U.S. Navy divers and special operators attached to SEAL Delivery Team (SDV) 2, perform SDV operations with the Ohio-Class nuclear-powered guided-missile submarine USS Florida (SSGN 728) for material certification. U.S. NAVY PHOTO BY SENIOR CHIEF MASS COMMUNICATION SPECIALIST ANDREW MCKASKLE (RELEASED).

In this concise monograph, the author argues that USSOF use their skills, capabilities, and relationships to provide planners and policymakers a unique deterrence tool. Mr. Haddick first provides a brief overview of deterrence theory as a baseline for presenting his viewpoints on this neglected special operations role. Then, presents a case study that effectively highlights how U.S. adversaries have adapted their tactics to exploit gaps in our current deterrence framework, thwarting or bypassing our legacy deterrence structure. The Joint Special Operations University is pleased to offer this monograph to inform policymakers and the SOF community of the deterrent value of both direct and indirect special operations.

Joint Special Operations University
7701 Tampa Point Boulevard
MacDill AFB, FL 33621

https://jsou.libguides.com/jsoupublications

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY
PRESS

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ISBN 978-1-941715-29-1

JSOU Report 17-11

How Do SOF Contribute to Comprehensive Deterrence?

Haddick

JSOU

JOINT SPECIAL OPERATIONS UNIVERSITY

How Do SOF Contribute to Comprehensive Deterrence?

Robert Haddick

JSOU Report 17-11

Joint Special Operations University and the Center for Strategic Studies

The Joint Special Operations University (JSOU) provides its publications to contribute toward expanding the body of knowledge about joint special operations. JSOU publications advance the insights and recommendations of national security professionals and the Special Operations Forces (SOF) students and leaders for consideration by the SOF community and defense leadership.

JSOU is the educational component of the United States Special Operations Command (USSOCOM), MacDill Air Force Base, Florida. The JSOU mission is to prepare SOF to shape the future strategic environment by providing specialized joint professional military education, developing SOF-specific undergraduate and graduate level curriculum and by fostering special operations research, analysis and outreach in support of USSOCOM objectives.

JSOU conducts research through its Center for Strategic Studies (CSS) where efforts center upon the USSOCOM mission:

> **USSOCOM mission.** USSOCOM synchronizes the planning of Special Operations and provides Special Operations Forces to support persistent, networked, and distributed Geographic Combatant Command operations in order to protect and advance our Nation's interests.

Press publications are available for download from the JSOU Library web page located at https://jsou.libguides.com/jsoupublications.

Joint Special Operations University

Editorial Advisory Board

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY
PRESS

How Do SOF Contribute to Comprehensive Deterrence?

Robert Haddick

JSOU Report 17-11
The JSOU Press
MacDill Air Force Base, Florida
2017

Comments about this publication are invited and should be forwarded to the Director of the Center for Strategic Studies, Joint Special Operations University, 7701 Tampa Point Blvd., MacDill AFB, FL 33621.

****

The JSOU Center for Strategic Studies (CSS) is currently accepting written works relevant to special operations for potential publication. For more information, please contact the CSS Director at jsou_research@socom.mil. Thank you for your interest in the JSOU Press.

****

This work was cleared for public release; distribution is unlimited.

Printed in December 2017.

ISBN 978-1-941715-29-1

Editor's note: Throughout this report are references to clandestine and covert operations. Executive Order 12333, United States Intelligence Activities, states in paragraph 1.7(a) (4) that "The Director of the Central Intelligence Agency shall: Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective."

Joint publication 3-05, Special Operations, describes the characteristics of special operations and the need for SOF to form partnerships to effectively execute SOF operations. "SOF routinely operate with Department of State (DOS) and other USG departments and agencies, intergovernmental organizations (IGOs), and other nations' forces. Clandestine, covert, and low-visibility operations may require extensive interagency or interorganizational coordination."

The views expressed in this publication 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 Special Operations Command, or the Joint Special Operations University.

Authors are granted academic freedom provided their work does not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers authors to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues.

Recent Publications of the JSOU Press

The Death of the Golden Hour and the Return of the Future Guerrilla Hospital, JSOU Report 17-10, Warner D. Farr

Property Rights and Social Justice as an Indicator of Stability: The SOF Nexus, JSOU Report 17-9, Bill Mandrick

Transitioning from War to Peace: Post-Deployment Support for Special Operations Forces, JSOU Report 17-8, Jennifer M. Hazen

2017 Special Operations Student Essays, JSOU Report 17-7

Special Operations Theory, JSOU Report 17-6, Volume 3, edited by Peter McCabe and Paul Lieber

Special Operations Contracting: 21st Century Approaches for Service and Technology Acquisition, JSOU Report 17-5, Benjamin Tkach

On the cover. The Zumwalt-class destroyer DDG 1000 is a new class of multi-mission U.S. Navy surface combatant ship designed to operate as part of a joint maritime fleet. PHOTO SOURCE: U.S. NAVY PHOTO ILLUSTRATION/RELEASED. The second ship in the Zumwalt-class of destroyers, DDG 1001 is named in honor of Medal of Honor recipient Navy Petty Officer 2nd Class (SEAL) Michael A. Monsoor. On Sept. 29, 2006 in Ar Ramadi, Iraq, as part of a sniper overwatch security position with two other SEALs and several Iraqi Army soldiers, an insurgent threw a fragmentation grenade into their position. Petty Officer Monsoor dropped onto the grenade, smothering it to protect his teammates. His Medal of Honor citation reads, "By his undaunted courage, fighting spirit, and unwavering devotion to duty in the face of certain death, Petty Officer Monsoor gallantly gave his life for his country, thereby reflecting great credit upon himself and upholding the highest traditions of the United States Naval Service." INFORMATION SOURCE: U.S. NAVY OFFICE OF INFORMATION STORY NUMBER NNS160617-07.

