/1240540.shtml Global Times is the English language outlet of People’s Daily, published by the Chinese Communist Party.

130 Jianli Yang and Xueli Wang, "Xi's Color Revolution Obsession", Providence, 29 August 2022. https://providencemag.com/2022/08/xis-color-revolution-obsession/

131 Nicholas Thompson, “This Ain't Your Momma's CIA”, Washington Monthly, March 2001. http://www.washingtonmonthly.com/features/2001/0103.thompson.html

132 History.Com Editors, “Arab Spring”, History.com, updated January 25, 2023. https://www.history.com/topics/middle-east/arab-spring

133 Kim Zetter, “An Unprecedented Look at Stuxnet, the World's First Digital Weapon”, Wired, Updated: Jan 17, 2020. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

134 Juan Carlos Zarate, Treasury's War: The Unleashing of a New Era of Financial Warfare, (New York: Public Affairs, 2020).

135 Abigail Ng, “Middle East leaders praise Trump’s ‘maximum pressure’ campaign on Iran as Biden takes office”, CNBC, January 22, 2021. https://www.cnbc.com/2021/01/22/us-iran-middle-east-praises-trumps-maximum-pressure-campaign-as-biden-takes-over.html

136 Office Of the Spokesperson, “FACT SHEET: The Impact of Sanctions and Export Controls on the Russian Federation”, U.S. Department of State, October 20, 2022. https://www.state.gov/the-impact-of-sanctions-and-export-controls-on-the-russian-federation/

137 Mary Louise Kelly, Alejandra Marquez Janse, and Sarah Handel, “2 years after the U.S. killed Iran's Qasem Soleimani, tensions remain”, Heard on All Things Considered, NPR, January 3, 2022. https://www.npr.org/2022/01/03/1069983221/2-years-after-the-u-s-killed-irans-qasem-soleimani-tensions-remain

138 General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, translated from Russian by Robert Coalson, “The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations” MILITARY REVIEW, 24 January-February 2016. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

139 Jianli Yang and Xueli Wang, "Xi's Color Revolution Obsession", Providence, 29 August 2022. https://providencemag.com/2022/08/xis-color-revolution-obsession/

140 Stuti Mishra, “China warns US to not ‘salami slice’ its ‘red line’ after sanctioning two Americans,” Independent, 23 December 2022. https://www.independent.co.uk/asia/china/china-sanctions-us-citizens-tibet-b2250502.html

141 David Gritten, “Iran protests: Supreme leader blames unrest on US and Israel”, BBC News, 4 October 2022. https://www.bbc.com/news/world-middle-east-63118637

142 Nicholas Carl, Kitaneh Fitzpatrick, Dana Alexander Gray, and Frederick W. Kagan, “IRAN CRISIS UPDATE, DECEMBER 31”, Institute for the Study of War, Dec 31, 2022. https://www.understandingwar.org/backgrounder/iran-crisis-update-december-31

143 Hossein Amir-Abdollahian, Foreign Minister of Iran, "'Terrorist' designation for Iran's IRGC would harm EU security", Al Jazeera, 23 Jan 2023. https://www.aljazeera.com/opinions/2023/1/23/348 ; Maziar Motamedi, "More sanctions as Iran and EU clash over IRGC 'terror' label", Al Jazeera, 23 Jan 2023. https://www.aljazeera.com/news/2023/1/23/more-sanctions-as-iran-and-eu-clash-over-irgc-terror-label ; Maziar Motamedi, "Iran blacklists more European officials as tensions rise", Al Jazeera, 25 Jan 2023. https://www.aljazeera.com/news/2023/1/25/iran-blacklists-more-european-officials-amid-rising-tensions

144 Rachel Treisman, "Russia responds to Zelenskyy's visit by accusing the U.S. of a proxy war in Ukraine" NPR, December 22, 2022. https://www.npr.org/2022/12/22/1145004513/russia-ukraine-us-proxy-war-zelenskyy-visit

145 "UN General Assembly condemns Russia's 'attempted illegal annexation' of four Ukrainian regions by a vote of 143-5", Al Jazeera, 12 Oct 2022. https://www.aljazeera.com/news/2022/10/12/un-condemns-russias-move-to-annex-parts-of-ukraine

146 Stijn Mitzer, et al., "Attack On Europe: Documenting Russian Equipment Losses During The 2022 Russian Invasion Of Ukraine", Oryx, accessed Jan 14, 2023. https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html

147 Andriy Zagorodnyuk, "Ukrainian victory shatters Russia's reputation as a military superpower", Atlantic Council, September 13, 2022. https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-victory-shatters-russias-reputation-as-a-military-superpower/

148 Alexandra Prokopenko, "The Cost of War: Russian Economy Faces a Decade of Regress: The economy's development will be in reverse for at least the next three to five years" Carnegie Endowment for International Peace, 19 December 2022. https://carnegieendowment.org/politika/88664

149 George Glover, "The EU is looking at seizing $330 billion in frozen Russian assets," Business Insider, Nov 30, 2022. https://markets.businessinsider.com/news/currencies/russia-ukraine-investing-european-union-frozen-assets-oligarchs-bonds-stocks-2022-11

150 Vikas Pandey, "Quad: The China factor at the heart of the summit", BBC News, 24 May 2022. https://www.bbc.com/news/world-asia-india-61547082

151 The White House, "FACT SHEET: Implementation of the Australia – United Kingdom – United States Partnership (AUKUS)" April 05, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/

152 Erik De Castro, "Philippines orders strengthened military presence after 'Chinese activities' near islands", Reuters, December 22, 2022. https://www.reuters.com/world/asia-pacific/philippines-orders-strengthened-military-presence-after-chinese-activities-near-2022-12-22/

153 Bethany Allen-Ebrahimian, "Europe turns on China", Axios, September 20, 2022. https://www.axios.com/2022/09/20/europe-turns-on-china

154 Milton Ezrati, "China's Vaunted Belt And Road Initiative Seems To Have Come A-Cropper", Forbes, Nov 21, 2022. https://www.forbes.com/sites/miltonezrati/2022/11/21/chinas-vaunted-belt-and-road-initiative-seems-to-have-come-a-cropper/?sh=2fb88b851e21

155 Chris Devonshire-Ellis, "US Chip Sanctions on China: Analysis and Implications", China Briefing, October 13, 2022. https://www.china-briefing.com/news/us-chip-sanctions-on-china-analysis-and-implications/

156 Abdul Sattar Qassem, "Does Iran control four Arab capitals?", Middle East Monitor, April 4, 2020. https://www.middleeastmonitor.com/20200404-does-iran-control-four-arab-capitals/

157 "Country Comparisons-Real Per Capita GDP", CIA World Fact Book, January 12, 2023 edition. https://www.cia.gov/the-world-factbook/field/real-gdp-per-capita/country-comparison/

158 Nasser Karimi, "Iran holds mass funeral for Guard officers killed in Syria", AP News, August 4, 2022. https://apnews.com/article/islamic-state-group-iran-syria-middle-east-civil-wars-98556e439b71c9ad91c84c454b4b044e

159 David S. Cloud and Ghassan Adnan, "Anti-Iran Protesters Break Into Baghdad Green Zone, Storm Iraqi Parliament", Wallstreet Journal, July 27, 2022. https://www.wsj.com/articles/anti-iran-protesters-break-into-baghdad-green-zone-storm-iraqi-parliament-11658952380

160 Iran International Newsroom, "Lebanese Set Up Opposition Group To 'End Iranian Occupation'", Iran International, 01/11/2022. https://www.iranintl.com/en/202201113052

161 Kasra Aarabi, "Iran's Regional Influence Campaign Is Starting to Flop", Foreign Policy, December 11, 2019. https://foreignpolicy.com/2019/12/11/collapse-iranian-shiism-iraq-lebanon/

162 Eldar Mamedov, "Two years after Soleimani killing: more shadows than light for Iran: Tehran vowed to purge American influence from the region. On that score, their record is decidedly mixed", Responsible Statecraft, January 7, 2022. https://responsiblestatecraft.org/2022/01/07/two-years-after-soleimani-assassination-more-shadows-than-light-for-tehran/

163 Omar Abdel-Baqui and Summer Said, “Hamas Leader Killed in Beirut Was Linchpin of Relations With Iran, Hezbollah” The Wall Street Journal, Jan. 3, 2024. https://www.wsj.com/world/middle-east/hamas-leader-killed-in-beirut-was-linchpin-of-relations-with-iran-hezbollah-dd8fd6e8

164 James Holmes, “Vladimir Putin Has Played Russia's Bad Hand Well”, The National Interest, May 25, 2021. https://nationalinterest.org/blog/reboot/vladimir-putin-has-played-russias-bad-hand-well-heres-russias-strategy-185997

165 Darragh Roche, “Vladimir Putin Says He Was Forced To Invade Ukraine: 'No Other Choice'”, Newsweek, 4/12/22. https://www.newsweek.com/vladimir-putin-forced-invade-ukraine-war-russia-no-other-choice-1697208

166 Anatol Lieven, “Putin’s regime may fall – but what would come next?”, The Guardian, September 27, 2022. https://www.theguardian.com/commentisfree/2022/sep/27/putin-regime-fall-ukraine-west-negotiate

167 Shelley Rigger, Lev Nachman, Chit Wai John Mok, and Nathan Kar Ming Chan, “Why is unification so unpopular in Taiwan? It’s the PRC political system, not just culture”, Brookings, February 7, 2022. https://www.brookings.edu/blog/order-from-chaos/2022/02/07/why-is-unification-so-unpopular-in-taiwan-its-the-prc-political-system-not-just-culture/

168 History.com Editors, “Bay of Pigs Invasion”, History.com, Updated November 9, 2022. https://www.history.com/topics/cold-war/bay-of-pigs-invasion

169 “We Won't Allow a Color Revolution in Venezuela, Moscow Says”, The Moscow Times, Feb. 15, 2019. https://www.themoscowtimes.com/2019/02/15/we-wont-allow-a-color-revolution-in-venezuela-moscow-says-a64509

170 General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, translated from Russian by Robert Coalson, “The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” MILITARY REVIEW, 24 January-February 2016. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

171 Vladimir Putin, “2007 Putin Speech and the Following Discussion at the Munich Conference on Security Policy,” RussiaList.org. https://russialist.org/transcript-putin-speech-and-the-following-discussion-at-the-munich-conference-on-security-policy/

172 Erin Doherty, “Why NATO formed and why Finland and Sweden want to join the alliance”, Axios Explains: Ukraine, Updated Jun 28, 2022. https://www.axios.com/2022/05/16/nato-expansion-ukraine-russia-putin-finland-sweden

173 Staff, “There are no independent countries in the world, Putin says”, CubaSi, 15 February 2019. https://cubasi.cu/en/world/item/16968-there-are-no-independent-countries-in-the-world-putin-says

174 NATO official website, Origins: NATO Leaders: Lord Ismay,

https://www.nato.int/cps/en/natohq/declassified_137930.htm

175 Joseph S. Nye, Jr., Soft Power: The Means to Success in World Politics, (New York: PublicAffairs, 2004).

176 “Marxist-Leninism”, Oxford Reference. https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100137769;jsessionid=03E810D2C48D1385547E71443173B17F

177 Andrew Roth, “Putin compares himself to Peter the Great in quest to take back Russian lands”, The Guardian, 10 June 2022. https://www.theguardian.com/world/2022/jun/10/putin-compares-himself-to-peter-the-great-in-quest-to-take-back-russian-lands

178 Thucydides, History of the Peloponnesian War, Book V, 5.89 https://en.wikisource.org/wiki/History_of_the_Peloponnesian_War/Book_5

179 Sam Meredith, “Few countries are truly sovereign, and Russia is a target of systematic US interference”, CNBC, June 2 2017 https://www.cnbc.com/2017/06/02/few-countries-are-truly-sovereign-and-russia-is-a-target-of-systematic-us-interference-says-putin.html

180 Patrick M. Cronin and Ryan Neuhard, China’s Political Warfare Campaign in the South China Sea, (Washington, D.C.: Center for a New American Security, 2020). http://www.jstor.com/stable/resrep20439.5

181 Lebanese Hezbollah, (Washington, D.C.: Congressional Research Service, January 11, 2023). https://crsreports.congress.gov/product/pdf/IF/IF10703

182 Seth G. Jones, Jared Thompson, Danielle Ngo, Joseph S. Bermudez Jr., and Brian McSorley, The Iranian and Houthi War against Saudi Arabia, (Washington, D.C.: Center for Strategic and International Studies, December 21, 2021). https://www.csis.org/analysis/iranian-and-houthi-war-against-saudi-arabia

183 Garrett Nada and Mattisan Rowan, Profiles: Pro-Iran Militias in Iraq, (Washington, D.C.: United States Institute for Peace, November 10, 2021). https://iranprimer.usip.org/blog/2021/nov/10/profiles-pro-iran-militias-iraq#:~:text=From%20its%20inception%20in%202006,41st%2C%2042nd%20and%2043rd%20brigades

184 Phillip Smyth, Iran Is Outpacing Assad for Control of Syria's Shia Militias, (Washington, D.C.: The Washington Institute for Near East Policy, April 12, 2018). https://www.washingtoninstitute.org/policy-analysis/iran-outpacing-assad-control-syrias-shia-militias

185 The ChinaFile Editors, "Document 9: A ChinaFile Translation", November 8, 2013. https://www.chinafile.com/document-9-chinafile-translation

186 Central Intelligence Agency, Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD, with Addendums, April 25, 2005. https://www.govinfo.gov/app/details/GPO-DUELFERREPORT

187 David E. Sanger, Anton Troianovski, Julian E. Barnes and Eric Schmitt, "Ukraine Wants the U.S. to Send More Powerful Weapons. Biden Is Not So Sure", New York Times, Sept. 17, 2022. https://www.nytimes.com/2022/09/17/us/politics/ukraine-biden-weapons.html

188 Doug Bandow, "Washington Will Fight Russia to the Last Ukrainian", CATO Institute, April 14, 2022. https://www.cato.org/commentary/washington-will-fight-russia-last-ukrainian

189 Sparkle Hayter, "France Rises Above Its Politics", New York Times, May 4, 2002. https://www.nytimes.com/2002/05/04/opinion/france-rises-above-its-politics.html

190 David H. Ucko and Thomas A. Marks, Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action, (Washington, D.C.: National Defense University Press, September 2022). https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/Crafting-Strategy-for-Irregular-Warfare_2ndEd.pdf?ver=mFY-dJC9aRGKfjz0E0KK5Q%3d%3d

191 https://www.brainyquote.com/quotes/harry_s_truman_109615

192 Jack A. Goldstone, Leonid Grinin, and Andrey Korotayev, ed.'s, Handbook of Revolutions in the 21st Century: The New Waves of Revolutions, and the Causes and Effects of Disruptive Political Change, (Switzerland: Springer, 2022). https://link.springer.com/book/10.1007/978-3-030-86468-2

193 For simplicity, this chapter uses the terms drone and unmanned [air, ground, or maritime] vehicle interchangeably, acknowledging but setting aside parochial debates over terminology.

194 Audrey Cronin, Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists, (New York: Oxford University Press, 2019), p. 1; James Abbot, "Best Drones 2023: Take flight with drones for beginners and experts alike," November 23, 2022, https://www.space.com/best-drones.

195 "Drone Surveillance: How Criminals Are Using Drones to Commit Crimes," n.d., https://www.911security.com/blog/drone-surveillance-how-criminals-are-using-drones-to-commit-crimes.

196 Edward Tenner, "Unintended Consequences," Ted Talks, September 6, 2011, 15:54, Edward Tenner: Unintended consequences | TED Talk..

197 Emanuel Fabian, "Gaza Terror Groups Send Fire Balloons into Israel, Sparking Four Blazes," The Times of Israel, August 6, 2021, https://www.timesofisrael.com/gaza-terror-groups-send-fire-balloons-into-israel-sparking-four-blazes/.

198 Norman Polmar, "An Early Pilotless Aircraft," Naval History Magazine, vol. 33, no. 4, (Aug 2019), https://www.usni.org/magazines/naval-history-magazine/2019/august/early-pilotless-aircraft.

199 "A Brief History of Drones," Imperial War Museum, (n.d.), https://www.iwm.org.uk/history/a-brief-history-of-drones; De Havilland Aircraft Museum, https://www.dehavillandmuseum.co.uk/aircraft/de-havilland-dh82b-queen-bee/.

200 Jack Olsen, Aphrodite: Desperate Mission, (New York: G.P. Putnam's Sons, 1970).

201 Federal Aviation Administration, https://www.faa.gov/uas/resources/timeline.

202 Federal Aviation Administration, https://www.faa.gov/sites/faa.gov/files/UAS-CTI-School-Directory-2023_February.pdf.

203 Travis Hoium, "Self-Driving Cars Are Here and the Leaders May Surprise You," The Motley Fool, September 7, 2021, https://www.fool.com/investing/2021/09/07/self-driving-cars-are-here-and-the-leaders-may-sur/.

204 "Healthcare by air: Rwanda's life-saving medical drones," The Guardian, April 20, 2022, https://www.theguardian.com/global-development/gallery/2022/apr/20/healthcare-by-air-rwandas-life-saving-medical-drones; "Drones: still an emerging technology in Africa," Military Africa, September 14, 2022, https://www.military.africa/2022/09/drones-still-an-emerging-technology-in-africa/.

205 Alyssa Sims, “The Rising Drone Threat from Terrorists,” Georgetown Journal of International Affairs, vol. 19, (Fall 2018), p. 99.

206 Christopher P. Cavas, “New Houthi Weapon Emerges: A Drone Boat,” DefenseNews, February 19, 2017, https://www. defensenews.com/digital-show-dailies/idex/2017/02/19/new-houthi-weapon-emerges-a-drone-boat/.