Back cover. U.S. Navy divers and special operators attached to SEAL Delivery Team (SDV) 2, perform SDV operations with the Ohio-Class nuclear-powered guided-missile submarine USS Florida (SSGN 728) for material certification. Material certification allows operators to perform real-world operations anytime, anywhere. U.S. NAVY PHOTO BY SENIOR CHIEF MASS COMMUNICATION SPECIALIST ANDREW MCKASKLE (RELEASED).

Contents

From the Director

This work represents a third successful research effort and monograph by Robert Haddick for the Joint Special Operations University. While other authors and leaders in the special operations community taught how special operations forces actions might achieve or affect U.S. national security at the strategic level, few make the connection relevant to the act or process of deterrence. Mr. Haddick's discussion should prove valuable to those military planners and strategists—both U.S. and our partner nations—who are looking for, and assessing, all available tools that support a nation's security strategy. We welcome your feedback on this and any other of our publications.

Boyd L. Ballard
Director, Center for Strategic Studies

Foreword

Deterrence amply served U.S. defense interests during the Cold War years, causing our adversaries to calculate the expected costs and benefits of aggression and dissuading them from acting in ways that put Americans at risk. In this monograph, Robert Haddick argues that deterrence continues to serve as a means of addressing security challenges from both state and non-state actors, as the nuclear threat of the Cold War has been superseded by terrorism, cyber and "hybrid" warfare, and other gray zone dangers. He explains how U.S. Special Operations Forces (SOF) can contribute to the concept of comprehensive deterrence described in the 2006 DOD *Deterrence Operations Joint Operating Concept*.

In this concise monograph, the author argues that SOF use their skills, capabilities, and relationships to provide planners and policymakers a unique deterrence tool. Mr. Haddick first provides a brief overview of deterrence theory as a baseline for presenting his viewpoints on this neglected special operations role. He then presents a case study that effectively highlights how U.S. adversaries have adapted their tactics to exploit gaps in our current deterrence framework, thwarting or bypassing our legacy deterrence structure. Examples offered by case studies of al-Qaeda, Iran, Russia, and China illustrate how hostile actors or rivals have adroitly circumvented our deterrence capabilities. Finally, he offers insight into the ways in which SOF capabilities can be of value in bridging these gaps by providing discrete, coercive leverage in ways that incur less risk and lower costs than more conventional approaches.

Mr. Haddick also offers insights drawn from Israel's application of deterrence theory and methods against several non-state adversaries. In addressing the threats posed by these adversaries, Israel developed its "cumulative deterrence" approach, which capitalizes on a history of military successes. While accepting that the complete destruction of groups such as Hezbollah, Hamas, and the Islamic State of Iraq and Syria are probably beyond their capabilities, Israeli policymakers and military leaders have managed to establish a climate of general deterrence through the use of airpower, special operations, intelligence, and covert action.

Preparing for comprehensive deterrence, the author argues, requires that planners continuously assess an adversary's perceptions, interests, and decision calculus. It also requires U.S. and partner forces—both conventional and SOF—to adapt traditional missions and capabilities to the demands of deterrence-by-denial and deterrence-by-punishment approaches. This is happening today with SOF deploying to assist the Baltic states of Lithuania, Latvia, and Estonia in resilience building activities aimed at deterring Russian intervention.

The Joint Special Operations University is pleased to offer this monograph to inform policymakers and the SOF community of the deterrent value of both direct and indirect special operations. This monograph should be of interest not only to defense policymakers and analysts, but also defense-sector scholars and the commanders and planners who must prepare SOF for roles and missions in support of comprehensive deterrence.

Will Irwin
Resident Senior Fellow, Center for Strategic Studies

About the Author

Robert Haddick is a visiting senior fellow at the Mitchell Institute for Aerospace Studies, the research affiliate of the Air Force Association. Haddick supports the Institute's mission to develop the roles of air, space, and cyber capabilities and explore their contributions to national security strategies.

He has been a research contractor at U.S. Special Operations Command's Joint Special Operations University (JSOU) since 2012. His research focuses on the changing security balance in the Asia-Pacific region and the implications for U.S. and partner strategies and military policies. In October 2014, Haddick authored and published through JSOU the monograph *Challenges in the Asia-Pacific Theater for U.S. and Partner Nation Special Operations Forces*, and in January 2016, *Improving the Sustainment of SOF Distributed Operations in Access-Denied Environments*.

Haddick also authored *Fire on the Water: China, America, and the Future of the Pacific* in 2014. The book discusses how China's reemergence as a great power is leading to a growing clash of interests in the Asia-Pacific region, and provides a detailed description of diplomatic, military, and acquisition reforms the United States and its partners in the region should undertake if they are to maintain stability and protect their interests. Fire on the Water received advanced endorsements from former Secretary of the Navy John Lehman; former commander of U.S. Pacific Command Admiral Timothy Keating, United States Navy (Retired); former Assistant Secretary of Defense for Asia & Pacific Security Affairs Lieutenant General Wallace "Chip" Gregson, United States Marine Corps (Retired); Lieutenant General David Deptula, United States Air Force (Retired), chief planner of the 1991 Persian Gulf air campaign; and Congressman J. Randy Forbes, (VA-4), chairman of the House Armed Services subcommittee on Seapower & Projection Forces.