207 Charles R. Davis., “Ukrainian Suicide Drone Boats Packed with Bombs Mean Nowhere is Safe for Russia’s Once Feared Black Sea Fleet,” Business Insider, November 3, 2022, https://www.businessinsider.com/ukraines-drone-boats-mean-nowheres-safe-russia-black-sea-fleet-2022-11.

208 Bergen, Peter, et al. “World of Drones: Non-State Actors with Drone Capabilities,” New America, July 30, 2020, https://www.newamerica.org/international-security/reports/world-drones/non-state-actors-with-drone-capabilities/.

209 Brent Goldfarb & David A. Kirsch, Bubbles and Crashes: The Boom and Bust of Technological Innovation, (Stanford, CA: Stanford University Press, 2019).

210 T.X. Hammes, “Cheap Technology Will Challenge U.S. Tactical Dominance,” Joint Force Quarterly, no. 81, (2016), p. 79.

211 Alex Roland, “War and Technology,” Foreign Policy Research Institute, February 27, 2009, https://www.fpri.org/ article/2009/02/war-and-technology/.

212 Bernard Brodie & Fawn M. Brodie, From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare, (Bloomington, IN: Indiana University Press, 1973).

213 Brig Gen Anthony J. Trythall, from a debate General Trythall participated in concerning the legacy of Maj Gen J.F.C. Fuller, sponsored by The Royal United Services Institute, October 12, 1978. Published in The Journal of the Royal United Service Institute, vol. 124, March 1979, p 22.

214 Patrick Tucker, “Come Test Your Gear Against Russian Forces, Ukrainians Urge US Defense Firms,” Defense One, March 4, 2023, https://www.defenseone.com/technology/2023/03/come-test-your-gear-against-russian-forces-ukrainians-urge-us-defense-firms/383622/.

215 Richard D. Newton, RAF and Tribal Control: Airpower and Irregular Warfare Between the World Wars, (Lawrence, KS: University Press of Kansas, 2019), pp. 35 – 40.

216 Yoav Stern, “Report: Iran Admits Supplying Hezbollah With Eight Drones,” Haaretz, November 11, 2004, https://www.haaretz.com/2004-11-11/ty-article/report-iran-admits-supplying-hezbollah-with-eight-drones/0000017f-e2e2-d38f-a57f-e6f2e92b0000; Milton Hoenig, “Hezbollah and the Use of Drones as a Weapon of Terrorism,” Federation of American Scientists, June 5, 2014, https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism/

217 John G. Bunnell, From the Underground to the High Ground: The Insurgent Use of Airpower, Maxwell AFB, AL: USAF Air War College, February 16, 2011, pp. 13-14.

218 Kerry Chávez & Ori Swed, “Off the Shelf: The Violent Nonstate Actor Drone Threat,” Air & Space Power Journal, (Fall 2020), p. 30.

219 Country Reports on Terrorism 2018, U.S. Department of State, Bureau of Counterterrorism, October 2019, p. 210.

220 Yaron Steinbuch, “Drone sighting shuts down London’s Heathrow Airport,” New York Post, January 8, 2019, https://nypost.com/2019/01/08/drone-sighting-shuts-down-london-heathrow-airport/.

221 Country Reports on Terrorism 2018, p. 237.

222 Ben Hubbard Palko Karasz, & Stanley Reed, “Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran,” New York Times, September 14, 2019, https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html.

223 Thomas E. Lawrence, Seven Pillars of Wisdom: A Triumph, (New York: Random House, 1991, reprint of 1935 U.S. Doubleday edition), pp. 192, 337.

224 Michael Boyle, The Drone Age: How Done Technology Will Change War and Peace, (New York: Oxford University Press, 2020), p. 139; Ben Riley-Smith, “ISIL Plotting to Use Drones for Nuclear Attack on West,” The Telegraph, April 1, 2016, https://www.telegraph.co.uk/news/2016/04/01/isil-plotting-to-use-drones-for-nuclear-attack-on-west/.

225 Don Rassler, The Islamic State and Drones: Supply, Scale, and Future Threats, (West Point, NY: Combating Terrorism Center, 2018), p. 1; Sam Blum, “ISIS Technicians Work on Self-Driving Cars at Terrorism R&D Lab in Leaked Video,” Inverse, January 7, 2016, https://www.inverse.com/article/9974-isis-technicians-work-on-self-driving-cars-at-terrorism-r-d-lab-in-leaked-video.

226 David B. Larter, “SOCOM Commander: Armed ISIS Drones were 2016’s 'Most Daunting Problem',” Defense News, May 16, 2017, https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/.

227 Peter Grier, “April 15, 1953,” Air Force Magazine, June 2011, pp. 55-57.

228 Nick Waters, “The Poor Man’s Air Force? Rebel Drones Attack Russia’s Airbase in Syria,” Bellingcat, January 12, 2018, https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/.

229 Ekene Lionel, “Al Shabaab Drones, and the African Conundrum,” Military Africa, September 15, 2022, https://www.military.africa/2022/09/al-shabaab-drones-and-the-african-conundrum/; Rueben Dass, “Militants and Drones: A Trend That is Here to Stay,” RUSI, September 6, 2022, https://www.rusi.org/explore-our-research/publications/commentary/militants-and-drones-trend-here-stay/.

230 Spencer Ackerman, “Libyan Rebels Are Flying Their Own Minidrone,” Wired, August 23, 2011, https://www.wired.com/2011/08/libyan-rebels-are-flying-their-own-mini-drone/.

231 Dass, “Militants and Drones.”

232 Lawrence, Seven Pillars of Wisdom, p. 192.

233 "Pantsir S-1," Missile Threat, Center for Strategic and International Studies, July 6, 2021, https://missilethreat.csis.org/defsys/pantsir-s-1/.

234 Cronin, Power to the People, p. 6.

235 Antonio Calcara et al, “Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare,” International Security, vol. 46, no. 4, (Spring 2022), p.171.

236 Country Reports on Terrorism 2021, U.S. Department of State, Bureau of Counterterrorism, 2022, pp. 126, 136.

237 Mark Bowden, “The Tiny and Nightmarishly Efficient Future of Drone Warfare,” The Atlantic, November 22, 2022, https://www.theatlantic.com/technology/archive/2022/11/russia-ukraine-war-drones-future-of-warfare/672241/.

238 Sarah Whittaker, “Record-Breaking Intel Drone Swarm Lights Up Pyeongchang 2018,” DroneBelow, February 10, 2018, https://dronebelow.com/2018/02/10/record-breaking-intel-drone-swarm-lights-pyeongchang-olympic-winter-games-2018/.

239 “Syria: Drone Swarm Attacks Russian Military Bases,” TRIPWire, Department of Homeland Security, January 12, 2018, https://tripwire.dhs.gov/news/209478.

240 H.I. Sutton, “Why Ukraine’s Remarkable Attack on Sevastopol Will Go Down in History,” Naval News, November 17, 2020, https://www.navalnews.com/naval-news/2022/11/why-ukraines-remarkable-attack-on-sevastopol-will-go-down-in-history/.

241 Daniel Boffey, “Financial Toll on Ukraine of Downing Drones ‘Vastly Exceeds Russian Costs’,” The Guardian, October 19, 2022, https://www.theguardian.com/world/2022/oct/19/financial-toll-ukraine-downing-drones-vastly-exceeds-russia-costs.

242 Loz Blain, “You Can Now Buy a Coordinated Multi-Drone Swarm in a Box,” New Atlas, June 2, 2022, https://newatlas.com/drones/red-cat-drone-swarm-product/.

243 George Orwell, “Politics and the English Language” (1946), reprinted in George Orwell, Politics and the English Language and Other Essays (Oxford: Oxford City Press, 2009), p.12.

244 The Random House Dictionary of the English Language: The Unabridged Edition, ed. Jess Stein (New York: Random House, 1973), s.v. “warfare”; Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, JP 1 (Washington, DC: Joint Chiefs of Staff, 2013), I-4.

245 George F. Kennan, “The Inauguration of Organized Political Warfare,” April 30, 1948, reprinted in U.S. Department of State, Foreign Relations of the United States, 1945-1950, eds. C. Thomas Thorne, Jr. and David S. Patterson (Washington: U.S. Government Printing Office, 1996).

246 Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms, JP 1-01 (Washington, DC: Joint Chiefs of Staff, 2001).il

247 U.S. Department of Defense, Summary of the Irregular Warfare Annex to the National Defense Strategy (Washington D.C.: Department of Defense, 2020), p. 2 (“Irregular warfare is a struggle among state and non-state actors to influence populations and affect legitimacy. IW 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.”)

248 People’s Republic of China, Regulation on Political Work of the Chinese People’s Liberation Army, December 5, 2003, art. 14.

249 Valery Gerasimov, "The Value of Science Is in the Foresight," (February 27, 2013), reprinted in Military Review (Jan.-Feb. 2016): p. 24; Timothy Thomas, The Chekinov-Bogdanov Commentaries of 2010-2017: What Did They Teach Us About Russia's New Way of War? (McLean, VA: MITRE, 2020), pp. 6-8.

250 General Treaty for Renunciation of War as an Instrument of National Policy (Kellogg-Briand Pact), August 27, 1928, 94 L.N.T.S. 57.

251 Charter of the United Nations, October 24, 1945, 1 U.N.T.S. XVI, preamble.

252 Charter of the United Nations, October 24, 1945, 1 U.N.T.S. XVI, art. 2(4).

253 Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949, 75 U.N.T.S. 31, art. 2; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, August 12, 1949, 75 U.N.T.S. 85, art. 2; Convention Relative to the Treatment of Prisoners of War, August 12, 1949, 75 U.N.T.S. 135, art. 2; Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949, 75 U.N.T.S. 287, art. 2.

254 Rosa Brooks, How Everything Became War and the Military Became Everything (New York: Simon & Schuster, 2016), p. 35.

255 President of the United States, U.S. National Security Strategy, December 2017, p. 28.

256 President of the United States, U.S. National Security Strategy, February 2015; President of the United States, U.S. National Security Strategy, October 2022.

257 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), p. 2.

258 Jonathan G. Odom, "Understanding China's Legal Gamesmanship in the Rules-Based Global Order," in China's Global Influence: Perspective and Recommendations, eds. Scott D. McDonald and Michael C. Burgoyne (Honolulu: DKI APCSS, 2019).

259 Brian Z. Tamanaha, Law as a Means to An End (Cambridge: Cambridge University Press, 2006), p. 6.

260 Jeremy Bentham, Principles of Penal Law, in The Works of Jeremy Bentham, ed. John Bowring (Edinburgh: William Tait, 1843), p. 564.

261 Robert Keohane, "International Relations and International Law: Two Optics," 38 Harvard International Law Journal 487 (1997): pp. 489-495.

262 Timothy Meyer, "Instrumentalism," in Concepts for International Law: Contributions to Disciplinary Thought, eds. Jean d'Aspremont and Sahib Singh (Cheltenham: Edward Elgar Publishing, 2019).

263 Charles J. Dunlap, Jr., "Law and Military Interventions: Preserving Humanitarian Values in 21st [Century] Conflicts" (lecture, Kennedy School of Government, Cambridge, MA, Nov. 29, 2001).

264 Charles J. Dunlap, "Lawfare Today: A Perspective," Yale Journal of International Affairs (Winter 2008): p. 146.

265 Orde F. Kittrie, Lawfare: Law as a Weapon of War (Oxford: Oxford University Press, 2016).

266 Dong Wang, China's Unequal Treaties: Narrating National History (Plymouth, United Kingdom: Lexington Books, 2005), p. 128.

267 Qiao Liang & Wang Xiangsui, Unrestricted Warfare (Brattleboro, Vermont: Echo Point Books & Media, 1999), p. 38.

268 Qiao Liang & Wang Xiangsui, Unrestricted Warfare (Brattleboro, Vermont: Echo Point Books & Media, 1999), pp. 38-43.

269 People's Republic of China, Regulations on Political Work of the Chinese People's Liberation Army, December 5, 2003, art. 14.

270 100 Cases of Legal Warfare: The Classic Case Analysis, ed. Cong Wensheng (Beijing: People's Liberation Army Publishing House, 2004).

271 100 Cases of Legal Warfare: The Classic Case Analysis, ed. Cong Wensheng (Beijing: People's Liberation Army Publishing House, 2004).

272 Hans J. Morgenthau, Politics Among Nations: The Struggle for Power and Peace, eds. Kenneth W. Thompson and W. David Clinton, 7th ed. (Boston: McGraw Hill, 2006), pp. 186-89.

273 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), p. 1.

274 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), , pp. 2-3.

275 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), pp. 2-3.

276 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), p. 3.

277 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), p. 1.

278 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), pp. 4, 9.

279 Pelé, My Life and the Beautiful Game (Garden City: Doubleday & Company, 1977).

280 Stephen Potter, The Theory and Practice of Gamesmanship: The Art of Winning Games Without Actually Cheating (London: Rupert Hart-Davis, 1947).

281 Non-state actors having no connection to a particular nation-state (e.g., transnational criminal organizations and transnational terrorist groups) could also engage in activities that satisfy all of the elements of the definition of legal gamesmanship outlined in this chapter. But to scope this discussion, this chapter will address only legal gamesmanship in the context of conduct by nation-states.

282 Permanent Court of International Justice, The Case of the S.S. Lotus (France v. Turkish Republic), September 7, 1927, p. 18.

283 UN International Law Commission, Articles of State Responsibility for Internationally Wrongful Acts, Nov. 2001, art. 2, commentary para. 5.

284 UN International Law Commission, Articles of State Responsibility for Internationally Wrongful Acts, Nov. 2001, art. 4.; UN International Law Commission, Articles of State Responsibility for Internationally Wrongful Acts, Nov. 2001, art. 5.; UN International Law Commission, Articles of State Responsibility for Internationally Wrongful Acts, Nov. 2001, art. 8.

285 Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, JP 1 (Washington, DC: Joint Chiefs of Staff, March 25, 2013, incorporating Change 1, July 12, 2017), I-7, to I-8.

286 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), p. 2.

287 Joint Chiefs of Staff, Competition Continuum, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), p. 2.

288 UN International Law Commission, Articles of State Responsibility for Internationally Wrongful Acts, art. 1.

289 Jonathan G. Odom, "Guerrillas in the Sea Mist: China's Maritime Militia and International Law," 3 Asia-Pacific Journal of Ocean Law and Policy (2018) p. 31.

290 Conor M. Kennedy & Andrew S. Erickson, "China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA," China Maritime Report 1, no. 1 (2017); Gregory B. Poling, Tabitha Grace Mallory & Harrison Pretat, Pulling Back the Curtain on China's Maritime Militia (Washington: Center for Strategic & International Studies, 2021).

291 Andrew S. Erickson & Conor M. Kennedy, China's Maritime Militia (Washington: Center for Naval Analyses, 2016); Gregory B. Poling, Tabitha Grace Mallory &Harrison Pretat, Pulling Back the Curtain on China's Maritime Militia (Washington: Center for Strategic & International Studies, 2021).

292 Charter of the United Nations, October 24, 1945, 1 U.N.T.S. XVI, art. 27.

293 UN Security Council, S/PV.6143, 6143rd meeting, June 15, 2009; UN Security Council, S/PV.8979, 8979th meeting, February 25, 2022.

294 David E. Sanger, "U.S. Says Russia Sent Saboteurs Into Ukraine to Create Pretext for Invasion," New York Times, January 14, 2022.

295 James A. Green, Christian Henderson &Tom Ruys, "Russia's Attack on Ukraine and the Jus Ad Bellum," Journal on the Use of Force and International Law (2022), pp. 5-13.

296 Peter Dickinson, "Russian Passports: Putin's Secret Weapon in the War Against Ukraine," UkraineAlert, Atlantic Council, April 13, 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/russian-passports-putins-secret-weapon-in-the-war-against-ukraine/.

297 Vladimir Putin, address by the President of the Russian Federation, February 24, 2022.

298 United Nations Convention on the Law of the Sea (UNCLOS), December 10, 1982, 1833 U.N.T.S. 397, arts. 19(1), 21 (1), 24(1), 41(1), 69(1), 70(1), 73(1), 240(d), 254(3), 256, and 257.

299 U.S. Department of Defense, Maritime Claims Reference Manual, available at https://www.jag.navy.mil/organization/code_10_mcrm.htm.

300 Charter of the United Nations, October 24, 1945, 1 U.N.T.S. XVI, art. 51; UN International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, art. 22.; Geneva Convention Relative to the Protection of Civilian Persons in Time of War: Commentary, ed. Jean S. Pictet (Geneva: International Committee of the Red Cross, 1958), p. 227.

301 Jacob T. Rob and Jacob N. Shapiro, "A Brief History of Online Influence Operations," Lawfare, (blog), October 28, 2021, https://www.lawfareblog.com/brief-history-online-influence-operations.

302 Christopher Paul et al., The Role of Information in U.S. Concepts for Strategic Competition (Santa Monica: RAND Corporation, 2022).

303 Michael J. McNerney et al., National Will to Fight: Why Some States Keep Fighting and Others Don't (Santa Monica: RAND Corporation, 2018).

304 Daniel Arnaudo et al., Combating Information Manipulation: A Playbook for Elections and Beyond, (National Democratic Institute, International Republican Institute, Stanford Internet Observatory Cyber Policy Center, September 2021); Shanthi Kalathil, "The Evolution of Authoritarian Digital Influence: Grappling with the New Normal," PRISM 9, no. 1 (October 2020): 33-50.

305 Christopher Paul and Miriam Matthews, The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It (Santa Monica: RAND Corporation, 2016).

306 Stephen G. Harkins and Richard E. Petty, "The Multiple Source Effect in Persuasion: The Effects of Distraction," Personality and Social Psychology Bulletin 7, no. 4 (1981): 627-635; Andrew J. Flanagin and Miriam J. Metzger, "Trusting Expert- Versus User-Generated Ratings Online: The Role of Information Volume, Valence, and Consumer Characteristics," Computers in Human Behavior 29 (2013): 1626-1634.