Haddick lectures on China's military power and U.S. strategy in the Asia-Pacific region at the U.S. Naval War College, National Defense University, the U.S. Department of State, U.S. Naval Academy, U.S. Central Command, the U.S. Air Force Air Staff A5/8, the Joint Staff (J5 and J7), the U.S.-China Economic and Security Review Commission, the Air Force Association, and other venues.

As a former U.S. Marine Corps officer, he served in infantry and field artillery units in the 3rd Marine Regiment and commanded a rifle company in the 23rd Marine Regiment. While deployed, he conducted security force assistance activities with host nation and partner military forces in the Western Pacific, East Asia, the Indian Ocean region, and Africa. He served on a battalion staff and participated in the Personnel Reliability Program.

From January 2009 to September 2012, Haddick was the author of "This Week at War," a weekly column on national security affairs for *Foreign Policy*. His column covered the counterinsurgency campaigns in Iraq, Afghanistan, and elsewhere; the Pentagon's budget and reform efforts; the evolution of U.S. military doctrine and operational concepts; and adaptation to emerging security challenges. Simultaneously, Haddick was the managing editor of *Small Wars Journal*, a leading intellectual resource on modern conflict, irregular warfare, and emerging threats.

In the private sector, Haddick was director of research at The Fremont Group, the investment affiliate of Bechtel Corporation. He led Fremont's economic and investment research team, founded and led its proprietary trading unit, led one of Fremont's overseas subsidiaries, and established a trading network that spanned the United States, Europe, Latin America, Asia, and Australia.

Haddick's essays on national security issues have appeared in numerous publications. He has conducted interviews with media outlets such as the BBC, various NPR affiliates, CNBC, and others. Haddick has been a paid adviser to the U.S. State Department, U.S. Central Command, and the National Intelligence Council.

Introduction

The concept of deterrence is central to how U.S. national defense policymakers and planners formulate strategy, design military forces and operational concepts, and strive to prevent conflict and defend U.S. national interests. The website of the U.S. Department of Defense (DOD) states the mission of the department: "The mission of the Department of Defense is to provide the military forces needed to *deter* war and to protect the security of our country [emphasis added]."[1] The 2015 National Military Strategy of the United States declares, "Our Nation requires a U.S. military with the capacity, capability, and readiness to simultaneously defend the homeland; conduct sustained, distributed counterterrorist operations; and, in multiple regions, *deter* aggression and assure allies through forward presence and engagement [emphasis added]."[2] U.S. defense policymakers and planners see deterrence as a key concept for achieving U.S. national security goals.

DOD defines deterrence as, "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits." A deterrent option provided to military commanders or policymakers is, "A course of action, developed on the best economic, diplomatic, and military judgment, designed to dissuade an adversary from a current course of action or contemplated operations."[3]

The concept of deterrence was a cornerstone of U.S. defense planning during the Cold War, when the paramount security challenge was to prevent nuclear or major conventional war against the Soviet Union while also preserving U.S. and allied interests. But, the end of the Cold War in 1991 and the emergence of new irregular threats in recent decades, has required strategists to reexamine the relevance and formulation of legacy deterrence concepts.

In December 2006, the DOD published the Deterrence Operations Joint Operating Concept (DO JOC).[4] This publication, signed by the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the commander of U.S. Strategic Command,[5] described how joint force commanders should apply the principles of deterrence to address challenges future joint forces will face.[6]

Written after 9/11, and while the "War on Terror" was well underway, DO JOC stated,

> In the future joint operating environment, deterrence must address a broader range of potential adversaries and situations than in any previous era of US history. Future deterrent success will be heavily influenced by how potential adversaries perceive US national will and resolve in the face of severe threats across all areas of responsibility (AORs) and the entire range of military operations (ROMO).[7]

DO JOC thus anticipated that deterrence operations would apply not to just nation-state adversaries, but also to non-state actors.[8] In addition, DO JOC stated that a successful deterrence strategy must integrate and bring to bear all elements of national power: diplomatic, information, military, and economic.[9] DO JOC attempted to fashion a more comprehensive concept of deterrence when compared to deterrence as designed and practiced during the height of the Cold War.

DO JOC attempted to anticipate how joint force commanders should prepare for deterrence operations through the year 2025.[10] The publication also anticipated that the U.S. government, the DOD, and joint force commanders would apply its expanded and more comprehensive deterrent principles to a broader range of security problems to include rogue states and non-state actors.[11]

Yet more than a decade after its publication, we can see that policymakers and joint force commanders have failed to, or not attempted to, apply DO JOC's deterrence principles to a variety of security challenges posed by both state and non-state actors. Examples of the shortcomings or irrelevance of DO JOC's precepts include the rise of the Islamic State of Iraq and Syria (ISIS) as both an international and domestic U.S. security problem; Russia's aggression against Ukraine and its threatening posture against NATO allies Estonia, Latvia, and Lithuania; and China's assertive maritime activity in the East and South China Seas. The United States and many of its security partners are now expending substantial resources on these and other similar cases, with active combat operations in the case of ISIS,[12] or attempting to fashion a deterrence position in Eastern Europe.[13] In all of these cases, the legacy, Cold War-era conception of deterrence failed to prevent the emergence of these security problems.

DO JOC defines deterrence operations as:

> operations [that] convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their

> decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.[14]

Deterrence remains a valuable concept for U.S. national security planning and, as stated above, a key organizing concept for policymakers and senior military planners. Effective deterrence will prevent otherwise costly conflicts from occurring. At one extreme in the range of military operations—strategic nuclear conflict—effective deterrence prevents a potentially existential outcome for U.S. society. At the other end of the spectrum, effective deterrence could prospectively avert the costs and consequences of terrorism, the violent or destabilizing activities of transnational criminal organizations, and the subversive consequences of "gray zone" conflicts.

At one extreme in the range of military operations—strategic nuclear conflict—effective deterrence prevents a potentially existential outcome for U.S. society.

Deterrence will continue to be a critical concept for national security planning for the simple reason that policymakers are not likely to find feasible or desirable alternatives. Attempting to remove incipient threats through preventive military action is likely to be impractical against most well-developed adversaries, leaving deterrence as the only realistic alternative. In 2002, the George W. Bush administration proposed preemptive military action as a course to consider against emerging threats for cases where it considered such military action feasible and not likely to be costly.[15] However, subsequent events revealed the forecasting errors that attended the preemption policy, resulting in grave costs that have presumably reduced preemption's appeal to current and prospective policymakers.

Thus, top-level policymakers will continue to rely on deterrence and likely seek to extend its employment to a widening array of security problems, as DO JOC itself anticipated in 2006. If so, it will be incumbent on policymakers and military planners to determine how to make deterrence more effective across the range of prospective security problems. This will mean fashioning a comprehensive range of deterrence operations, activities, and tools that policymakers and planners can assemble to address the wide range of security problems they will face including traditional nuclear-armed and conventional states, as well as rogue states, gray zone challenges, terror organizations, transnational criminal organizations, and other irregular threats.

The shortfall between the application of deterrence principles envisioned by DO JOC and what has subsequently occurred has revealed problems that policymakers and military planners should address. There are at least three reasons why policymakers and planners have failed to apply deterrence principles to hostile non-state actors and nation-states employing gray zone tactics. First, in some cases, these officials have not imagined that deterrence was a relevant conceptual response to the security problems in question.[16] Second, policymakers and planners may have possessed various elements of national power (diplomatic, informational, military, and economic) but chose not to employ them as tools of deterrence because of constraints on their employment or because these tools were not available or fashioned for this use. Finally, officials may have not sought to employ deterrence against certain security problems because they lacked the appropriate tools to do so.

This monograph explains that U.S. Special Operations Forces (USSOF) should play an important role achieving the vision of comprehensive deterrence originally described by DO JOC. Policymakers and planners can employ the unique skills and statutory missions of Special Operations Forces (SOF) as tools of comprehensive deterrence, and by doing so, fill in gaps that legacy tools of deterrence such as nuclear weapons and major conventional forces, cannot fill. The prevalence of hostile non-state actors and the growth of nation-state employment of gray zone tactics are examples of adversary players circumventing legacy deterrence tools as they pursue their objectives. As this monograph will explain, SOF' skills, capabilities, and relationships can add critical competencies to the overall deterrence toolbox available to policymakers and planners.

Attaining this state will require SOF commanders and planners to deliberately position SOF within a larger comprehensive deterrence framework. It, in turn, will require an understanding of how SOF can best contribute to comprehensive deterrence, and then prepare SOF to effectively perform its deterrence tasks. This monograph explains how SOF leaders and planners can prepare SOF to accomplish these deterrence roles and missions.

Chapter 1 describes the characteristics of deterrence theory. Establishing a baseline understanding of deterrence theory, its uses and shortcomings, is critical for orienting the reader for the analyses revealed in subsequent chapters. Chapter 1 draws on classic and contemporary academic sources, DOD doctrinal publications, and practitioner conclusions. The chapter describes the variants of deterrence theory, the theory's assumptions, risks, and the factors that must be present for deterrence to be useful as a policy tool. The chapter will also include critiques of the theory and its practicality.

Chapter 2 discusses the current and emerging security problems U.S. policymakers and military planners face. This chapter will employ a case study approach and the deterrence theory elements established in Chapter 1. Chapter 2 will reveal how current and emerging adversary players have adapted their tactics to circumvent the current limited U.S. deterrence framework. The cases discussed in Chapter 2 will reveal the gaps in the current deterrence framework and the additional tools planners need for a more comprehensive deterrence framework.

Chapter 3 discusses how USSOF can employ its statutory activities, skills, and capabilities to establish effective deterrence against hostile non-state actors. The chapter describes how Israeli conventional military and SOF have built deterrence against highly capable and hostile non-state actors, and examines the lessons from these cases for U.S. policymakers and planners. The chapter references other research on deterring non-state actors and organizations.

Chapter 4 discusses how USSOF can employ its statutory activities, skills, and capabilities to establish effective deterrence against state actors that employ gray zone tactics against U.S. and partner interests. This chapter will draw on research from a variety of sources to explain how SOF capabilities can expand the tools available to planners, fill gaps in the current deterrence framework, and address nation-state gray zone challenges in ways that increase U.S. and partner leverage while controlling conflict risks.

The conclusion draws on the discussions and analyses from the previous chapters and explains how SOF commanders and planners should prepare SOF for comprehensive deterrence roles and missions.

Hostile non-state actors and state actors employing gray zone tactics are imposing costs on the U.S. and its partners and revealing gaps in their military doctrines and theories of deterrence as they do so. The United States and its partners need a more comprehensive approach to deterrence as a realistic and cost-effective response to current and emerging security challenges. SOF can and should make a critical contribution to such a comprehensive national deterrence strategy. When SOF fulfill this role, the United States and its security partners will be in a better position to protect their interests with less risk and lower costs.

Chapter 1. Deterrence Theory: Characteristics, Assumptions, and Shortcomings

As mentioned in the introduction, the DOD's DO JOC defines deterrence as:

> Operations [that] convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.

Deterrence thus seeks to maintain the status quo when the defender dissuades the aggressor from doing something the defender considers harmful to his interests. Deterrence employs the threat of force to influence an adversary's calculations. With deterrence, the defender attempts to convince the aggressor that the defender's capacity for violence is something that the aggressor must reckon with when making his calculations.