307 Teresa Garcia-Marques and Diane M. Mackie, "The Feeling of Familiarity as a Regulator of Persuasive Processing," Social Cognition 19, no. 1 (2001): 9-34; Stephan Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," Psychological Science in the Public Interest 13, no. 3 (2012): 106-131; Richard E. Petty et al, "To Think or Not To Think: Exploring Two Routes to Persuasion," in T.C. Brock and M.C. Green, eds., Persuasion: Psychological Insights and Perspectives, 2nd ed. (Thousand Oaks: Sage Publications, 2005), 81-116.

308 Lewandowsky, et al., "Misinformation and Its Correction,".

309 Petty, et al., "To Think or Not To Think,".

310 Lewandowsky, et al., "Misinformation and Its Correction,".

311 Paul and Matthews, The Russian "Firehose of Falsehood"; Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russia and Chinese Models," Democracy & Disorder, (Brookings Institute, August 2019).

312 Polyakova and Meserole, "Exporting Digital Authoritarianism,".

313 WeChat is a Chinese instant messaging, social media, and mobile payment platform, while Vkontakte is a Russian-language social media platform popular in Russia, Belarus, Ukraine and other countries in Eastern Europe.

314 Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," Connections: The Quarterly Journal 15, no. 1 (2016): 5-31.

315 Both journalists and news are in quotes to note that propaganda programming is a perversion of the notion of news, and the reporters and anchors working for these stations are not really journalists in most senses of the word.

316 Accounts that once belonged to a real person appear to have greater authenticity and can be more convincing to audiences.

317 Jessica Dawson, "Microtargeting as Information Warfare," The Cyber Defense Review 6, no. 1 (Winter 2021): 63 – 79; Samantha Bradshaw, et al., Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, (Oxford: The computational Propaganda Project at the Oxford Internet Institute, 2021).

318 Miriam Matthews et al., Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe (Santa Monica: RAND Corporation, 2021).; Daniel Arnaudo, et al, Combating Information Manipulation: A Playbook for Elections and Beyond (National Democratic Institute, International Republican Institute, Stanford Internet Observatory Cyber Policy Center, September 2021).

319 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," Journal of Slavic Military Studies 17, no. 2 (2004).

320 Matthews et al., Understanding and Defending.

321 Peter Pomerantsev, “Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare,” Atlantic, (September 9, 2014); Matthew Armstrong, “Russia’s War on Information,” War on the Rocks, (December 15, 2014).

322 Paul and Matthews, The Russian “Firehose of Falsehood”.

323 Ben Nimmo, Anatomy of Info-War: How Russia’s Propaganda Machine Works, and How to Counter It, Central European Strategy Council, undated.

324 Both RT and Sputnik are much closer to a blend of infotainment and disinformation than to fact-checked journalism, though their formats do indeed intentionally take the appearance of news programs.

325 Adrian Chen, “The Agency,” New York Times Magazine, June 2, 2015; Peter Pomerantsev and Michael Weiss, The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money (New York: The Institute of Modern Russia, 2014).

326 Peter Pomerantsev and Michael Weiss, The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money, (New York: A Special Report presented by The Interpreter, a project of the Institute of Modern Russia, 2014).

327 Pomerantsev and Weiss, How the Kremlin Weaponizes Information.

328 Dmitry Volchek and Daisy Sindelar, “One Professional Russian Troll Tells All,” Radio Free Europe/Radio Liberty (March 25, 2015).

329 Christopher Paul et al., Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case Studies (Santa Monica: RAND Corporation, 2018).

330 Bilyana Lily, Russian Information Warfare: Assault on Democracies in the Cyber Wild West, (Newport, RI: Naval Institute Press, 2022)

331 Paul et al., Case Studies.

332 Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, Chinese Disinformation Efforts on Social Media (Santa Monica: RAND Corporation, 2021).

333 Christopher Paul et al., A Guide to Extreme Competition with China (Santa Monica: RAND Corporation, 2021).

334 Yasuyuki, Sugiura, NIDS China Security Report 2022: The PLA’s Pursuit of Enhanced Joint Operations Capabilities, (Toyoko: National Institute for Defense Studies, 2021).

335 Paul, Mozur, Raymond Zhong and Aaron Krolik, “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags,” New York Times, March 1, 2020.

336 Megan Robertson, “China’s Social Credit System: Speculation vs. Reality,” The Diplomat, March 30, 2021.

337 While initially suspected to be paid proxies or independent contractors posting content favorable to the CCP, research shows that these individuals are more likely to be regular government employees. See, Harry Farrell, “The Chinese Government Fakes Nearly 450 Million Social Media Comments A Year”, The Washington Post, May 16, 2016.

338 Italy Haiminis, “Iran’s Information Warfare,” The Cognitive Campaign: Strategic and Intelligence Perspectives no. 4 (October 2019): 135 – 147.

339 Ariane M. Tabatabai, “A Brief History of Iranian Fake News,” Foreign Affairs, (August 24, 2018).

340 Abbas Al Lawati and Nadeen Ebrahim, “The Battle of Narratives on Iran Is Being Fought on Social Media,” CNN, October 5, 2022

341 Haiminis, “Iran’s Information Warfare 135 – 147.

342 Haiminis, “Iran’s Information Warfare135 – 147.

343 Allan Hassaniyan, “How Longstanding Iranian Disinformation Tactics Target Protests,” Fikra Forum, (November 2022).

344 Office of the Director of National Intelligence, Annual Threat Assessment of the US Intelligence Community, (Washington, D.C., April 2021).

345 Sonja Swanbeck, “How to Understand Iranian Information Operations,” Lawfare, (February 2021).

346 Ben Caspit, “How Iran interferes in Israel’s Election Campaign,” Al-Monitor, (March 18, 2019).

347 Laura Courchesne, et al., “Review of Social Science Research on The Impact of Countermeasures Against Influence Operations,” Harvard Kennedy School Misinformation Review 2, no. 5 (September, 2021).

348 “Summary of the Irregular Warfare Annex to the National Defense Strategy” (United States Department of Defense, 2020).

349 Kevin Bilms, “What’s in a Name? Reimagining Irregular Warfare Activities for Competition,” War on the Rocks, January 15, 2021, https://warontherocks.com/2021/01/whats-in-a-name-reimagining-irregular-warfare-activities-for-competition/.

350 Graham T. Allison, “Destined for War?,” The National Interest, no. 149 (2017): 9–21; Juan Carlos Zarate, Treasury’s War: The Unleashing of a New Era of Financial Warfare, First edition. (New York: PublicAffairs, 2013); Nicholas A. Lambert, Planning Armageddon: British Economic Warfare and the First World War (Cambridge, Mass.: Harvard University Press, 2012); Richard Dunley, “Rebuilding the Mills of Sea Power: Interwar British Planning for Economic Warfare against Japan,” International History Review, 2021, 1–17, https://doi.org/10.1080/07075332.2021.1989704; Edward S. Miller, Bankrupting the Enemy: The U.S. Financial Siege of Japan Before Pearl Harbor, 1st edition (Annapolis, Md: Naval Institute Press, 2007).

351 Zarate, Treasury’s War; MIAN AHAD HAYAUD-DIN, “THE HAWALLAH NETWORK: CULTURE AND ECONOMIC DEVELOPMENT IN AFGHANISTAN,” International Social Science Review 78, no. 1/2 (2003): 21–30; “When History Rhymes,” IMF, November 5, 2018, https://www.imf.org/en/Blogs/Articles/2018/11/05/blog-when-history-rhymes.

352 “习近平接见2017年度驻外使节工作会议与会使节并发表重要讲话-新华网,” 2017 CCP Diplomatic Envoy Working Conference, 2017, http://www.xinhuanet.com/politics/leaders/2017-12/28/c_1122181743.htm; Jinping Xi, “习近平：顺应时代潮流 实现共同发展--新闻报道-中国共产党新闻网 Xi Jinping: Follow the Trend of the Times and Achieve Common Development,” 2018, http://cpc.people.com.cn/n1/2018/0726/c64094-30170246.html; Daniel Tobin, “How Xi Jinping’s ‘New Era’ Should Have Ended U.S. Debate on Beijing’s Ambitions,” accessed January 17, 2023, https://www.csis.org/analysis/how-xi-jinpings-new-era-should-have-ended-us-debate-beijings-ambitions; Liza Tobin, “China’s Brute Force Economics: Waking Up from the Dream of a Level Playing Field,” Texas National Security Review, 2022, https://tnsr.org/2022/12/chinas-brute-force-economics-waking-up-from-the-dream-of-a-level-playing-field/.

353 Xi Jinping, “Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for The Great Success of Socialism with Chinese Characteristics for a New Era(I),” Beijing Review 60, no. 46 (2017)：后插1-后插9, https://doi.org/10.3969/j.issn.1000-9140.2017.46.017.

354 Administration of Donald John Trump, “Statement on the 2017 National Security Strategy,” 2017; David H. McCormick, “Economic Might, National Security, and the Future of American Statecraft,” Texas National Security Review, May 6, 2020, https://tnsr.org/2020/05/economic-might-national-security-future-american-statecraft/.

355 Michael Beckley, Unrivaled: Why America Will Remain the World’s Sole Superpower, Cornell Studies in Security Affairs (Ithaca, Baltimore, Md.: Cornell University Press, Project MUSE, 2018); John J. Mearsheimer, The Tragedy of Great Power Politics, Updated edition., The Norton Series in World Politics (New York: WWNorton & Company, 2014); Joseph S. Nye, The Future of Power, 1st ed. (New York: PublicAffairs, 2011); James Sullivan, “The Nature of Power: A Metcalfe’s Law National Security Strategy,” Security Nexus, Perspectives, 23, no. 2022 (2022), https://apcss.org/nexus_articles/the-nature-of-power-a-metcalfes-law-national-security-strategy/; Rosella Cappella Zielinski, “Paying the Defense Bill: Financing American and Chinese Geostrategic Competition,” Texas National Security Review, April 4, 2023, https://tnsr.org/2023/04/paying-the-defense-bill-financing-american-and-chinese-geostrategic-competition/.

356 Giacomo Magistretti and Marco Tabellini, “Economic Integration and the Transmission of Democracy,” Working Paper, Working Paper Series (National Bureau of Economic Research, May 2022), https://doi.org/10.3386/w30055.

357 Wag the Dog (S.l.]: New Line Home Video, 1998); GD HESS and A. ORPHANIDES, “War Politics: An Economic, Rational-Voter Framework,” The American Economic Review 85, no. 4 (1995): 828–46.

358 Heike Holbig and Bruce Gilley, “Reclaiming Legitimacy in China,” Politics & Policy 38, no. 3 (2010): 395–422, https://doi.org/10.1111/j.1747-1346.2010.00241.x; Alastair Iain Johnston, “Is Chinese Nationalism Rising? Evidence from Beijing,” International Security 41, no. 3 (January 1, 2017): 7–43, https://doi.org/10.1162/ISEC_a_00265.

359 Jennifer Mitzen, “Ontological Security in World Politics: State Identity and the Security Dilemma,” European Journal of International Relations 12, no. 3 (September 1, 2006): 341–70, https://doi.org/10.1177/1354066106067346; Jennifer Mitzen and Kyle Larson, “Ontological Security and Foreign Policy,” Oxford Research Encyclopedia of Politics, August 22, 2017, https://doi.org/10.1093/acrefore/9780190228637.013.458.

360 William A. Callahan, “National Insecurities: Humiliation, Salvation, and Chinese Nationalism,” Alternatives 29, no. 2 (March 1, 2004): 199–218, https://doi.org/10.1177/030437540402900204; Alanna Krolikowski, “State

Personhood in Ontological Security Theories of International Relations and Chinese Nationalism: A Sceptical View," The Chinese Journal of International Politics 2, no. 1 (2008): 109–33; for more on the interlinkage between populism and economic growth please see James Sullivan and Rajiv Batra, "Politics by Numbers: Quantifying Populism" (J.P. Morgan, August 15, 2020).

361 Robert Higgs, "How U.S. Economic Warfare Provoked Japan's Attack on Pearl Harbor | Robert Higgs," The Independent Institute, accessed February 22, 2023, https://www.independent.org/news/article.asp?id=1930; Greg Kennedy, "Maritime Power and Economic Warfare in the Far East, 1937–1941," in Economic Warfare and the Sea (Liverpool University Press, 2020), https://doi.org/10.3828/liverpool/9781789621594.003.0012.

362 Nicholas Mulder, "Opinion | Sanctions Against Russia Not Slowing War Effort - The New York Times," New York Times, February 9, 2023, https://www.nytimes.com/2023/02/09/opinion/sanctions-russia-ukraine-economy.html; Agathe Demarais, "The End of the Age of Sanctions?," Foreign Affairs, December 27, 2022, https://www.foreignaffairs.com/united-states/end-age-sanctions.

363 "The Treasury 2021 Sanctions Review" (Washington, D.C.: United States Department of the Treasury, 2021).

364 Incremental sanctions tools include to include arms embargoes, foreign assistance reductions and cut offs, export and import limitations, asset freezes, revocation of Most Favored Nation (MFN) status, negative votes in international financial institutions, withdrawal of diplomatic relations, visa denials, cancellation of air links, prohibitions on credit, financing and investment, please see Richard N. Haass, "Economic Sanctions: Too Much of a Bad Thing," Brookings (blog), June 1, 1998, https://www.brookings.edu/research/economic-sanctions-too-much-of-a-bad-thing/.

365 Zarate, Treasury's War.

366 Nicholas Mulder, "The Sanctions Weapon," IMF, June 2022, https://www.imf.org/en/Publications/fandd/issues/2022/06/the-sanctions-weapon-mulder.

367 Mulder.

368 Vladimir Milov, "Yes, It Hurts: Measuring the Effects of Western Sanctions Against Russia," GLOBSEC - A Global Think Tank: Ideas Shaping the World, July 21, 2022, https://www.globsec.org/what-we-do/press-releases/yes-it-hurts-measuring-effects-western-sanctions-against-russia.

369 "Are Sanctions on Russia Working?," The Economist, accessed February 21, 2023, https://www.economist.com/leaders/2022/08/25/are-sanctions-working?gclid=EAIaIQobChMIi7j697ml_QIVj6uWCh2mpAGDEAAYASAAEgIhFvD_BwE&gclsrc=aw.ds.

370 Wally Adeyemo, "America's New Sanctions Strategy," Foreign Affairs, December 16, 2022, https://www.foreignaffairs.com/russian-federation/americas-new-sanctions-strategy.

371 William Howey, "Russia Can Count on Support from Many Developing Countries," Economist Intelligence Unit, March 30, 2022, https://www.eiu.com/n/russia-can-count-on-support-from-many-developing-countries/.

372 "The Inner Workings of Rostec, Russia's Military-Industrial Behemoth | Wilson Center," accessed May 3, 2023, https://www.wilsoncenter.org/blog-post/the-inner-workings-rostec-russias-military-industrial-behemoth.

373 Haass, "Economic Sanctions."

374 Zarate, Treasury's War.

375 The cyber-economy is defined as a network of economic activity linked by information technology. Cybersecurity is a critical enabler of this economic activity, and a key focus of defensive economic warfare tactics. Please see Vladimir M. Filippov et al., eds., The Cyber Economy: Opportunities and Challenges for Artificial Intelligence in the Digital Workplace, Contributions to Economics (Cham: Springer International Publishing, 2019), https://doi.org/10.1007/978-3-030-31566-5; "Prosper in the Cyber Economy," IBM, November 14, 2022, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy.

376 For a full list of the evolving sanctions please see "Sanctions against Russia – a Timeline," accessed February 21, 2023, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/sanctions-against-russia-8211-a-timeline-69602559.

377 Boris Grozovski, "Why Western Sanctions against Russia Work, and How to Make Them Work Better | Wilson Center," The Russia File / Kennan Institute (blog), June 27, 2022, https://www.wilsoncenter.org/blog-post/why-western-sanctions-against-russia-work-and-how-make-them-work-better.

378 Nicholas Mulder, "Opinion | Sanctions Against Russia Not Slowing War Effort - The New York Times," New York Times, February 9, 2023, https://www.nytimes.com/2023/02/09/opinion/sanctions-russia-ukraine-economy.html; "Russian Oil Is Getting Mixed in Singapore and Then Re-Exported, Sources Say," Bloomberg.Com, January 19, 2023, https://www.bloomberg.com/news/articles/2023-01-19/singapore-oil-tanks-snapped-up-as-russian-inflows-boost-profits.

379 Anders Aslund and Maria Snegovaya, “Report: The Impact of Western Sanctions on Russia and How They Can Be Made Even More Effective,” Atlantic Council (blog), May 3, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-impact-of-western-sanctions-on-russia/.

380 “How many Russian soldiers have died in Ukraine? - The Economist,” accessed February 27, 2024, https://www.economist.com/graphic-detail/2024/02/24/how-many-russian-soldiers-have-died-in-ukraine.

381 Frédéric Bastiat, “That Which Is Seen and That Which Is Not Seen | Frédéric Bastiat,” May 29, 2015, https://fee.org/resources/that-which-is-seen-and-that-which-is-not-seen/.

382 Nicholas Mulder, “Opinion | Sanctions Against Russia Ignore the Economic Challenges Facing Ukraine,” The New York Times, February 9, 2023, sec. Opinion, https://www.nytimes.com/2023/02/09/opinion/sanctions-russia-ukraine-economy.html.

383 “Bp Statistical Review of World Energy 2021: A Dramatic Impact on Energy Markets,” Plus Company Updates, 2021.

384 Richie Ruchuan Ma, Tao Xiong, and Yukun Bao, “The Russia-Saudi Arabia Oil Price War during the COVID-19 Pandemic,” Energy Economics 102 (October 1, 2021): 105517, https://doi.org/10.1016/j.eneco.2021.105517; Dermot Gately, “Lessons from the 1986 Oil Price Collapse,” Brookings (blog), June 1, 1986, https://www.brookings.edu/bpea-articles/lessons-from-the-1986-oil-price-collapse/.