Forms of Deterrence

Since it employs the threat of violence, deterrence is one type of coercive strategy. Compellence is another coercive strategy. Deterrence seeks to preserve the status quo by inducing inaction. With compellence, by contrast, the defender employs the threat of force to persuade the aggressor to take actions he would not otherwise perform had the defender not issued his instructions and threats. In contrast to deterrence, compellence actively seeks to change the status quo. All else equal, compellence is likely to be more difficult and require greater levels of threatened force to achieve than deterrence. This is because when an aggressor is compelled to act or change his ongoing actions, perhaps visibly, the reputation of the aggressor and its leaders are more exposed than in the case of deterrence, when non-action is less likely to have reputational costs.[17] With compellence, the aggressor's level of resistance to persuasion is likely to be higher, requiring more forceful threats, and presumably attendant risk-taking, by the defender.

The beginning of Operation Desert Shield, in August-September 1990, offers an illustration of the differences between deterrence and compellence. After the Iraqi army overran Kuwait in early August 1990, the United States and other partners rushed military forces to northern Saudi Arabia. The initial purpose of these deployments was to deter a possible Iraqi invasion of Saudi Arabia. Iraq did not subsequently invade Saudi Arabia during the remainder of 1990 and did not appear to suffer reputational damage for not doing so. By contrast, subsequent coalition threats to employ force to compel Iraq to voluntarily abandon Kuwait would have been much damaging to Iraq's reputation and, unsurprisingly, were rejected by Iraq. A debate over whether the coalition deployment effectively deterred Iraq from invading Saudi Arabia or whether Iraq had no intention of invading only support the argument that the aggressor can better avoid reputational costs when deterred, as compared to compelled.

Denial Versus Punishment

There are two forms of deterrence: deterrence by denial, and deterrence by punishment. With deterrence by denial, the defender employs the threat of force to convince the aggressor that the defender's military power will deny the aggressor the objective he might seek, usually through the defender's convincing threat to destroy the aggressor's military forces should he attempt to use them. With deterrence by punishment, the defender threatens to inflict costs and pain on the aggressor, and perhaps his associates and society, should the aggressor attempt actions against the defender's interests.[18]

Deterrence by denial is a stronger form of deterrence than deterrence by punishment.[19] When able to execute deterrence by denial, the defender is in greater control and leaves very little for the aggressor to decide other than to respect the status quo. This would be the case when the defender's military forces can defeat the aggressor should the aggressor defy the defender by acting. With deterrence by punishment, the aggressor will get a chance to determine how much punishment he is willing to suffer before complying with the defender's demands. It may be the case that the aggressor is willing to withstand more punishment than the defender is willing or able to inflict. During the Vietnam War, U.S. officials hoped that Operation Rolling

Thunder, a two-year bombing campaign of North Vietnam, would induce compliance by the North Vietnamese government. However, the pain tolerance of the North's leadership exceeded what U.S. policymakers were willing or able to inflict with the bombing campaign.

In spite of policymakers' understandable preference for deterrence by denial, circumstances may prevent denial from being a realistic deterrent option. During the early stages of the Cold War, the United States and its NATO allies were unwilling to match the Soviet Union's conventional military forces then arrayed against Western Europe. The Dwight D. Eisenhower administration's "New Look" policy and its reliance on massive retaliation with nuclear weapons is a classic example of deterrence by punishment, employed as an alternative to deterrence by denial, which policymakers at that time considered a prohibitively expensive course of action.[20]

Deterrence can be immediate or general. Immediate deterrence occurs when the defender generates deterrent responses in reaction to specific indications and warning of impending actions by the aggressor.[21] The aforementioned rapid deployment of coalition military forces to Saudi Arabia in August 1990 in response to Iraqi's conquest of Kuwait, with the goal of deterring another move south by Iraqi forces, is an example of immediate deterrence. Another type of immediate deterrence would be specific contingency plans designed as a deterrent signal against a known threat. The U.S. military's Return of Forces to Germany (REFORGER) exercises during the late Cold War period rapidly transferred U.S. Army personnel to meet up with prepositioned equipment stored in Germany.[22] REFORGER was a form of immediate deterrence since it was designed to deter a specific threat, that of a Warsaw Pact assault across the inter-German border.

General deterrence refers to a broader, non-specific perception by the aggressor that aggression against the defender's interests will either be thwarted (general deterrence by denial) or will result in unspecified yet unacceptable pain (general deterrence by punishment). With general deterrence established, it is not necessary for the defender to state specific conditions, threats, or deterrent actions. The defender's reputation, and perhaps an imbalance of military power among the players, are sufficient to generate a broad climate of deterrence.[23]

Policymakers will likely prefer establishing the conditions for general deterrence. Players can use instances of immediate deterrent responses during crises to establish the broader reputational conditions for general deterrence. For example, the acumen displayed by Israel's conventional forces between 1948 and 1973 resulted in the establishment of general deterrence with respect to Israel's nation-state adversaries. Indeed, Israel signed peace treaties with Egypt and Jordan in the years after the 1973 war, and there has been no major conventional ground combat with Syria since 1973.

Components of Deterrence

Deterrence must exist inside the mind of the adversary. The task for the defender is to convince the aggressor that his contemplated aggression either will fail, or result in unacceptable pain. In his 1960 book *The Necessity for Choice: Prospects of American Foreign Policy*, former Secretary of State Henry Kissinger proposed deterrence as the product of the defender's capabilities and will, and the aggressor's belief in those components.