385 “JPMorgan Sees Oil at $380 on Worst-Case Cut by Russia - Bloomberg,” accessed May 5, 2023, https://www.bloomberg.com/news/articles/2022-07-01/jpmorgan-sees-stratospheric-380-oil-on-worst-case-russian-cut.

386 Columbia | CGEP, “Q&A | Exit or Stay? The Decisions of International Oil Companies Involved in Russia After Its Invasion of Ukraine,” Center on Global Energy Policy at Columbia University | SIPA, April 20, 2022, https://www.energypolicy.columbia.edu/publications/qa-exit-or-stay-decisions-international-oil-companies-involved-russia-after-its-invasion-ukraine/.

387 “Russian Oil Price Cap, a Pointless Gesture - The Economic Times,” accessed February 24, 2023, https://economictimes.indiatimes.com/opinion/et-editorial/russian-oil-price-cap-a-pointless-gesture/articleshow/96010712.cms?from=mdr.

388 Elliot Smith, “Sanctions on Russian Oil Are Having the ‘intended Effect,’ IEA Says,” CNBC, February 16, 2023, https://www.cnbc.com/2023/02/16/sanctions-on-russian-oil-are-having-the-intended-effect-iea-says.html.

389 “Halliburton, Schlumberger Draw Back from Russia amid U.S. Energy Sanctions | Reuters,” accessed February 24, 2023, https://www.reuters.com/business/energy/halliburton-suspends-future-business-russia-2022-03-18/.

390 Jackie Northam, “Russia’s Oil Drilling Plans May Be in Jeopardy without the West’s Support,” NPR, April 15, 2022, sec. World, https://www.npr.org/2022/04/15/1093121762/russias-oil-drilling-plans-may-be-in-jeopardy-without-the-wests-support.

391 “Halliburton, Schlumberger Draw Back from Russia amid U.S. Energy Sanctions | Reuters.”

392 John A. [D-KY-3 Rep. Yarmuth, “H.R.5376 - 117th Congress (2021-2022): Inflation Reduction Act of 2022,” legislation, August 16, 2022, 08/16/2022, http://www.congress.gov/; Parsley Ong et al., “Asia Energy & EV Battery: Deep Dive on US Inflation Reduction Act, and Our Stock Picks; Prefer LGC/LGES/SK” (J.P. Morgan, 2022).

393 Volodymyr Zelenskyy: Diia app is the first step towards building a state-service" Official website of the President of Ukraine. Retrieved 2021-03-31.

394 Dmitry Ovcharenko, “Why Ukraine is a great fit for international tech companies.” 21 April 2020. https://alcor-bpo.com/your-own-rd-office-news/.

395 Akshaya Asokan• April 20 and 2023, “Cyber Experts Predict More Harmful Cyberattacks in Ukraine,” accessed May 10, 2023, https://www.bankinfosecurity.com/cyber-experts-predict-more-harmful-cyberattacks-in-ukraine-a-21726.

396 DHS Cyber and Infrastructure Security Agency (CISA) warns Russia’s invasion of Ukraine could impact organizations both within and beyond the region, to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners. They provide on-going information at https://www.cisa.gov/shields-up/.

397 Keith Alexander, “Cyber Warfare in Ukraine Poses a Threat to the Global System,” Financial Times, February 15, 2022; Paul R. Kolbe, Maria Robson Morrow, and Lauren Zabierek, “The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict,” Harvard Business Review, February 18, 2022, https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict.

398 Patrick Howell O’Neill, “Russia hacked an American satellite company one hour before the Ukraine invasion.” MIT Technology Review, 10 May 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion

399 Microsoft "Defending Ukraine: Early Lessons from the Cyber War." June 22, 2022.

400 Todd Bishop, "Microsoft's president on turbulent times for the company, country, and world," GeekWire, 30 June 2022, https://www.geekwire.com/2022/interview-microsofts-president-on-turbulent-times-for-the-company-country-and-world/.

401 Alissa Starzak, "The latest on attacks, traffic patterns and cyber protection in Ukraine"

https://blog.cloudflare.com/ukraine-update/, last accessed 25 Feb 2023.

402 According to the Russian government-backed attackers ramped up cyber operations beginning in 2021 during the run up to the invasion. In 2022, Russia increased targeting of users in Ukraine by 250 percent compared to 2020. Targeting of users in NATO countries increased over 300 percent in the same period from https://twitter.com/dsszzi, last accessed 25 Feb 2023.

403 Greg Rattray, Geoff Brown, Robert Taj Moore, "The Cyber Defense Assistance Imperative: Lessons from Ukraine," Aspen Digital Group of the Aspen Institute, February 2023.

404 eschroeder, "A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment," Atlantic Council (blog), February 27, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.

405 The National Council for the Recovery of Ukraine from the Consequences of the War, "Draft Ukraine Recovery Plan Materials of the "Digitalization" working group," from https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/eng/digitization-eng.pdf, last accessed 25 Feb 2023.

406 James Timbie, "A Large Number of Small Things: A Porcupine Strategy for Taiwan," Texas National Security Review, December 7, 2021, https://tnsr.org/2021/12/a-large-number-of-small-things-a-porcupine-strategy-for-taiwan/.

407 Cleveland, Charles T., and Daniel Egel. 2020. "The American Way of Irregular War: An Analytical Memoir | RAND." RAND Corporation. https://www.rand.org/pubs/perspectives/PEA301-1.html. This title in part is a nod to the seminal work, The American Way of Irregular War An Analytical Memoir, by Charles T. Cleveland and Daniel Egel.

408 Fox, Amos C. 2019. "In Pursuit of a General Theory of Proxy Warfare." Association of the United States Army. https://www.ausa.org/file/44775/download?token=bIb3jp3c., Cleveland, Charles T., Daniel Egel, David Maxwell, and Hy Rothstein. 2023. "The Need for Irregular Warfare Professional Military Education." RAND Corporation. https://www.rand.org/blog/2023/02/preparing-for-strategic-competition-the-need-for-irregular.html.

409 Fox 2019.

410 Fox 2019. Derived from: "…a significant problem for the U.S. military, and more importantly, the U.S. Army, is that it refuses to speak openly or clearly about proxy environments and proxy warfare. Instead, it chooses to hoodwink its practitioners through complex language. Terms and phrases such as security force assistance, training and advising, partnered force and by, with and through are all misleading and meant to soften or hide the coarseness of proxy warfare. This practice—speaking through euphemism—high-lights the problem that arises when the manner in which we must operate does not mirror the method or narrative in which we want to operate. A doctrine built around misleading or obfuscated outward intentions does little to nothing to help the Soldiers, staffs and leaders who find themselves in proxy situations"

411 Constitutional Congress. 1788. "The Constitution of the United States: A Transcription." National Archives |. https://www.archives.gov/founding-docs/constitution-transcript.

412 Cambridge Dictionary. 2023. "PROXY | definition in the Cambridge English Dictionary." Cambridge Dictionary. https://dictionary.cambridge.org/us/dictionary/english/proxy.

413 Cambridge Dictionary. n.d. "PROXY WAR | definition in the Cambridge English Dictionary." Cambridge Dictionary. Accessed February 11, 2023. https://dictionary.cambridge.org/us/dictionary/english/proxy-war.

414 Luttwak, Edward N. 1979. Coup D'etat: A Practical Handbook. Cambridge, Massachusetts: Harvard University Press. 24 - 27. Seven different types of illegal government overthrow: Revolution, Civil War, Pronunciamiento, Putsch, Liberation, War of National Liberation, and Coup d'etat The Director of Strategic Services. 1944. Special Operations Field Manual - Strategic Services (Provisional) Strategic Services Field Manual No. 4. Reprint 2023 ed. Washington, DC: Office of Strategic Services. 4, 10, & 14,Cline, Ray S. 1976. Secrets Spies and Scholars: Blueprint of the Essential CIA. Washington, DC: Acropolis Books Ltd. 129-131, 180-181, Clausewitz, Carl v. 1976. On war. Edited by Michael Howard, Bernard Brodie, and Peter Paret. Translated by Peter Paret and Michael Howard. Princeton, New Jersey: Princeton University Press. 479-483

415 Tommy

416 Lewis, Goncharov and Xue 1993

417 Pillsbury 2015. Aldrich, Rawnsley and Rawnsley 2000.

418 Berlinger, Joshua. 2017. “Kim Jong Nam death: What we've learned so far.” CNN. https://www.cnn.com/2017/02/20/asia/kim-jong-nam-death-timeline/index.html.

419 US National Security Council. 2017. “Trump National Security Strategy.” Trump White House Archive. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, US National Security Council. 2022. “Biden National Security Strategy.” The White House. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

420 Azizi, Arash. 2020. The Shadow Commander: Soleimani, the US, and Iran's Global Ambitions. Amazon: Oneworld Publications.

421 Ibid.

422 Ibid.

423 Ibid Michael Knights, Hamid Malik, Aymenn Jawad al Tamimi. “Honored, Not Contained: The Future of Iraq’s Popular Mobilization Forces.” Washington: The Washington Institute for Near East Policy, 2023.

424 Ibid.

425 US National Security Council 2022. US National Security Council 2017. Cleveland and Egel, The American Way of Irregular War: An Analytical Memoir | RAND 2020.

426 Golkar, Saeid. 2015. Captive Society: The Basij Militia and Social Control in Iran. New York City, New York: Woodrow Wilson Center Press / Columbia University Press. Marr, Phebe. 2004. The Modern History Of Iraq. Boulder, Colorado: Avalon Publishing.

427 Zubok, Vladislav M., Vladislav Zubok, and Konstantin Pleshakov. 1996. Inside the Kremlin's cold war : from Stalin to Khrushchev. Paperback ed. Cambridge, Massachusetts: Harvard University Press. 140-142, 146-147.

428 Eidenmuller 2021.

429 Rid, Thomas. 2021. Active Measures: The Secret History of Disinformation and Political Warfare. New York, New York: Picador. 323. Lewis, Goncharov and Xue 1993. Romerstein and Evans 2012. .E. N. Luttwak, Coup D'etat: A Practical Handbook 1979.

430 Zubok, Zubok and Pleshakov 1996

431 Andrew S. Bowen 2023. Marten 2020.

432 Pillsbury 2015, E. N. Luttwak, The Rise of China Vs. the Logic of Strategy 2012

433 Gershaneck 2020.

434 Xiangsui and Liang 2015.

435 Tzu 1963, 66

436 Chang, Jung, Rong Zhang, and Jon Halliday. 2005. Mao: The Unknown Story. New York, New York: Knopf. 445, (Albania), 461-463 (Indochina Viet Minh, Algerian rebels, Albania, Cuba’s Che, Venezuelan leftists, 371 (Pol Pot), Xue, Litai, John W. Lewis, and Sergeĭ N. Goncharov. 1993. Uncertain Partners: Stalin, Mao, and the Korean War. Stanford, California: Stanford University Press. 108

437 Pillsbury 2015. Gershaneck 2020.

438 E. N. Luttwak, The Rise of China Vs. the Logic of Strategy 2012.

439 Xiangsui and Liang 2015. Pillsbury 2015.

440 Xiangsui, Wang, and Qiao Liang. 2015. Unrestricted Warfare. Brattleboro, Vermont: Echo Point Books & Media, LLC. xix-xxii, 4-5, 7-10.

441 Gershaneck 2020.

442 Tzu, Sun. 1963. The Art of War. Translated by Samuel B. Griffith. Paperback 1971 ed. New York, New York: Oxford University Press.

443 Xiangsui and Liang 2015. Yu 1996. E. Luttwak 2009. Pillsbury 2015.

444 “China's Overseas United Front Work.” 2018. U.S.-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf. Pillsbury 2015.

445 Xiangsui and Liang 2015, 175-177, 189-19. E. N. Luttwak, The Rise of China Vs. the Logic of Strategy 2012. Luttwak describes this as the three phases of Barbarian Handeling.

446 Drew 1994, 97

447 Rosenau, William, and Zach Gold. 2019. “The Future of Conflict is Proxy Warfare, Again.” Defense One. https://www.defenseone.com/ideas/2019/07/future-conflict-proxy-warfare-again/158697/. , (Fox 2019), Rosenau, William, and Zack Gold. 2019. ““The Cheapest Insurance in the World”? The United States and Proxy Warfare.” CNA.org. https://www.cna.org/reports/2019/07/proxy-warfare. CNA Study found 7 Key themes in case analysis of U.S. use of Proxy Warfare: 1. Proxy forces have helped the United States achieve at least some of its objectives. But the proxies themselves only sometimes achieve their goals. 2. Proxy warfare reduces, but does not eliminate, a US footprint. For example, proxies tend to rely heavily on American airpower. 3. Proxies are most effective when used to fight irregular wars. 4. “Secret” wars do not stay secret for long. Large-scale US support tends to become public knowledge. 5. Proxy warfare is transactional, and relationships with surrogates should not be viewed as permanent. 6. Proxy legitimacy matters. Surrogates that are seen as mere pawns or mercenaries perform less effectively. 7. Proxies are likely to commit human rights abuses, such as deliberately targeting civilians.

448 Murray, Heather. 2021. “Transactional Analysis - Eric Berne.” Simply Psychology. http://www.simplypsychology.org/transactional-analysis-eric-berne.html.

449 (US National Security Council 2017), (US National Security Council 2022), Wilson, Woodrow. 1918. “President Woodrow Wilson's 14 Points (1918) | National Archives.” National Archives |. https://www.archives.gov/milestone-documents/president-woodrow-wilsons-14-points

450 Kretchik, Walter E. 2011. U.S. Army Doctrine: From the American Revolution to the War on Terror. Lawrence, Kansas: University Press of Kansas. 81, (Luttwak 2009, 85), McClintock, Michael. 1992. Instruments of statecraft: U.S. guerrilla warfare, counterinsurgency, and counter-terrorism, 1940-1990. New York, New York: Pantheon Books. 15, 112, 123, 351, 353, & 455.

451 Bibb 2019. Civil reconnaissance is one of the methods by which Civil Affairs personnel collect relevant civil data as specified by the information-collection requirements formulated by their chain of command. Although doctrine allocates this function to Civil Affairs forces, the capabilities and traditional competencies of a reconnaissance formation place them in a unique position to contribute civil information about the state of host-nation (HN) transportation infrastructure, and therefore enhance the commander’s understanding of the operational environment.

452 Fox 2019

453 Deep, Alex, and Yelena Biberman. 2021. “The Proxy Gambit - Modern War Institute.” Modern War Institute -. https://mwi.usma.edu/the-proxy-gambit/., (Fox 2019)

454 Fox 2019.

455 Jensen, Michael C., and William H. Meckling. 2009. The Economic Nature of the Firm: A Reader. Edited by Louis Putterman and Randall S. Kroszner. 3rd ed. Cambridge, Massachusetts: Cambridge University Press. 315 - 335. “The principal and agent theory emerged in the 1970s from the combined disciplines of economics and institutional theory. There is some contention as to who originated the theory, with theorists Stephen Ross and Barry Mitnick both claiming authorship.[14] Ross is said to have originally described the dilemma in terms of a person choosing a flavor of ice-cream for someone whose tastes he does not know (Ibid). The most cited reference to the theory, however, comes from Michael C. Jensen and William Meckling. The theory has come to extend well beyond economics or institutional studies to all contexts of information asymmetry, uncertainty and risk.”

456 Gallimore, Derek. 2022. Inside Outsourcing: How Remote Work, Offshoring & Global Employment is Changing the World. Orlando, Florida: Amazon Digital Services LLC - Kdp. 1-13.

457 Dunigan, Molly, Sarah K. Cotton, and Ulrich Petersohn. 2013. “A Lesson from Iraq War: How to Outsource War to Private Contractors.” RAND Corporation. https://www.rand.org/blog/2013/03/a-lesson-from-iraq-war-how-to-outsource-war-to-private.html.

458 Singer, Peter W. 2005. “Outsourcing War.” Brookings. https://www.brookings.edu/articles/outsourcing-war/.

459 McFate, Sean. 2019. The New Rules of War: Victory in the Age of Durable Disorder. New York, New York: HarperCollins. 1-25., (Dunigan, Cotton, and Petersohn 2013)

460 Burlingame, EM, Paul Meyer, Jake Smith, Jay Lajoie, Diane Taylor, Lori Butierries, and E. M. Burlingame. 2020. “Unconventional Warfare, Venture Capital Style • The Havok Journal.” The Havok Journal. https://havokjournal.com/culture/military/unconventional-warfare-venture-capital-style/.

461 Tim Butcher, The Trigger: Hunting the Assassin Who Brought the World to War, (New York: Grove Atlantic, 2014).

462 Leon Trotsky’s defense of terrorism by the Soviet Union is a rare exception, but he was justifying the Soviet government’s use of terror against its own citizens rather than terrorist attacks outside the USSR. Leon Trotsky, Terrorism and Communism - A Reply to Karl Kautsky, (Ann Arbor, MI: University of Michigan Press, 1961).

463 Hossein Amir-Abdollahian, Foreign Minister of Iran, "'Terrorist' designation for Iran's IRGC would harm EU security: Iran's Islamic Revolutionary Guard Corps is a leading counterterror force and essential to Europe's security interests in the Middle East," Al Jazeera, 23 Jan 2023. https://www.aljazeera.com/opinions/2023/1/23/348

464 Web page: U.S. Naval War College, Center on Irregular Warfare and Armed Groups. https://usnwc.edu/Research-and-Wargaming/Research-Centers/Center-on-Irregular-Warfare-and-Armed-Groups

465 The term "state sponsored terrorism" exists because "terrorism" is otherwise assumed to be conducted by non-state actors acting independent of states.

466 Joe Biden, National Security Strategy, October 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf and Donald Trump, National Security Strategy of the United States of America, December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

467 Justin Hustwitt, "Letter dated 13 February 2023 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council," United Nations Security Council Analytical Support and Sanctions Monitoring Team, 13 February 2023. https://www.ecoi.net/en/file/local/2087006/N2303891.pdf

468 Edward Wong, "Biden Puts Defense of Democracy at Center of Agenda," New York Times, Sept. 6, 2022. https://www.nytimes.com/2022/09/06/us/politics/biden-democracy-threat.html

469 Alexander Hamer, "13 Vendémiaire: the day that made Napoleon," Real History, Date: January 13, 2020. https://realhistory.co/2020/01/13/napoleon-bonaparte-13-vendemiaire/

470 Lorraine Boissoneault, "The True Story of the Reichstag Fire and the Nazi Rise to Power," Smithsonian Magazine, February 21, 2017. https://www.smithsonianmag.com/history/true-story-reichstag-fire-and-nazis-rise-power-180962240/

471 Greg Myre, "Russia's wars in Chechnya offer a grim warning of what could be in Ukraine," NPR, March 12, 2022. https://www.npr.org/2022/03/12/1085861999/russias-wars-in-chechnya-offer-a-grim-warning-of-what-could-be-in-ukraine

472 Staff, "Egypt state of emergency lifted after 31 years," BBC News, 1 June 2012. https://www.bbc.com/news/world-middle-east-18283635

473 Daniel Byman, "Will Afghanistan Become a Terrorist Safe Haven Again?" Foreign Affairs, August 18, 2021.

474 Charles H. Briscoe, Richard L. Kiper, James A. Schroder, and Kalev I. Sepp, Weapon of Choice: U.S. Army Special Operations Forces in Afghanistan, (Fort Leavenworth, Kansas: Combat Studies Institute Press, 2003).

475 https://www.washingtoninstitute.org/policy-analysis/foreign-irregulars-iraq-next-jihad

476 Mary Anne Weaver, "The Short, Violent Life of Abu Musab al-Zarqawi," The Atlantic, July/August 2006.

477 Richard Shultz, Military Innovation in War: It Takes a Learning Organization - A Case Study of Task Force 714 in Iraq, (MacDill AFB, FL: Joint Special Operations University Press, 2016).

478 William A. Knowlton, Jr., The Surge: General Petraeus and the Turnaround in Iraq, (Washington, D.C.: National Defense University Press, 2010). https://ndupress.ndu.edu/Publications/Article/718062/the-surge-general-petraeus-and-the-turnaround-in-iraq/

479 "Timeline: the Rise, Spread, and Fall of the Islamic State," The Wilson Center, October 28, 2019. https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state

480 Official website of the Global Coalition against Daesh https://theglobalcoalition.org/en/

481 https://en.wikipedia.org/wiki/Battle_of_Mosul_(2016%E2%80%932017) and https://en.wikipedia.org/wiki/Battle_of_Mosul_(2016%E2%80%932017)

482 Cedric Barnes & Harun Hassan (2007) "The Rise and Fall of Mogadishu's Islamic Courts," Journal of Eastern African Studies, 1:2, 151-160, DOI: 10.1080/17531050701452382. https://doi.org/10.1080/17531050701452382

483 Grégory Chauzal and Thibault van Damme, The Roots of Mali's Conflict, CRU Report March 2015, Netherlands Institute of International Relations Clingendael. https://www.clingendael.org/pub/2015/the_roots_of_malis_conflict/3_a_playing_field_for_foreign_powers/

484 Jim Garamone, "U.S. Drone Strike Kills al-Qaida Leader in Kabul," DOD News, Aug. 2, 2022. https://www.defense.gov/News/News-Stories/Article/Article/3114362/us-drone-strike-kills-al-qaida-leader-in-kabul/

485 Natasha Bertrand, Oren Liebermann, Zachary Cohen and Ellie Kaufman, "US nearing a formal agreement to use Pakistan's airspace to carry out military operations in Afghanistan," CNN, October 23, 2021. https://www.cnn.com/2021/10/22/politics/us-pakistan-afghanistan-airspace/index.html

486 Niha Dagia, "Will Imran Khan Grant the US Access to Pakistani Airspace Again? Should the prime minister do so, he would be contradicting his years-long anti-war, anti-U.S. political rhetoric," The Diplomat, November 09, 2021. https://thediplomat.com/2021/11/will-imran-khan-grant-the-us-access-to-pakistani-airspace-again/

487 Special Inspector General for Afghanistan Reconstruction, Quarterly Report to the United States Congress, January 30, 2023. https://www.sigar.mil/pdf/quarterlyreports/2023-01-30qr.pdf

488 Catrina Doxsee, Jared Thompson, and Grace Hwang, "Examining Extremism: Islamic State Khorasan Province (ISKP)," Center for Strategic and International Studies, September 8, 2021. https://www.csis.org/blogs/examining-extremism/examining-extremism-islamic-state-khorasan-province-iskp

489 Joseph Biden, "Remarks by President Biden on the End of the War in Afghanistan," The White House: Briefing Room: Speeches and Remarks, August 31, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/

490 Australian Government, "Terrorism will remain a critical global threat," 2017 Foreign Policy White Paper, 2017. https://www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/foreign-policy-white-paper/chapter-two-contested-world/terrorism-will-remain-critical-global-threat.html

491 James Doubek, "50 years ago, the Munich Olympics massacre changed how we think about terrorism," NPR, September 4, 2022. https://www.npr.org/2022/09/04/1116641214/munich-olympics-massacre-hostage-terrorism-israel-germany

492 IDF Editorial Team, "Operation Entebbe", Wars and Operations, Israeli Defense Forces (IDF) web site. https://www.idf.il/en/mini-sites/wars-and-operations/operation-entebbe/

493 Wilson Center, "ISIS Leader Killed in U.S. Raid in Syria," February 4, 2022. https://www.wilsoncenter.org/microsite/8/node/109340

494 James Bennet, "U.S. Cruise Missiles Strike Sudan and Afghan Targets Tied to Terrorist Network," New York Times, August 21, 1998. https://archive.nytimes.com/www.nytimes.com/library/world/africa/082198attack-us.html and History.com, "Osama bin Laden killed by U.S. forces," This Day in History, May 02, 2011. https://www.history.com/this-day-in-history/osama-bin-laden-killed-by-u-s-forces

495 Idrees Ali, "U.S. special forces rescue American held in Nigeria," Reuters, October 31, 2020. https://www.reuters.com/article/us-usa-nigeria-military/u-s-special-forces-rescue-american-held-in-nigeria-officials-idUSKBN27G0JI

496 Arshad Mehmood, "10 Years After US Forces Killed Osama Bin Laden, Pakistan's Anger Has Not Abated," themedialine, 05/01/2021. https://themedialine.org/top-stories/10-years-after-us-forces-killed-osama-bin-laden-pakistans-anger-has-not-abated/

497 Megan Brenan, "A Look Back at Reaction to Bin Laden's Death," Gallup Blog, April 29, 2021. https://news.gallup.com/opinion/gallup/348971/look-back-reaction-bin-laden-death.aspx

498 Nussaibah Younis, "Achieving a Durable Peace by Reforming Post-ISIS Justice Mechanisms in Iraq," Religion, Violence, and the State in Iraq, (Washington, D.C.: Project On Middle East Political Science Studies, 2019). https://pomeps.org/achieving-a-durable-peace-by-reforming-post-isis-justice-mechanisms-in-iraq

499 ACLU, "ACLU Says That Patriot Act Has Been Misused, Extent Unknown Because of Government Stonewalling," PRESS RELEASES, June 7, 2004. https://www.aclu.org/press-releases/aclu-says-patriot-act-has-been-misused-extent-unknown-because-government-stonewalling

500 Jonathan Masters, "Guantanamo Bay: Twenty Years of Counterterrorism and Controversy," Council on Foreign Relations, September 9, 2022. https://www.cfr.org/article/guantanamo-bay-twenty-years-counterterrorism-and-controversy

501 Timothy H. Edgar, "Memorandum To Congress On President Bush's Order Establishing Military Tribunals," ACLU, November 29, 2001. https://www.aclu.org/other/memorandum-congress-president-bushs-order-establishing-military-tribunals

502 Jessica D. Lewis, Al-Qaeda in Iraq Resurgent, (Washington, D.C.: Institute for the Study of War, 2013). https://docs.house.gov/meetings/FA/FA18/20131212/101591/HHRG-113-FA18-Wstate-LewisJ-20131212.pdf

503 Heba Malik, "ISIS is defeated. What becomes of the 'Cubs of the Caliphate' in Iraq?" MENASource, Atlantic Council, August 19, 2021. https://www.atlanticcouncil.org/blogs/menasource/isis-is-defeated-what-becomes-of-the-cubs-of-the-caliphate-in-iraq/

504 U.S. Central Command, “Statement regarding Syrian Democratic Forces security operation in al-Hol camp,” U.S. Central Command Communication Integration, September 18, 2022. https://www.centcom.mil/MEDIA/STATEMENTS/Statements-View/Article/3161976/statement-regarding-syrian-democratic-forces-security-operation-in-al-hol-camp/

505 Marc R. DeVore, “Exploring the Iran-Hezbollah Relationship,” Perspectives on Terrorism, Vol. 6, No. 4/5, October 2012. https://www.jstor.org/stable/26296878?seq=10

506 U.S. House of Representatives Committee on Foreign Affairs, “Attacking Hezbollah's Financial Network: Policy Options,” One Hundred Fifteenth Congress, First Session, June 8, 2017. https://www.govinfo.gov/content/pkg/CHRG-115hhrg25730/html/CHRG-115hhrg25730.htm

507 Marc R. DeVore, “Exploring the Iran-Hezbollah Relationship,” Perspectives on Terrorism, Vol. 6, No. 4/5, October 2012. https://www.jstor.org/stable/26296878?seq=10

508 Tricia Bacon, “Deadly Cooperation: The Shifting Ties Between al-Qaeda and the Taliban,” War on the Rocks, September 11, 2018. https://warontherocks.com/2018/09/deadly-cooperation-the-shifting-ties-between-al-qaeda-and-the-taliban/n

509 Ijaz Ahmad Khan, “Understanding Pakistan's Pro-Taliban Afghan Policy,” Pakistan Horizon, Vol. 60, No. 2, April 2007. https://www.jstor.org/stable/41500068

510 Staff, “Mullah Omar: Taliban leader 'died in Pakistan in 2013',” BBC News, 29 July 2015. https://www.bbc.com/news/world-asia-33703097

511 Syed Ali Raza, Muhammad Iqbal Chawla, Amjad Abbas Magsi, Abdul Basit Mujahid, Farzana Arshad, and Nasir Khan, War on Terror and its Impacts on Pakistani Society, Journal of Pakistan Vision Vol. 20 No. 2, 2019. http://pu.edu.pk/images/journal/studies/PDF-FILES/29_v20_2_19.pdf

512 Editorial Board, “Pakistan is the Real Victim of Bush's great 9/11 folly,” Dawn, October 10, 2011. https://www.dawn.com/news/665318/pakistan-is-real-victim-of-bushs-great-911-folly

513 Justin Hustwitt, “Letter dated 13 February 2023 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da’esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council,” United Nations Security Council Analytical Support and Sanctions Monitoring Team, 13 February 2023. https://www.ecoi.net/en/file/local/2087006/N2303891.pdf

514 Asfandyar Mir and Colin P. Clarke, “Making Sense of Iran and al-Qaeda’s Relationship,” Lawfare, March 21, 2021. https://www.lawfareblog.com/making-sense-iran-and-al-qaedas-relationship

515 John Psaropoulos, “Europe awakens to the threat of sabotage by Russian agents: Attacks on critical infrastructure from France to Denmark bear the hallmark of Russian operatives, experts say,” Al Jazeera, 17 Jan 2023. https://www.aljazeera.com/news/2023/1/17/europe-awakens-to-the-threat-of-sabotage-by-russian-agents

516 Catrina Doxsee and Jared Thompson, “Massacres, Executions, and Falsified Graves: The Wagner Group’s Mounting Humanitarian Cost in Mali,” Center for Strategic and International Studies, May 11, 2022. https://www.csis.org/analysis/massacres-executions-and-falsified-graves-wagner-groups-mounting-humanitarian-cost-mali

517 Dr Satya Shrestha-Schipper, Convenor and Marloes Rozing, “Conference: Maoist Insurgency in Asia and Latin America: Comparative Perspectives,” International Institute of Asian Studies, February 2006. https://www.iias.asia/event/maoist-insurgency-asia-latin-america-comparative-perspectives

518 United States Mission to the United Nations, “FACT SHEET: U.S. Introduces Commonsense Resolution to Extend Arms Embargo on World’s Leading State Sponsor of Terrorism,” 13 August, 2020. https://usun.usmission.gov/fact-sheet-u-s-introduces-commonsense-resolution-to-extend-arms-embargo-on-worlds-leading-state-sponsor-of-terrorism/

519 Nathan Brown, “U.S. Counterterrorism Policy and Hezbollah’s Resiliency,” Georgetown Security Studies Review Vol. 1 Issue 3 December 2013. https://georgetownsecuritystudiesreview.org/2013/12/10/u-s-counterterrorism-policy-and-hezbollahs-resiliency/

520 Ethan Bronner, “How Israel and Iran Attack Each Other While Avoiding All-Out War,” Washington Post, January 30, 2023. https://www.washingtonpost.com/business/how-israel-and-iran-attack-each-other-while-avoiding-all-out-war/2023/01/30/1bb33a56-a0ca-11ed-8b47-9863fda8e494_story.html

521 Daniel L. Byman, “Hezbollah’s Dilemmas,” Brookings Policy Brief, November 2022. https://www.brookings.edu/wp-content/uploads/2022/11/FP_20221110_hezbollah_dilemmas_byman.pdf

522 United States House of Representatives, “Hezbollah’s Growing Threat Against U.S. National Security Interests in the Middle East,” Hearing Before the Subcommittee on the Middle East and North Africa of the Committee On Foreign Affairs, One Hundred Fourteenth Congress, Second Session, March 22, 2016. https://www.govinfo.gov/content/pkg/CHRG-114hhrg99555/html/CHRG-114hhrg99555.htm

523 In the twentieth century, the Communist International (Comintern) was supposed to serve this function for communist revolutionaries, but it was tightly controlled by the USSR and served instead as a vehicle for traditional state sponsorship by the USSR.

524 Linda Robinson, "The SOF Experience in the Philippines and the Implications for Future Defense Strategy," PRISM, Volume 6, No 3 Dec. 7, 2016. https://cco.ndu.edu/News/Article/1020239/the-sof-experience-in-the-philippines-and-the-implications-for-future-defense-s/

525 Colonel Edwin Amadar, Philippine Marine Corps, and Major Bobby Tuttle, US Army Special Forces, "The Rise of ISIS in the Philippines and the Battle of Marawi," CTX, Volume 9, No. 2, 2019. https://nps.edu/documents/110773463/120088589/CTX+Vol+9+No+2+WEB+FINAL-2.pdf/ad18a518-59b1-b7dc-d2cb-a1a4b3c545f2?t=1589823012894

526 Amos Yadlin and Udi Eventual, "Why Israel Slept," Foreign Affairs, November 21, 2023. https://www.foreignaffairs.com/israel/why-israel-slept-yadlin-eventual

527 Guy Davies and Patrick Reevell, "ANALYSIS: Is Israel winning the war against Hamas?" abcNEWS, January 31, 2024. https://abcnews.go.com/International/analysis-is-israel-winning-war-hamas/story?id=106795525

528 Daniel Byman, "Can the Palestinian Authority Govern Gaza?" Foreign Affairs, January 4, 2024. https://www.foreignaffairs.com/israel/can-palestinian-authority-govern-gaza

529 Tom Soufi Burridge, Angus Hines, Nicky deBlois, Anna Burd, Latifeh Abdellatif, Desiree Adib, and Nasser Atta, "Who is Yahya Sinwar, Israel's most-wanted Hamas terrorist," abcNews, December 22, 2023. https://abcnews.go.com/International/yahya-sinwar-hamas-wanted-terrorist/story?id=105834815 and Al Jazeera Staff, "Hamas says it has enough Israeli captives to free all Palestinian prisoners," Al Jazeera, 7 Oct 2023. https://www.aljazeera.com/news/2023/10/7/hamas-says-it-has-enough-israeli-captives-to-free-all-palestinian-prisoners

530 Erik Skare, "Iran, Hamas, and Islamic Jihad: A marriage of convenience," European Council on Foreign Relations, 18 December 2023. https://ecfr.eu/article/iran-hamas-and-islamic-jihad-a-marriage-of-convenience/

531 Dr. Mohamed ELDoh, "Iran: The Real Beneficiary of The Gaza Conflict," Geopolitical Monitor, December 13, 2023. https://www.geopoliticalmonitor.com/iran-the-real-beneficiary-of-the-gaza-conflict/

532 Office of Director of National Intelligence, "ISIS-Sinai," Counter Terrorism Guide: Foreign Terrorist Organizations, August 2022. https://www.dni.gov/nctc/ftos/isis_sinai_fto.html

533 U.S. DoD, Annual Report to Congress on Military and Security Developments Involving PRC (Washington, DC: OSD, 2018), p. 72, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF. DIA, China Military Power, Modernizing Force to Fight and Win (Washington, DC: ODNI, 2019), p. 79, https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf.

534 Derek Grossman and Logan Ma, "Short History of CMM and What It May Tell Us," RAND Corporation, 6 Apr 2020, https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html.

535 Priscilla Tacujan, "Chinese Lawfare in SCS," Journal of Political Risk, Vol. 10, No. 7, Jul 2022, https://www.jpolrisk.com/chinese-lawfare-in-the-south-china-sea-a-threat-to-global-interdependence-and-regional-stability/

536 DIA, p. 79.

537 Gregory Poling, Tabitha Grace Mallory, and Harrison Pretat, "Pulling Back Curtain on CMM," CSIS, Nov 2021, p. vii, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211118_Poling_Maritime_Militia.pdf?Y5iaJ4NT8eITSlAKTr.TWxtDHuLIq7wR.