Deterrence = capability x will x belief

Should any of the three components equal zero, deterrence will not exist.[24]

To establish and strengthen deterrence, the defender will seek to increase the value of each of the three components. But, that is not enough. Deterrence will succeed only when the aggressor's estimation of these values also goes up (the focus of the third factor, belief). The defender's task is to strengthen each component, communicate that strengthening to the aggressor, and ensure that he has received and understands the messages.

Capabilities

The capabilities component can refer to all the instruments of national power (diplomacy, information, military, and economic) a defender might be able to employ as coercive leverage against an aggressor. In order for a capability to function as a deterrent, the defender must not only develop the capability, he must also display it to potential aggressors. For example, the atmospheric testing of nuclear weapons conducted by the United States and the Soviet Union from 1945 to 1963 left no doubt about these weapons as effective tools of deterrence.

By contrast, the potential of offensive cyber weapons employed by the United States or other players as effective tools of deterrence has not achieved the same clarity that nuclear weapons achieved in the 1950s. The United

States government has yet to openly demonstrate an offensive cyber application against an adversary's military forces, governmental institutions, or national infrastructure. The United States may have clandestinely employed such weapons. But clandestine employment of any capability does nothing for general deterrence. Observers are left to question the nature of this purported capability, its forcefulness, and policymakers' will to employ such weapons.

To deter determined adversaries, the defender will have an interest in visibly demonstrating his coercive capabilities. In peacetime, and with respect to capabilities at the high end of military operations, the best the defender may be able to manage is demonstrations at formal trainings exercises. Such scripted events may not be convincing to certain adversaries and may instead reveal ways for the adversary to thwart the capabilities' intended effects, producing the opposite of the intended deterrent result. Since it ceased full power testing in 1992, the United States can no longer demonstrate its nuclear weapons capabilities, except by conjuring the memories of the testing era. As just mentioned, the United States government has displayed a reticence to demonstrate its purported offensive cyber warfare capabilities. Thus, in many cases, capability demonstrations will not be feasible, they might strain the limits of morality, or they would reveal military secrets that commanders and planners might prefer to reserve for other contingencies.

Will

Next, after developing useful capabilities, the defender must convince potential aggressors of their willingness to employ them.

A player's will to employ coercive capabilities is likely correlated to the value the player attaches to the deterrent objective he seeks. During the Cold War, both the United States and the Soviet Union sought to display a high willingness to employ nuclear weapons as deterrents when the stake for each was national survival. Similarly, during this same period the NATO alliance, through its deployments and training exercises, attempted to demonstrate its willingness to employ tactical nuclear weapons as part of its defense doctrine to deter the Warsaw Pact's conventional numerical superiority.

Employing capabilities, whether military or nonmilitary, usually requires a player to pay some cost for doing so. That cost could be financial, physical (through the exposure to military retaliation), diplomatic, or moral. These costs and their attendant risks can temper a player's will and are subject to an adversary's manipulation.

Uncertainty will attend to the values a player assigns to these parameters. That uncertainty can create questions about a player's credibility, or what his true willingness is to implement deterrent courses of action, compared to what the player has stated publicly. Scenario context can further complicate calculations of will and credibility. Depending on the situation, a player may want to reduce uncertainty to boost the appearance of will. In another context, the player may wish to increase uncertainty, in order to allow greater flexibility and perhaps a face-saving disengagement from the crisis.[25]

A player's history of decision-making during crises accumulate to establish the player's reputation. Reputation has been a cornerstone, albeit a disputed one, of deterrence theory. In his *History of the Peloponnesian War*, Thucydides asserted that fear, honor, and interest were the reasons statesmen chose war, with the protection of one's reputation a great part of honor as a reason for committing to war.

Twenty-five centuries later, U.S. President George H.W. Bush saw reputation, and a version of Thucydides' logic, animating one of his rationales for the military campaign to eject the Iraqi army from Kuwait. Bush believed that visibly routing the Iraqi army in Kuwait offered a chance to impress the rest of the neighborhood, and indeed adversaries everywhere, with U.S. military capabilities. He believed a decisive display would reinforce deterrence generally, enhancing stability, and creating "a better peace."[26]

Following through on threats and commitments to protect a player's reputation entails taking risks, which can turn out badly. An internal U.S. Department of Defense memo to Secretary of Defense Robert McNamara dated 24 March 1965 (just after the initial commitment of U.S. conventional ground forces to South Vietnam) asserted that 70 percent of the U.S. aim for its emerging commitment to the war was to avoid a humiliating defeat and to protect the U.S. reputation as a reliable security guarantor.[27] It is arguable that when the United States had to subsequently withdraw from the war without having achieved its principal aims, and with its policymakers and the U.S. public less willing to support new defense commitments elsewhere in the world, the failed intervention in Vietnam had left the perception of U.S. will reduced from where it would have been had U.S. policymakers instead passed on escalation in Vietnam in 1965.

International relations scholars do not agree on the efficacy of reputation with respect to effective deterrence. Establishing a reputation for always following through on threats may not alone be enough to compel compliance by subsequent adversaries.[28] On the other hand, failing to follow through on threats may, as expected, result in more challenges to the irresolute actor.[29] Taken together, these two academic views suggest that squandering a reputation can be costly, but a reputation for always following through is no guarantee of subsequent success with coercive strategies.

Demonstrating will to current and prospective adversaries is easy when the costs of doing so are low. Airpower-centered strategies are relatively cheap for U.S. policymakers to implement, which may explain why they are so frequently employed. However, the usefulness of airpower-centered strategies for deterrence will depend on the extent to which they will be effective at coercing specific actors in specific circumstances, combined with the adversary's perception of their effectiveness.