538 Conor Kennedy and Andrew Erickson, "China's Third Sea Force, PAFMM: Tethered to PLA," USNWC, Mar 2017, p. 2, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1000&context=cmsi-maritime-reports.

539 CRS, U.S.-China Strategic Competition in SCS/ECS (Washington, DC: U.S. Congress, 26 Jan 2022), p. 15, https://crsreports.congress.gov/product/pdf/R/R42784/.

540 Shuxian Luo and Jonathan Panter, "CMM and Fishing Fleets, Primer for Operational Staffs and Tactical Leaders," Military Review, Jan-Feb 2021, p. 7, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Panter-Maritime-Militia-1.pdf.

541 James Kraska and Michael Monti, "Law of Naval Warfare and CMM," USNWC, 2015, p. 451, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1406&context=ils.

542 "Paquete Habana, 175 U.S. 677 (1900)," Justia U.S. Supreme Court, https://supreme.justia.com/cases/federal/us/175/677/.

543 Kraska and Monti, p. 458-465.

544 Hu Bo, “CMM in SCS – Myths and Realities,” Nanyang Technological University (Singapore), 30 May 2022, https://www.rsis.edu.sg/rsis-publication/idss/ip22032-chinas-maritime-militia-in-the-south-china-sea-myths-and-realities/#.Y74s3HbMLIV.

545 U.S. DoD, p. 72. DIA, p. 79.

546 Grossman and Ma.

547 Ibid. Robert Herrick, Soviet Naval Strategy: Fifty Years of Theory and Practice, Annapolis, MD: U.S. Naval Institute (USNI), 1968, p. 9, 21-22.

548 Bernard Cole, "History of Twenty-First-Century Chinese Navy," Naval War College Review: Vol. 67, No. 3 , Article 5, 2014, p. 13-14, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1292&context=nwc-review.

549 Huang Youyi, “Context, Not History, Matters for Deng’s Famous Phrase,” Global Times, 15 Jun 2011, https://www.globaltimes.cn/content/661734.shtml. “Backgrounder: Xi Jinping Thought on Socialism with Chinese Characteristics for New Era,” Xinhua, 17 Mar 2019, http://www.xinhuanet.com/english/2018-03/17/c_137046261.htm. “Chinese Dream,” China Daily, 2023, http://www.chinadaily.com.cn/china/Chinese-dream.html.

550 U.S. DoD, Military and Security Developments Involving PRC (Washington, DC: OSD, 2022), p. 50, https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

551 **Andrew Erickson, “CCG: Organization, Forces, and Yellow Sea Applications,” in Andrew Erickson, ed.,** *Maritime Gray Zone Operations: Challenges and Countermeasures in Indo-Pacific* **(**New York, NY: Routledge Cass Series: Naval Policy & History**, 2022), p. 54–76.** DIA, p. 78.

552 Food and Agriculture of United Nations (UN), “State of World Fisheries and Aquaculture 2022,” UN, 2022, https://www.fao.org/3/cc0461en/online/sofia/2022/fishing-fleet.html#:~:text=SOURCE%3A%20FAO.,the%20world's%20largest%20fishing%20fleet.

553 Luo and Panter, p. 15, 21. DIA, p. 79.

554 Grossman and Ma. Poling, Mallory, and Pretat, p. vii, 3-8.

555 “Statement of Government of PRC on China's Territorial Sovereignty and Maritime Rights and Interests in SCS,” PRC Ministry of Foreign Affairs, 12 Jul 2016, https://www.fmprc.gov.cn/nanhai/eng/snhwtlcwj_1/201607/t20160712_8527297.htm.

556 Grossman and Ma. Poling, Mallory, and Pretat, p. 4.

557 Grossman and Ma. Poling, Mallory, and Pretat, p. vii, 3-8. Andrew Erickson and Conor Kennedy, “CMM,” Center for Naval Analyses, Feb 2016, p. 2-3, https://www.cna.org/archive/CNA_Files/pdf/chinas-maritime-militia.pdf. “Philippines Tells China to Back Off After SCS Standoff,” Reuters, 17 Nov 2021, https://www.reuters.com/world/china/philippines-condemns-chinese-coast-guards-action-south-china-sea-2021-11-18/. Frances Mangosing, “China Testing Philippine Resolve to Keep Ayungin Shoal,” Philippine Daily Inquirer, 13 Jun 2022, https://newsinfo.inquirer.net/1609831/china-testing-ph-resolve-to-keep-ayungin-shoal. Shannon Tiezzi, “Vietnam to China: Move Your Oil Rig out of SCS,” Diplomat, 9 Apr 2016, https://thediplomat.com/2016/04/vietnam-to-china-move-your-oil-rig-out-of-the-south-china-sea/. Khanh Vu, “Chinese Ship Leaves Vietnam’s Waters After Disputed SCS Survey,” Reuters, 23 Oct 2019, https://www.reuters.com/article/us-vietnam-southchinasea/chinese-ship-leaves-vietnams-waters-after-disputed-south-china-sea-surveys-idUSKBN1X30EK. Ben Werner, “Maritime Standoff Between China and Malaysia Winding Down,” USNI, 13 May 2020, https://news.usni.org/2020/05/13/maritime-standoff-between-china-and-malaysia-winding-down. Sebastian Strangio, “China Demanded Halt to Indonesian Drilling Near Natuna Islands,” Diplomat, 2 Dec 2021, https://thediplomat.com/2021/12/china-demanded-halt-to-indonesian-drilling-near-natuna-islands-report/.

558 Grossman and Ma. Poling, Mallory, and Pretat, p. vii, 3-8.

559 Poling, Mallory, and Pretat, p. 7.

560 “Counter-coercion Series–Scarborough Shoal Standoff,” AMTI, 22 May 2017, https://amti.csis.org/counter-co-scarborough-standoff/.

561 CRS, China Primer: SCS Disputes (Washington, DC: U.S. Congress, 19 Dec 2022), p. 1-2, https://crsreports.congress.gov/product/pdf/IF/IF10607.

562 “Ebb and Flow of Beijing SCS’s Militia,” AMTI, 9 Nov 2022, https://amti.csis.org/the-ebb-and-flow-of-beijings-south-china-sea-militia/.

563 Poling, Mallory, and Pretat, p. vii, 3-9.

564 Erickson and Kennedy, p. 1.

565 Erickson and Kennedy, p. 4-5.

566 Erickson and Kennedy, p. 5-6. U.S. DoD, Annual Report to Congress on Military and Security Developments Involving PRC, p. 72. DIA, p. 79.

567 Erickson and Kennedy, p. 8. Kennedy and Erickson, p. 6. See Figure 1 for graphical depiction of CMM organization.

568 Erickson and Kennedy, p. 10-11.

569 Kraska and Monti, p. 452-453.

570 Kraska and Monti, p. 465-466.

571 Steve Sacks, "Using 1202 Authorities to Counter CMM," War on the Rocks, 24 Mar 2023, https://warontherocks.com/2023/03/using-1202-authorities-to-counter-chinas-maritime-militia/.

572 Grossman and Ma.

573 Hu Bo.

574 The views expressed here are entirely those of the author and do not necessarily reflect the views, policy or position of the United States Government, Department of Defense, United States Army Special Operations Command, or the National Defense University.

575 Sandor Fabian and Gabrielle Kennedy, The Conceptualization of Irregular Warfare in Europe (Washington, DC: Irregular Warfare Center, 2023).

576 Source.

577 Martijn Kitzen, "Operations in Irregular Warfare," in Anders Sookermany, ed., Handbook of Military Sciences (Cham: Springer International Publishing, 2020), pp. 1-21.

578 James D. Kiras, "Irregular Warfare," in David Jordan, James Kiras, et al, eds., Understanding Modern Warfare (Cambridge: Cambridge University Press, 2008), Chapter 5.

579 For an excellent review of the evolution of U.S. IW definitions and activities, see Jared Tracy, "From 'irregular warfare' to Irregular Warfare: History of a Term," Veritas, Vol. 19, No. 1 (2023), 29-34.

580 Fabian and Kennedy, p. 6.

581 Ibid.

582 Interview with the LTC Stephan Bolton, U.S. Army Special Operations Command, Fort Leavenworth, KS, April 28, 2023.

583 Aleksandr Kolpakidi and Vladimir Sever, Spetsnaz GRU (Moscow: Yauza and Eksmo, 2008). See also, Vladimir Kvachkov, Spetsnaz Rossii (Moscow: Voennaya Literatura, 2004).

584 Valeriy Gerasimov, "Tsennost' nauki v predvidenii," Voyenno Promyshlennyy Kuryer (February 26, 2013), http://vpk-news.ru/articles/14632. (2013); See also Charles Bartles, "Russia's Indirect and Asymmetric Methods as a Response to the New Western Way of War," Special Operations Journal, Vol. 2, No. 1 (2016).

585 Ivanov, Vladimir, "SShA delaiut stavku na neregulyarnye voiny," Nezavisimoe voennoe obozrenie (Oct. 15, 2020). https://nvo.ng.ru/realty/2020-10-15/8_1113_pentagon.html. Accessed 30 April 2023.

586 Interview with the LTC Stephan Bolton, U.S. Army Special Operations Command, Fort Leavenworth, KS, April 28, 2023.

587 Lester Grau and Charles Bartles, The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), 231.

588 Elisabeth Edwards, "Spetsnaz: How Russia's Special Forces Became So Deadly," War History Online (July 19, 2022). Available at: https://www.warhistoryonline.com/featured/russian-spetsnaz.html?safari=1. Accessed April 29, 2023.

589 John Dziak, "The Soviet Approach to Special Operations," in Special Operations in US Strategy, Frank Barnett, B. Hugh Tovar, and Richard Schultz, eds. (Washington, DC: National Defense University Press, 1984), 100.

590 Mark Galeotti, Spetsnaz: Russia's Special Forces (New York: Osprey, 2015), 7.

591 Dziak, 98.

592 Adam Ulam, The Bolsheviks (New York: Collier, 1968).

593 Dziak, 98.

594 Grau and Bartles, 232.

595 Dziak, 103.

596 Steven Zaloga, Inside the Blue Berets: A Combat History of Soviet and Russian Airborne Forces, 1930-1995 (Novato, CA: Presidio, 1995), 204-205.

597 John Collins, Green Berets, SEALs & Spetsnaz: U.S. & Soviet Special Military Operations (Washington, DC: Pergamon-Brassey's, 1987), 1.

598 Active measures and disinformation were actions of political warfare that were conducted by the Soviet security services (Cheka, OGPU, NKVD, KGB) during the Cold War to influence the course of world events, in addition to collecting intelligence and producing "politically correct" assessment of it. Active measures ranged "from media manipulations to special actions involving various degrees of violence." They were used both abroad and domestically, and included disinformation, propaganda, counterfeiting official documents, assassinations, and political repression. See Richard Shultz and Roy Godson, Dezinformatsia: Active Measures in Soviet Strategy (Washington, DC: Pergamon-Brassey's, 1984). See also Oleg Gordievsky and Christopher Andrew, KGB: The Inside Story (London: Hodder & Stoughton, 1990).

599 Director of Central Intelligence, Soviet Support for International Terrorism and Revolutionary Violence: Special National Intelligence Estimate (Langley: Central Intelligence Agency, 1981).

600 Grau and Bartles, 231.

601 Collins, 4.

602 Galeotti, 2015, 21-22.

603 Ibid.

604 Tony Balasevicius, Squandering the Capability: Soviet Special Operations Forces in Afghanistan (Ottawa: Canadian Defence Academy Press, 2011).

605 Ibid.

606 Anatol Lieven, Chechnya: Tombstone of Russian Power (New Haven, CT: Yale University Press, 1998).

607 See Christopher Marsh, "The Desecularization of Conflict: The Role of Religion in Russia's Confrontation with Chechnya, 1785-present," Review of Faith and International Affairs, Vol. 14, No. 1 (2016), 66-79. See also Robert Schaefer, The Insurgency in Chechnya and the North Caucasus: From Gazavat to Jihad (Santa Barbara, CA: Praeger, 2011).

608 U.S. Army Special Operations Command, "Little Green Men": A Primer on Modern Unconventional Warfare, Ukraine, 2013-2014 (Fort Bragg: U.S. Army Special Operations Command, 2016).

609 Aleksandr Kolpakidi and Vladimir Sever, Spetsnaz GRU (Moscow: Yauza and Eksmo, 2008).

610 Nikolai Protopopov, "Rebyata iz 'Al'fy': Kak rabotaet elitnyi spetsnaz FSB Rossii," RIA Novosti (July 29, 2019). https://ria.ru/20190729/1556911713.html. Accessed April 30, 2023.

611 Vladimir Sedov, "Samoe Sekretnoe nodrazdelenie strany: 40 let nazad v SSSR sozdalu unikal'nyi spetsnaz. Lenta.ru (19 August 2021), https://turbo.lenta.ru/articles/2021/08/19/vympel/. Accessed April 30, 2023.

612 Ibid.

613 Ibid.

614 Grau and Bartles, 232.

615 Interfax Online, 6 March 2013. As quoted in Lester Grau and Charles Bartles, The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), 234.

616 Dmitry Trenin, "Russia's New Tip of the Spear," Foreign Policy (May 8, 2013). Available at: http://www.foreignpolicy.com/articles/2013/05/08/russia_new_special_ops_command_afghanistan, accessed 8 August 2016.

617 "Shoigu sozdaet otvergnutye Serdyukovym sily spetsoperatsii, otstav of SShA na 26 let," Newsru.com (March 6, 2013). Available at: http://www.newsru.com/russia/06mar2013/minob.html

618 Grau and Bartles (2016). See also R. McDermott (2012). The Reform of Russia's Conventional Armed Forces: Problems, Challenges, & Policy Implications. Washington, DC: Jamestown Foundation.

619 For a more detailed analysis of Russia's special operations units, see Christopher Marsh, Developments in Russian Special Operations: Russia's Spetsnaz, SOF and Special Operations Forces Command (Kingston, ON: Canadian Special Operations Forces Command, 2017).

620 Roger McDermott, "Putin's Secret Force Multiplier: Special Operations Forces," Eurasian Daily Monitor, Vol. 13, No. 81, (26 April 2016). https://jamestown.org/program/putins-secret-force-multiplier-special-operations-forces/. Accessed 13 April 2023.

621 Aleksey Mikhailov, “Boitsy Chetvertogo Izmereniya,” Voyenno Promyshlennyy Kuryer. (20 April 2016). http://www.vpk-news.ru/articles/30319. Accessed 10 October 2017.

622 Alexey Nikolsky, “Little, Green and Polite: The Creation of Russian Special Operations Forces,” in Brothers Armed: Military Aspects of the Crisis in Ukraine, Colby Howard and Ruslan Pukhov, eds. (Minneapolis: East View Press, 2015).

623 Mikhailov, 2016.

624 Ibid.

625 Grau and Bartles, 236.

626 Aleksey Mikhailov, “General Staff asks Shoigu to Create ‘Commandos’,” Izvestiya Online, 27 November 2012. Cited in Grau and Bartles, 235.

627 Alexsey Nikolsky, “Russian Special Operations Forces – Eight Years and Three Wars,” in Ruslan Pukhov and Christopher Marsh, eds., Elite Warriors: Special Operations Forces from Around the World (Minneapolis: East View, 2017).

628 Ibid.

629 Aleksey Nikolsky, “Russian ‘Spetsnaz’ Forces – From Saboteurs to Court Bailiffs,” Moscow Defense Brief, Vol. 40, No. 2 (2014). Available at: http://mdb.cast.ru/mdb/1-2014/item4/article2/, accessed 6 August 2016.

630 Ministerstvo Oborony Rossiiskoi Federatsii, Formy primeneniya Vooruzhyonnykh sil Rossiiskoi Federatsii (Moscow: Ministerstvo Oborony Rossiiskoi Federatsii, n.d.). Available at: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14014

631 Alexander Sladkov, “Novyi Rossiiskii Spetsnaz dlya zagranitsy,” Television Channel “Rossiya 24”, program “Vesti Nedeli,” (28 April 2013).

632 Nikolsky, 2015, 126-127.

633 Viktor Stepankov, Bitva za “Nord-Ost” (Moscow: Yaza, 2003).

634 See, for example, Timothy Phillips, Beslan: The Tragedy of School No. 1 (London: Granta, 2014).

635 Graham Turbiville, Russian Special Forces: Issues of Loyalty, Corruption, and the Fight against Terror (Hurlburt Field, FL: JSOU Press, 2005).

636 Nikolsky, 2015, 131.

637 U.S. Army Special Operations Command (2016). “Little Green Men”: A Primer on Modern Unconventional Warfare, Ukraine, 2013-2014. Fort Bragg, NC: U.S. Army Special Operations Command.

638 Nikolsky, 2015.

639 Anton Lavrov, “Civil War in the East: How the Conflict Unfolded Before Minsk,” in Howard and Pukhov, 2015), 204-205.

640 Ibid.

641 Intergovernmental Panel on Climate Change, IPCC Sixth Assessment Report: Summary for Policymakers (Geneva: IPCC, 2022), p. 9, https://www.ipcc.ch/report/ar6/wg2/downloads/report/IPCC_AR6_WGII_SummaryForPolicymakers.pdf.

642 Ibid, p. 8.

643 Al Gore, “Statement from Former Vice President Al Gore on the IPCC Report—Climate Change 2021: The Physical Science Basis,” AlGore.com, August 9, 2021, https://algore.com/news/statement-from-former-vice-president-al-gore-on-the-ipcc-report-climate-change-2021-the-physical-science-basis.