If the defender concludes that more costly (for them) courses of action will be required to demonstrate effectiveness, questions about credibility will grow. President Eisenhower administration's massive retaliation nuclear strategy was at first a low-cost and seemingly credible approach, when the United States enjoyed a virtual nuclear monopoly compared to the Soviet Union. But once the Soviet Union developed its own nuclear retaliatory capability, the credibility of massive retaliation came into question. Observers began to doubt that U.S. leaders would have the will to implement a strategy that would result in retaliatory devastation. Needing new approaches that were more credible, and that thus would allow an increase in the "will" component in Secretary Kissinger's equation, the succeeding Kennedy administration soon implemented "flexible response" and counterforce targeting as replacements for massive retaliation.[30]

Policymakers will apply constant pressure on the military services, acquisition officials, and war planners to come up with new weapons, tactics, and operational concepts that will allow them to employ coercive strategies at low costs for themselves. When these pressures for low-cost courses of action reach their limits, policymakers may be compelled to demonstrate their willingness to suffer the higher costs that effective deterrence strategies may require.

The NATO alliance's recent decision to deploy four battalions of ground troops to the Baltic states of Estonia, Latvia, and Lithuania, plus Poland, is an attempt to demonstrative deterrent will.[31] Few analysts believe such relatively small military units could hold out long against much larger Russian military forces that could be available in the Baltic region. NATO policymakers believe such a symbolic "tripwire"—the prospective visible sacrifice of alliance soldiers—would be sufficient to trigger a more costly conflict for both sides incurring prospective costs that are intended to deter possible Russian aggression.

Adversary Belief

Finally, prospective aggressors need to accurately receive, understand, and believe a defender's deterrent message—the third component of Secretary Kissinger's equation. Achieving a belief in the mind of the adversary is not always simple.

For example, the defender may not be fully aware who his adversaries are and who should receive the deterrent message, either because the defender is unaware of a particular threat or because the key decision-makers behind that threat are unknown.[32] If the defender knows the potential threat and its decision makers, cultural or language barriers may prevent his deterrent message from getting through to the adversary's decision makers.[33] The defender might not understand the cultural context in which an aggressor operates, or his motivations, interests, and values. If so, the defender will likely struggle to formulate a coercive threat that will matter to the aggressor.

What Deterrence Requires for Success

Even when the defender, following Secretary Kissinger's formula, has developed coercive capabilities, displayed his will to employ them, and persuaded potential aggressors, successful deterrence still requires many additional requirements for success.

Deterrence theory rests on several assumptions. When these are not present, deterrence could fail to restrain an aggressor's behavior. Deterrence theory assumes that the aggressor evaluates his alternatives in a logical manner and that the defender can accurately determine the aggressor's interests and his rational approach to decision-making. The theory further assumes that the aggressor's subsequent decisions come from decision makers that a certain player communicates with and has targeted for coercive influence, and that the aggressor's actions are not the result of automatic, unintended, or random processes.[34]

Deterrence theory assumes that the aggressor has assets or conditions he values and that the defender has coercive capabilities that can hold these assets and conditions at risk. The nature and level of commitment the aggressor holds to his interests is likely to be dynamic and will swing during the course of a prospective crisis. The theory assumes that the defender recognizes these changes and can adjust his tactics as required in response to the aggressor's fluctuating levels of resistance and calculations.[35]

This list of assumptions and conditions complicate the task of successfully implementing an effective deterrence strategy. For a player like the United States, with global interests, policymakers and planners must multiply the complications contained in this list by the number of potential adversaries they must plan for, each with its own culture, interests, and characteristics. Policymakers and planners will have to customize deterrence strategies for each, with each requiring its own analysis, coercive tools, and communication approaches.

Planning Deterrence Operations

DO JOC includes a checklist for joint force commanders planning deterrence operations.[36] The checklist is a familiar adaptation of operational planning routines, and is directed toward cases of immediate deterrence for specific situations, rather than for constructing a broad environment of general deterrence.

According to DO JOC, deterrent operation planners should begin by specifying the discrete objectives of the deterrence operation. This should take the form of "deter adversary X from taking action Y under conditions Z."[37] Next the deterrent planner should undertake an assessment of the adversary's decision calculus. This entails determining the factors that influence the adversary's evaluation of costs, benefits, and risks (such as the assets and conditions the adversary highly values) and how the adversary processes those factors in making his judgments about costs, benefits, and risks. The planner needs to evaluate his own uncertainties about his assessment of the adversary and his thinking, and incorporate those uncertainties into the subsequent steps in the planning process.[38]

Equipped with an assessment of the adversary's interests and decision process, the planner can then determine which variables in the adversary's decision process are most opportune for influence, either because they powerfully influence the adversary, because they are accessible to the planner's tools of leverage, or both. After the planner has determined the variables he plans to influence (which might also be described as a theory of success), the planner can then develop courses of action that will apply elements of national power (or tools of coercion) to the variables that influence the adversary's calculations. The final step is executing chosen courses of action and evaluating their effects.[39]

This simple process is likely familiar to military planners. But to paraphrase Clausewitz, simple does not mean easy, and, as with all military planning, there is much that can go wrong. For example, the planner, in specifying his objectives ("deter adversary X from taking action Y under conditions Z") may miss other options available to X, or other threats from other sources. Next, it may be impossible to develop a useful assessment of the adversary's perception of his costs, benefits, and risks because much of the needed data will be inaccessible, hidden inside the adversary's mind. For the same reason, the planner may not be able to determine the variables that are most influential on the adversary, or the planner may lack the capability to influence those variables.