644 Robert Reinhold, “Summit of Sorts on Global Warming,” The New York Times, August 27, 1989, https://www.nytimes.com/1989/08/27/us/summit-of-sorts-on-global-warming.html.

645 Peter Schwarz & Doug Randall, An Abrupt Climate Change Scenario and Its Implications for United

States National Security (Pasadena, CA: Jet Propulsion Laboratory, 2003), p. 2, https://training.fema.gov/hiedu/docs/crr/catastrophe%20readiness%20and%20response%20-%20appendix%202%20-%20abrupt%20climate%20change.pdf.

646 “Security Council Holds First-Ever Debate on Impact of Climate Change on Peace, Security, Hearing Over 50 Speakers,” United Nations, April 17, 2007, https://press.un.org/en/2007/sc9000.doc.htm.

647 National Security and the Threat of Climate Change (Alexandria: CNA Corporation, 2007), https://www.cna.org/CNA_files/pdf/National%20Security%20and%20the%20Threat%20of%20Climate%20Change.pdf.

648 Chad Briggs, "Climate Change and Hybrid Warfare Strategies" Journal of Strategic Security, 13, no. 4 (2020): pp. 45-57, https://doi.org/10.5038/1944-0472.13.4.1864.

649 Department of Defense, Summary of the Irregular Warfare Annex to the National Defense Strategy (Washington, DC: Department of Defense, 2020), https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.

650 "What is Climate Change?" United Nations, undated, https://www.un.org/en/climatechange/what-is-climate-change. Accessed December 14, 2022.

651 Rebecca Lindsey, "Climate Change: Global Sea Level," NOAA Climate, April 19, 2022, https://www.climate.gov/news-features/understanding-climate/climate-change-global-sea-level.

652 "Weather-related disasters increase over past 50 years, causing more damage but fewer deaths," World Meteorological Organization, August 31, 2021, https://public.wmo.int/en/media/press-release/weather-related-disasters-increase-over-past-50-years-causing-more-damage-fewer.

653 Ibid.

654 Robert Hart, "Climate Change Could Spark Future Pandemics, Study Finds," Forbes, April 29, 2022, https://www.forbes.com/sites/roberthart/2022/04/28/climate-change-could-spark-future-pandemics-study-finds/?sh=6fa54ec55787; Claire Klobucista & Lindsay Maizland, "Perilous Pathogens: How Climate Change Is Increasing the Threat of Diseases," Council on Foreign Relations, November 4, 2022, https://www.cfr.org/article/perilous-pathogens-how-climate-change-increasing-threat-diseases.

655 Li Cohen, "Climate change will start impacting global supply of corn and wheat as early as 2030, NASA study finds," CBS News, November 2, 2021, https://www.cbsnews.com/news/climate-change-food-supply-corn-wheat-crops-study/; Sara Schonhardt, "Wake-Up Call: Climate Change Threatens Rice Farming," Scientific American, August 18, 2021, https://www.scientificamerican.com/article/wake-up-call-climate-change-threatens-rice-farming/.

656 Dan Robitzski, "60% of the world's fish species at risk of extinction due to climate change," World Economic Forum, July 9, 2020, https://www.weforum.org/agenda/2020/07/climate-change-threatens-60-percent-of-the-world-s-fish-species/.

657 IPBES-IPCC Co-Sponsored Workshop Report on Biodiversity and Climate Change (Bonn: Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services, 2021), https://ipbes.net/sites/default/files/2021-06/20210609_workshop_report_embargo_3pm_CEST_10_june_0.pdf.

658 Barbara Neumann et al., "Future Coastal Population Growth and Exposure to Sea-Level Rise and Coastal Flooding - A Global Assessment" PLoS One, 10, no. 3 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4367969/.

659 Susan Murcott & Elizabeth Gribkoff, "Freshwater and Climate Change," MIT Climate Portal, Undated, https://climate.mit.edu/explainers/freshwater-and-climate-change.

660 Groundswell: Preparing for Internal Climate Migration (Washington, DC: World Bank, 2018), https://openknowledge.worldbank.org/handle/10986/29461; Report on the Impact of Climate Change on Migration (Washington, DC: White House, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/Report-on-the-Impact-of-Climate-Change-on-Migration.pdf.

661 Office of the Undersecretary of Defense, Department of Defense Climate Adaptation Plan (Washington, DC: United States Department of Defense, 2021), https://media.defense.gov/2021/Oct/07/2002869699/-1/-1/0/DEPARTMENT-OF-DEFENSE-CLIMATE-ADAPTATION-PLAN.PDF.

662 Intergovernmental Panel on Climate Change, IPCC Sixth Assessment Report, p. 12.

663 Ibid; Joshua Busby & Nina von Uexkull, "Climate Shocks and Humanitarian Crises: Which Countries Are Most at Risk?," Foreign Affairs, November 29, 2018, https://www.foreignaffairs.com/articles/world/2018-11-29/climate-shocks-and-humanitarian-crises.

664 "Agriculture, forestry, and fishing, value added (% of GDP)," World Bank, undated, https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS?most_recent_value_desc=true. Accessed February 20, 2023.

665 Intergovernmental Panel on Climate Change, IPCC Sixth Assessment Report, p.12; Busby & von Uexkull, "Climate Shocks and Humanitarian Crises."

666 Andrea Malji, Laurabell Obana & Cidney Hopkins, "When Home Disappears: South Asia and the Growing Risk of Climate Conflict," Terrorism and Political Violence, 34, no.5 (2022): pp. 939-957.

667 Busby & von Uexkull, "Climate Shocks and Humanitarian Crises"; Intergovernmental Panel on Climate Change, IPCC Sixth Assessment Report; Malji, Obana &Hopkins "When Home Disappears."

668 Busby & von Uexkull, “Climate Shocks and Humanitarian Crises.”

669 National Intelligence Council, National Intelligence Estimate: Climate Change and International Responses Increasing Challenges to US National Security Through 2040 (Washington, DC: Office of the Director of National Intelligence, 2021), pp. 11-15, https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf.

670 Melissa Fleming, “Rampant climate disinformation online is distorting dangers, delaying climate action,” Medium, May 16, 2022, https://medium.com/we-the-peoples/rampant-climate-disinformation-online-is-distorting-dangers-delaying-climate-action-375b5b11cf9b; René Marsh, “Big Oil has engaged in a long-running climate disinformation campaign while raking in record profits, lawmakers find,” CNN, December 9, 2022, https://www.cnn.com/2022/12/09/politics/big-oil-disinformation-record-profits-climate/index.html; Jeffrey Pierre & Scott Neuman, “How decades of disinformation about fossil fuels halted U.S. climate policy,” NPR, October 27, 2021, https://www.npr.org/2021/10/27/1047583610/once-again-the-u-s-has-failed-to-take-sweeping-climate-action-heres-why.

671 Lottie Limb, “How climate disinformation is spreading after Elon Musk’s Twitter takeover,” Euronews, November 17, 2022, https://www.euronews.com/green/2022/11/17/how-climate-disinformation-is-spreading-after-elon-musks-twitter-takeover; Naomi Oreskes, (2004) “The Scientific Consensus on Climate Change” Science, 306, no.5702 (2004): p. 1686, https://www.science.org/doi/10.1126/science.1103618. A

672 National Intelligence Council, National Intelligence Estimate, pp. 5-7, 11.

673 Ibid.

674 Ibid, p. 6.

675 Sedona Chinn, P. Sol Hart, &Stuart Soroka, “Politicization and Polarization in Climate Change News Content, 1985-2017” Science Communication 42, no. 1 (2020): pp. 112-129; Sinan Ülgen, “How Deep Is the North-South Divide on Climate Negotiations?,” Carnegie Europe, October 6, 2021, https://carnegieeurope.eu/2021/10/06/how-deep-is-north-south-divide-on-climate-negotiations-pub-85493.

676 Craig Timberg & Tony Romm, “Russian trolls sought to inflame debate over climate change, fracking, Dakota pipeline,” Chicago Tribune, March 1, 2018, https://www.chicagotribune.com/nation-world/ct-russian-trolls-climate-change-20180301-story.html.

677 Briggs, “Climate Change and Hybrid Warfare Strategies.”

678 “Over 1,700 environment activists killed in decade – report,” BBC News, September 29, 2022, https://www.bbc.com/news/science-environment-63064471.

679 Ali Hines, Decade of Defiance: Ten Years of Reporting Land and Environmental Activism Worldwide (London: Global Witness, 2022) ch.7, https://www.globalwitness.org/en/campaigns/environmental-activists/decade-defiance/#state-play-ten-years.

680 Rachael Burford, “Extinction Rebellion protests have cost police £60million since 2019,” Evening Standard, August 11, 2022, https://www.standard.co.uk/news/politics/extinction-rebellion-london-met-police-cost-bill-september-b1017959.html.

681 Department of Justice, “Des Moines Woman Sentenced to Eight Years in Prison for Conspiracy to Damage the Dakota Access Pipeline,” June 30, 2021, https://www.justice.gov/usao-sdia/pr/des-moines-woman-sentenced-eight-years-prison-conspiracy-damage-dakota-access-pipeline.

682 Colin Clarke & Rasha Al Aqeedi, “What Terrorism Will Look Like in the Near Future,” Newlines Institute, June 29, 2021, https://newlinesinstitute.org/nonstate-actors/what-terrorism-will-look-like-in-the-near-future/.

683 Glenn Kessler, “The bogus ‘allegation’ that Putin is funding a California environmental charity,” The Washington Post, March 17, 2022, https://www.washingtonpost.com/politics/2022/03/17/bogus-allegation-that-putin-is-funding-california-environmental-charity/; Merrill Matthews, “Investigate Russia’s covert funding of US anti-fossil fuel groups,” The Hill, March 1, 2022, https://thehill.com/opinion/energy-environment/596304-investigate-russias-covert-funding-of-us-anti-fossil-fuel-groups/.

684 Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Picador, 2020).

685 The eight Arctic States, and members of the Arctic Council, are Canada, Denmark, Finland, Iceland, Norway, Sweden, Russia, and the United States.

686 “Arctic Military Activity Tracker,” Center for Strategic and International Studies, accessed February 23, 2023, https://arcticmilitarytracker.csis.org/.

687 National Intelligence Council, National Intelligence Estimate, p. 8.

688 Sherri Goodman et al., Climate Change and Security in the Arctic (Washington, DC: The Center for Climate Security, 2021), https://climateandsecurity.org/wp-content/uploads/2021/01/Climate-Change-and-Security-in-the-Arctic_CCS_NUPI_January-2021-1.pdf.

689 Ibid, p. 5.

690 Ibid, p. 15.

691 Josh Jacobs, "Has Interpol become the long arm of oppressive regimes?," The Guardian, October 17, 2021, https://www.theguardian.com/global-development/2021/oct/17/has-interpol-become-the-long-arm-of-oppressive-regimes; Shelby Magid & Yulia Shalomov, "Russia's veto makes a mockery of the United Nations Security Council," The Atlantic Council, March 15, 2022, https://www.atlanticcouncil.org/blogs/ukrainealert/russias-veto-makes-a-mockery-of-the-united-nations-security-council/; Yaroslav Trofimov, Drew Hinshaw & Kate O'Keeffe, "How China Is Taking Over International Organizations, One Vote at a Time," The Wall Street Journal, September 29, 2020, https://www.wsj.com/articles/how-china-is-taking-over-international-organizations-one-vote-at-a-time-11601397208.

692 Goodman et al., Climate Change and Security in the Arctic, pp. 14-15.

693 Pratnashree Basu, "Troubled waters: Marine ecology threats in the South China Sea," Observer Research Foundation, June 18, 2021, https://www.orfonline.org/research/troubled-waters-marine-ecology-threats-in-the-south-china-sea/.

694 Haakon Sagbakken et al., "Climate Change, Security and Regional Cooperation in ASEAN," ASEAN Climate Change and Energy Project, March 31, 2020, https://accept.aseanenergy.org/climate-change-security-and-regional-cooperation-in-asean/; Wilson Vorndick, "China's Island Building + Climate Change: Bad News," Real Clear Defense, March 9, 2015, https://www.realcleardefense.com/articles/2015/03/10/chinese_island_reclamation_the_climate_change_challenge_107722-2.html.

695 National Intelligence Council, National Intelligence Estimate, p.10.

696 Brian McGleenon, "Water wars: the battle to harness 'Asia's water tower,'" The Independent, April 9, 2021, https://www.proquest.com/docview/2509894246/948CB4F8CED944C1PQ/1.

697 Ibid.

698 Joel Wuthnow, Satu Limaye & Nilanthi Samaranayake, "Brahmaputra: A Conflict-Prone River Takes a Step Backwards," War on the Rocks, December 23, 2020, https://warontherocks.com/2020/12/a-conflict-prone-river-takes-a-step-backwards/.

699 McGleenon, "Water wars."

700 "Renegotiate Indus Water Treaty to address impact of climate change: Parliamentary Panel," The Hindu (India), August 6, 2021, https://www.thehindu.com/news/national/renegotiate-indus-water-treaty-to-address-impact-of-climate-change-parliamentary-panel/article35766702.ece.

701 "India plans to resort to water terrorism in region," Associated Press of Pakistan (Pakistan), August 6, 2021, https://www.app.com.pk/national/india-plans-to-resort-to-water-terrorism-in-region/.

702 John Vater, "The Indus Waters Treaty: Prospects for India-Pakistan Peace," Institute of South Asian Studies, National University of Singapore, June 23, 2021, https://www.isas.nus.edu.sg/papers/the-indus-waters-treaty-prospects-for-india-pakistan-peace/.

703 Jeff Goodson, "Infrastructure and Irregular Warfare: A Good Year for Afghan Dams," Real Clear Defense, December 19, 2016, https://www.realcleardefense.com/articles/2016/12/20/infrastructure_and_irregular_warfare_afghan_dams_110524.html.

704 Katharina Nett & Lukas Rüttinger, Insurgency, Terrorism and Organised Crime in a Warming Climate: Analysing the Links Between Climate Change and Non-State Armed Groups (Berlin, Adelphi: 2016), pp.10-19, https://climate-diplomacy.org/sites/default/files/2020-10/CD%20Report_Insurgency_170724_web.pdf; Binh Pham-Duc et al., "The Lake Chad hydrology under current climate change," Scientific Reports, 10, no. 5498, (2020), https://www.nature.com/articles/s41598-020-62417-w;

705 Vincent Foucher, ""The Tale of a Disappearing Lake". The Boko Haram Insurgency and the Narrative Politics of the Climate Crisis," Megatrends, March 6, 2023, https://www.megatrends-afrika.de/en/publication/mta-spotlight-23-boko-haram-and-the-alleged-disappearance-of-lake-chad; Nett & Rüttinger, Insurgency, Terrorism and Organised Crime in a Warming Climate; Pham-Duc et al, "The Lake Chad hydrology under current climate change."

706 Nett & Rüttinger, Insurgency, Terrorism and Organised Crime in a Warming Climate; Siobhán O'Grady, "This little-known conflict in Nigeria is now deadlier than Boko Haram," The Washington Post, July 26, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/07/26/this-little-known-conflict-in-nigeria-is-now-deadlier-than-boko-haram/.

707 Nett & Rüttinger, Insurgency, Terrorism and Organised Crime in a Warming Climate; Caroline Varin , "No Opportunity Lost: The ISWAP Insurgency in the Changing Climate of Lake Chad Region," African Conflict and Peacebuilding Review, 10 no. 2 (2020): pp. 141-157.

708 Peter Schwartzstein, "Climate Change and Water Woes Drove ISIS Recruiting in Iraq," National Geographic, November 13, 2017, https://www.nationalgeographic.com/science/article/climate-change-drought-drove-isis-terrorist-recruiting-iraq.

709 Luis Chaparro, "The Sinaloa Cartel Is Controlling Water in Drought-Stricken Mexico," Vice News, September 20, 2022, https://www.vice.com/en/article/4ax479/mexico-sinaloa-cartel-water.

710 Ibid.

711 Ben Heubl, "Water conflict: Data shows how climate-change protests are expanding," Engineering and Technology, June 9, 2021, https://eandt.theiet.org/content/articles/2021/06/data-shows-climate-change-related-protests-are-on-the-rise/.

712 National Intelligence Council, National Intelligence Estimate, p. 10.

713 Ecological Threat Register 2020: Understanding Ecological Threats, Resilience and Peace (Sydney: Institute for Economics and Peace, 2020), https://www.economicsandpeace.org/wp-content/uploads/2020/09/ETR_2020_web-1.pdf.

714 Ibid; Report on the Impact of Climate Change on Migration: A Report by the White House (Washington, DC: The White House, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/Report-on-the-Impact-of-Climate-Change-on-Migration.pdf.

715 Abhishek Chakravarty, "Climate refugees and Assam's future," Indian Express (India), January 28, 2021, https://indianexpress.com/article/opinion/climate-refugees-and-assams-future-7165653/.

716 Report on the Impact of Climate Change on Migration, pp. 9-10.

717 Agnieszka Legucka, "Russia's Long-Term Campaign of Disinformation in Europe," Carnegie Europe, March 19, 2020, https://carnegieeurope.eu/strategiceurope/81322; Roberto Rocha & Jeff Yates, "Twitter trolls stoked debates about immigrants and pipelines in Canada, data show," CBC News (Canada), February 12, 2019, https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.50147502; Trish Turner, "Russian trolls are meddling in US immigration controversy, a top GOP senator says," ABC News, June 20, 2018, https://abcnews.go.com/Politics/russian-trolls-meddling-us-immigration-controversy-top-gop/story?id=56032588.

718 Kelly Greenhill, "When Migrants Become Weapons: The Long History and Worrying Future of a Coercive Tactic," Foreign Affairs, March/April 2022, https://www.foreignaffairs.com/articles/europe/2022-02-22/when-migrants-become-weapons.

719 Ibid.

720 Report on the Impact of Climate Change on Migration, pp. 9-10.

721 Ibid, p. 9.

722 Ibid; Sam Mullins, Jihadist Infiltration of Migrant Flows to Europe: Perpetrators, Modus Operandi and Policy Implications (Cham: Palgrave MacMillan, 2019).

723 Mullins, Jihadist Infiltration of Migrant Flows to Europe, pp. 6-11.

724 José Ignacio Castañeda Perez, "'Boom of opportunities': How smugglers, Mexican cartels profit from US border restrictions," Arizona Central, December 16, 2022, https://www.azcentral.com/in-depth/news/politics/border-issues/2022/12/16/how-cartels-profit-migrants-desperation-along-u-s-mexico-border/10704315002/.

725 Mullins, Jihadist Infiltration of Migrant Flows to Europe, pp. 85-90.

726 Ibid.

727 Report on the Impact of Climate Change on Migration, pp. 9-10.

728 Briggs, "Climate Change and Hybrid Warfare Strategies."

729 Office of the Undersecretary of Defense, Department of Defense Draft Climate Adaptation Plan (Washington, DC: Department of Defense, 2021), https://media.defense.gov/2021/Oct/07/2002869699/-1/-1/0/DEPARTMENT-OF-DEFENSE-CLIMATE-ADAPTATION-PLAN.PDF.

730 Goodson, "Infrastructure and Irregular Warfare"; Sam Mullins, ""Great Power Competition Versus Counterterrorism: A False Dichotomy," Just Security, October 23, 2020, https://www.justsecurity.org/72811/great-power-competition-versus-counterterrorism-a-false-dichotomy/.

731 Briggs, “Climate Change and Hybrid Warfare Strategies.”

732 Summary of the Irregular Warfare Annex to the National Defense Strategy.

733 National Intelligence Council, National Intelligence Estimate, p. ii.

734 Charles N. Black & David C. Ellis, “Complexity, Statecraft, and the Consortium for Irregular Warfare,” Irregular Warfare Center, January 3, 2023, https://irregularwarfarecenter.org/2023/01/complexity-statecraft-and-the-consortium-for-irregular-warfare/; James W. Derleth, “Great Power Competition, Irregular Warfare, and the Gray Zone,” Irregular Warfare Center, January 13, 2023, https://irregularwarfarecenter.org/2023/01/great-power-competition-irregular-warfare-and-the-gray-zone/.

735 Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms, JP 1-01 (Washington, DC: Joint Chiefs of Staff, 2001).

736 Håkon Lunde Saxi, Bengt Sundelius & Brett Swaney,“Baltics Left of Bang: Nordic Total Defense and Implications for the Baltic Sea Region,” Strategic Forum, no. 304 (January 2020), https://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-304.pdf.

737 Francis Fukuyama, “The End of History,” The National Interest no. 16 (1989): pp. 3-18, https://www.jstor.org/stable/24027184.

738 Saxi, Sundelius & Swaney,“Baltics Left of Bang: Nordic Total Defense and Implications for the Baltic Sea Region.”

739 Ibid, pp. 7-11.

740 Ibid, p. 6.

741 Mykhaylo Zabrodskyi et al., “Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022,” Royal United Services Institute, November 30, 2022, https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-converntional-warfighting-russias-invation-ukraine-february-july-2022/.

742 Ivan Arreguin-Toft, “How the Weak Win Wars: A Theory of Asymmetric Conflict,” International Security 26 no. 1 (2001): pp. 93-128.

743 Dennis Gyllensporre, “Contemporary Hybrid Warfare and the Evolution of Special Operations Theory,” in Operations from a Small State Perspective: Future Security Challenges ed. Gunilla Eriksson and Ulrica Pettersson (Charm: Palgrave Macmillan, 2017), p. 32.

744 Ulrica Pettersson & Hans Ilis-Alm, “Resistance Operations: Challenges and Opportunities for Special Operations Forces,” Journal on Baltic Security, 8 no. 1 (2022): pp. 76-93.

745 Sean McFate, The New Rules of War (New York, Harper and Collins Publishers, 2019), p. 250.

746 Pettersson & Ilis-Alm, “Resistance Operations: Challenges and Opportunities for Special Operations Forces.”

747 HI Sutton, “Ukraine´s New Weapon to strike Russian Navy in Sevastopol,” Naval News, September 21, 2022, https://www.navalnews.com/naval-news/2022/09/ukraines-new-weapon-to-strike-russian-navy-in-sevastopol/.

748 David Kilcullen, “The Evolution of Unconventional Warfare,” Scandinavian Journal of Military Studies, 2, no. 1 (June 20, 2019): pp. 61–71, https://doi.org/10.31374/sjms.35.

749 Andrew Roth, “Russia issues list of demands it says must be met to lower tensions in Europe,” The Guardian, December 17, 2021, https://www.theguardian.com/world/2021/dec/17/russia-issues-list-demands-tensions-europe-ukraine-nato.

750 Frank Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Arlington: Potomac Institute, December 2007), p. 8.

751 Colin S. Gray, Explorations in Strategy—Strategic Utility of Special Operation Forces (Westport: Praeger Publishers, 1996), p. 169.

752 James Kiras, Special Operations and Strategy From World War II to the War on Terrorism (New York: Routledge, 2006), p. 115.

753 Bernd Horn, “When Cultures collide: The Conventional Military/ SOF Chasm,” Canadian Military Journal, Autumn (2004): p. 5.

754 Ronny Modigs, “The Utility of Special Operations Forces in Small State,” in Operations from a Small State Perspective: Future Security Challenges ed. Gunilla Eriksson and Ulrica Pettersson (Charm: Palgrave Macmillan, 2017).

755 UK Ministry of Defence, "Future Security Challenges in the Baltic Sea Region," (Shrivenham: Development, Concepts and Doctrine Centre, November 2015), p. 22.

756 Matthieu Boulègue, "Russia´s Military Posture in the Arctic: Managing Hard Power in a "Low Tension" Environment," Chatham House, June 2019, pp. 6-7.

757 S.G. Chekinov & S.A. Bogdanov, "The Nature and Content of a New-Generation War," Voennaya Mysl [Military Thought] (Russia), accessed January 9, 2023, pp. 12-23.

758 Tony Balasevicius, "Future War: Continuous Conflict in an Era of Rising Peer Competition," CANSOFCOM Education & Research Centre, 2019, p. 44.

759 Zabrodskyi et al,. "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine."

760 Ibid, p. 43.

761 In several ways comparable to the first phases in sixth-generation warfare (6GW) or what has been defined as the Gray Zone.

762 Frank Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars" (Arlington, VA: Potomac Institute, December 2007), pp. 30-31.

763 Rob de Wijk et al., "The Future of NLD SOF: Towards an all domain force" (Hague: The Hague Centre for Strategic Studies, July 2021), p. 75.

764 Law (2006:343), Swedish Armed Forces support to the Police during war on terror [Lag (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning], accessed January 18, 2023, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2006343-om-forsvarsmaktens-stod-till_sfs-2006-343.

765 De Wijk et al,. "The Future of NLD SOF: Towards an all domain force."

766 Ibid, p. 73.

767 Ibid, p. 77.

768 Gyllensporre, Contemporary Hybrid Warfare and the Evolution of Special Operations Theory, p. 35.

769 Rivard Piché & Breede H. Christian, "Adapting Special Operations Forces Employment in Great Power Competition: Reflections on the future of Canadian Special Operations Forces," Kingston Consortium on International Security 1, no, 5 (June 2021): p. 3.

770 Elin Berg & Ulrica Pettersson, "Resilience and Resistance in the Digital Age: Revisiting the Threshold Effect in Total Defence," Journal on Baltic Security 8, no. 2 (2022): pp. 41-60.

771 Asta Maskaliūnaitė, "Exploring Resistance Operating Concept. Promises and pitfalls of (violent) underground resistance," Journal on Baltic Security 7, no. 1 (2021): pp. 27-38.

772 Otto C. Fiala, Resistance Operating Concept (Stockholm, Swedish Defence University, 2019). This was the first edition of the Resistance Operating Concept.

773 Otto C. Fiala and Ulrica Pettersson, "ROC(K) Solid Preparedness: Resistance Operations Concept in the Shadow of Russia," PRISM 8, no. 4 (2020): pp. 17-28.

774 See https://mv.group. TheMW Group is a modern Nordic defence and security service and solution provider with a mission to serve a strong society.

775 Bradely C. Nindl et. al, "Perspectives on resilience for military readiness and preparedness: Report of an international military physiology roundtable," Journal of Science and Medicine in Sport 21, no. 11 (2018): pp. 1116–1124.

776 Ulrica Pettersson & Hans Ilis-Alm, "Resistance Operations: Challenges and Opportunities for Special Operations Forces," Journal on Baltic Security 8, no. 1 (2022): pp. 77-94.

777 Sandor Fabian, "Modern Resistance – Learning From Non-Western Examples," Journal on Baltic Security 8, no. 1 (2022): pp. 44-66.

778 Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy," Center for Security and Strategic Research no. 2 (2014).

779 Ibid, pp. 35-36.

780 Gray, Explorations in Strategy, p. 169.

781 Rivard Piché & Breede, "Adapting Special Operations Forces Employment in Great Power Competition," p. 4.

782 Jack Watling, “Sharpening the Dagger: Optimizing Special Forces for Future Conflict,” Whitehall Report 1, no. 21(2021).

783 Gyllensporre, Contemporary Hybrid Warfare and the Evolution of Special Operations Theory, pp. 36-37.

784 Zabrodskyi et al., “Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine,” p. 33.

785 David Kilcullen, Dragons and Snakes: How the Rest Learned to Fight the West (Oxford: Oxford University Press, 2020), pp. 243-244.

786 Marc Bloch, Strange Defeat (Oxford: Oxford University Press, 1949), pp. 36–37, 45.

787 William Mitchell, Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military (New York: G. P. Putnam’s Sons, 1924), pp. 25–26.

788 Internet Movie Database (IMDb), https://www.imdb.com. https://www.argunners.com/new-upcoming-war-movies-2019/.

789 Chart data: Uppsala Conflict Data Program (UCDP)/Peace Research Institute Oslo (PRIO) Armed Conflict Dataset, version 17.2. (Note: This data set includes only armed conflicts that involved at least one state and disregards conflicts between nonstate actors alone.) See also Marie Allansson, Erik Melander &Lotta Themnér, “Organized Violence, 1989–2016,” Journal of Peace Research, 54, no. 4 (2017); Nils Petter Gleditsch et al., “Armed Conflict, 1946–2001: A New Dataset,” Journal of Peace Research, 39, no. 5 (2002): pp. 615–37.

790 Mark Thompson, “The Pentagon’s F-35: The Most Expensive Weapon Ever Built,” Time, Feburary 25, 2013, https://content.time.com/time/magazine/article/0,9171,2136312-3,00.html; James Drew, “F-35A Cost and Readiness Data Improves in 2015 as Fleet Grows,” FlightGlobal.com, February 2, 2016, www.flightglobal.com/news/articles/f-35a-cost-and-readiness-data-improves-in-2015-as-fl-421499.

791 Qiao Liang & Wang Xiangsui, Unrestricted Warfare (Beijing: PLA Literature and Arts Publishing House, 1999); Stefan Halper, China: The Three Warfares (New York: University of Cambridge, ,2013), https://cryptome.org/2014/06/prc-three-wars.pdf; Eugene Rumer, “The Primakov (Not Gerasimov) Doctrine in Action,” Carnegie Endowment for International Peace, June 5, 2019, https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

792 Hearing to receive testimony on United States European Command, 114th Cong. 2 (March 1, 2016) (statement of Philip Breedlove, the Commander of the United States European Command and Supreme 9Allied Commander, Europe), www.armed-services.senate.gov/imo/media/doc/16-20_03-01-16.pdf.

793 Stefan Halper, China: The Three Warfares.

794 Ivo Juurvee & Anna-Mariita Mattiisen. The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict (Tallinn: International Centre for Defence and Security, August 21, 2020), https://icds.ee/en/the-bronze-soldier-crisis-of-2007/.

795 For Estonia, see Income and Assets Profiles, Foresight Centre, March 29, 2019, https://arenguseire.ee/en/raportid/income-and-assets-profiles/; For Latvia, see Kārlis Vilerts & Olegs Krasnopjorovs, “Can Differences in Characteristics Explain Ethnic Wage Gap in Latvia?,” Economics and Business, 30, no.1 (2017): pp. 5-15, https://doi.org/10.1515/eb-2017-0001.

796 “Authority: Sharp surge in cyberattacks on media houses this year,” ERR News (Estonia),September 21, 2022, https://news.err.ee/1608722875/authority-sharp-surge-in-cyberattacks-on-media-houses-this-year.

797 Ieva Berzina, Mitigating Nonmilitary Vulnerabilities of Latvia, American Enterprise Institute, February 2018, p. 1, https://www.aei.org/wp-content/uploads/2018/02/Mitigating-Nonmilitary-Vulnerabilities-of-Latvia.pdf.

798 Michael Jonsson & Jakob Gustafsson, Espionage by Europeans 2010-2021. A Preliminary Review of Court Cases, (Stockholm, Swedish Defence Research Agency, 2022), https://www.foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5312--SE.

799 Greg Miller & Catherine Belton, “Russia’s spies misread Ukraine and misled Kremlin as war loomed,” The Washington Post, August 19, 2022, https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/.

800 Department of Defense, Summary of the Irregular Warfare Annex to the National Defense Strategy (Washington, DC: Department of Defense, 2020), https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.

801 David H. Ucko & Thomas A. Marks, Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action, 2nd ed., (Washington, DC: National Defense University Press, 2022), p. 10.

802 Carl Bildt, The Baltic Litmus Test, 73, no. 5 (New York: Foreign Affairs, Sep-Oct, 1994), p. 72, https://www.jstor.org/stable/20046832.

803 "Russian interest in Estonian citizenship spikes," ERR News (Estonia), January 5, 2023, https://news.err.ee/1608841270/russian-interest-in-estonian-citizenship-spikes.

804 Andrew Radin, Hybrid Warfare in the Baltics: Threats and Potential Responses, (Santa Monica: RAND, 2017), p. 13,https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf.

805 Nick Reynolds & Jack Watling, "Ukraine Through Russia's Eyes," Royal United Services Institute for Defence and Security Studies, February 25, 2022, https://rusi.org/explore-our-research/publications/commentary/ukraine-through-russias-eyes.

806 "Internal Security reserve more expensive than planned," ERR News (Estonia), December 12, 2019, https://news.err.ee/1013603/internal-security-reserve-more-expensive-than-planned.

807 Erika Kinetz, '"We Will Find You:" Russians Hunt Down Ukrainians on Lists," PBS, December 21, 2022, https://www.pbs.org/wgbh/frontline/article/russians-hunt-down-ukrainians-on-lists/.

808 Andrew Krepinevich, 7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century (New York: Bantam Book, 2009), pp. 63-67.

809 Ruth Henig, The League of Nations (London, UK: Haus Publishing, 2010), pp. 144-173.

810 Peter Wyden, The Passionate War: The Narrative History of the Spanish Civil War (New York: Simon & Schuster, 1983), pp.19-20, 77-100

811 Bernadette Whelan, review of "Wilson, War, and Peace: The Will to Believe, Woodrow Wilson, World War I and America's Strategy for Peace and Security," by Ross A. Kennedy War in History, 17, no. 4 (November 1, 2010): pp. 527-530.

812 Robert Dallek, The Lost Peace: Leadership in a Time of Horror and Hope, 1945-1953 (New York: HarperCollins Publishers, 2010), pp. 95-106.

813 Michael Burleigh, Small Wars, Faraway Places: Global Insurrection and the Making of the Modern World 1945-1965 (New York: Viking, 2013), pp. 131-155

814 John Lewis Gaddis, Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy (New York: Oxford University Press, 1982), p. 210.

815 Dallek, The Lost Peace, pp. 104-106.

816 James Traub, "Cold War 2.0 is Ushering in Non-alignment 2.0: Countries in the Developing World Don't want to choose sides – and don't feel they have to," Foreign Policy, July 9, 2022.

817 Francis Fukuyama, "The End of History?" The National Interest, no. 16 (1989) : pp. 5-15.

818 Samuel Huntington, "The Clash of Civilizations?" Foreign Affairs 72, no. 3 (1993) : pp. 22–29.

819 Orlando Figes, Revolutionary Russia 1881-1991: A History (New York: Henry Holt and Company, 2014), pp. 276-294.

820 Sandra Mackey, The Iranians: Persia, Islam, and the Soul of the Nation, (New York: Plume, 1998), pp. 393-410.

821 Don Oberdorfer and Robert Carlin, The Two Koreas: A Contemporary History (New York: Basic Books, 2013), pp. 419-464.

822 Francis Fukuyama, "More Proof That This Really Is the End of History," The Atlantic, October 17, 2022.

823 X (George Kennan), "The Sources of Soviet Conduct," Foreign Affairs, July 1, 1947.

824 White House, Report to the National Security Council on the Objectives and Programs for National Security, (Washington DC: National Security Council, 1950), Section VI.

825 William R Gery, SeYoung Lee & Jacob Ninas, "Information Warfare in an Information Age," Joint Forces Quarterly 85, (2nd Quarter, 2017): pp. 25-29.

826 Hal Brands, "Democracy vs. Authoritarianism: How Ideology Shapes Great Power Conflict," Survival 60, no. 5 (October-November 2018): pp. 87-90.

827 Hugh Rockoff, "The Peace Dividend in Historical Perspective," The American Economic Review 88, no. 2, (1998), p. 50.

828 Joseph L Votel et al., "Unconventional Warfare in the Gray Zone," Joint Forces Quarterly, 80, (First Quarter, 2016): pp. 101-102.

829 Dwight Eisenhower, Farewell Address, (Eisenhower Presidential Library KS: D.D. Eisenhower's Papers as President, Speech Series, Box 38, January 17, 1961), pp. 12-15.

THE END