Finally, in many cases it will not be possible to determine whether the implemented courses of action actually deterred the adversary. This is due to a paradox of deterrence; deterrence is a negative act in that it refers to an event that has not occurred. It will rarely be the case that an aggressor openly admits to a defender that he was deterred by the defender's coercion. It is a logical conundrum to prove a negative—the event that didn't happen. This conundrum continues to hang over the concept of deterrence, leading some critics to wonder whether policymakers are wise to rely on the concept.[40]

It will rarely be the case that an aggressor openly admits to a defender that he was deterred by the defender's coercion.

Capabilities Required for Deterrence Operations

Such misgivings notwithstanding, the DOD's joint operations concept for deterrence operations describes numerous capabilities joint force commanders should possess to implement deterrence operations. The concept sorts this list into direct capabilities and enabling capabilities.

Direct capabilities employed for deterrence include:

- Global strike operations (nuclear, conventional, non-kinetic, and special operations surgical strike);
- Force projection operations (including the capability to decisively defeat regional aggression);
- Active and passive defense operations (such as missile defense and base hardening); and
- Strategic communications (employed to rally regional supporters and demoralize the adversary and their supporters).

Enabling capabilities include:

- Command and control;
- Global situational awareness (intelligence, surveillance, and reconnaissance in all its forms); and
- Forward presence, security cooperation, and deterrence assessment and experimentation.[41]

The DO JOC's list of required capabilities overlaps completely with the DOD's broad list of capabilities that it develops and maintains for all its operations and responsibilities. In this sense, the vast majority of capabilities the DOD invests in could have applications directly or indirectly for deterrence operations. It will be up to policymakers, planners, and joint force commanders to create ways to apply the DOD's broad portfolio of capabilities to ongoing and prospective deterrence missions.

In its description of these direct and enabling capabilities (or means), DO JOC explains how each can support both deterrence by denial and deterrence by punishment—the two principal ways of executing deterrence operations.[42] In reality, the vast majority of these capabilities have been designed and fielded for conventional military operations which are almost always focused on defeating opposing military forces (conventional or irregular). These preponderant capabilities are thus designed for deterrence by denial.

The DOD's investment in strategic nuclear forces clearly supports the deterrence by punishment approach, but spending on such forces will amount to about five percent of the DOD's budget over the next decade.[43] The configuration of U.S. defense spending, heavily weighted toward conventional and enabling capabilities, supports the notion that U.S. policymakers and defense planners prefer deterrence by denial, as deterrence theory suggests. They expect that the first mission of U.S. military forces is to deny adversary forces their military objectives, with the strategic nuclear forces both a notable exception and a small fraction of defense investments.

Shortfalls in Applying Deterrence Capabilities

DO JOC, written during the height of counterinsurgency and counterterror operations in the United States Central Command area of responsibility, attempted to broaden the application of deterrence theory to address threats from hostile non-state actors.[44] However, the United States and its security partners have fallen short on this particular aspiration, for reasons explained in the next chapter.

DO JOC anticipated the difficulties policymakers would face applying the tenets of deterrence theory to non-state actors. But, in spite of these challenges, the next chapter will show that policymakers have not employed deterrence capabilities and concepts as fully as they could have against non-state actor threats. In particular, policymakers have not fully employed SOF as a tool of deterrence against hostile non-state actors. USSOF have been very active against a variety of hostile non-state actors since DO JOC's release in 2006. But in spite of this activity, policymakers and planners have not capitalized on SOF' potential as a tool of deterrence, as the remainder of this monograph will discuss.

Even more notable was DO JOC's failure to anticipate how well-established and near-peer state actors like Russia and China would use "gray zone" and "hybrid warfare" tactics to bypass the legacy construct of deterrence the U.S. had established during the Cold War to counter nuclear and large-scale conventional warfare threats. DO JOC included a vignette that discussed how to apply deterrence operations against a regional rogue state plotting both a major conventional attack and the use of a biological weapon.[45]

But DO JOC did not anticipate Russia's use of "little green men" (disguised Russian SOF) in Crimea, or China's employment of quasi-civilian maritime militia and paramilitary maritime forces in the East and South China Seas. In these cases, Russia and China devised offensive military capabilities that have successfully seized territory, and bypassed legacy deterrence structures as they did so.

Thus, we can see that in spite of DO JOC's attempt a decade ago to broaden thinking about deterrence, the legacy structure of U.S. deterrence planning remains narrow, fragmented, and fixated on deterring nuclear and major conventional conflicts. U.S. policymakers and planners have failed to apply deterrence concepts to comprehensively cover the entire range of military threats and operations.

State and non-state adversaries are exploiting the gaps that exist in the fragmented legacy deterrence structure. As the remainder of this monograph will discuss, U.S. and partner SOF will have fundamental roles to play filling these gaps and fashioning a more comprehensive approach to deterrence that will address the entire range of security challenges.

Chapter 2. How Adversaries Have Bypassed the Legacy Deterrence Structure

This chapter applies the tenets of deterrence theory discussed in chapter 1 to examine how recent and current state and non-state security challengers—al-Qaeda, Iran, Russia, and China—have fashioned and executed strategies that have bypassed or ignored the legacy U.S. deterrence structure by exploiting gaps in that structure. These gaps, at least initially, limited the effectiveness of U.S. and partner responses to the offensive actions of these adversaries. Adversary confidence in these limitations on U.S. response effectiveness negated any perception of U.S. general deterrence, allowing the adversaries to execute their offensive operations.

The chapter employs a brief case study approach to examine how each adversary exploited gaps in the U.S. legacy deterrence structure. Summing the results of the four cases will reveal the gaps recent and current adversaries are exploiting and result in a diagnosis of the problem U.S. policymakers and planners will experience applying deterrence concepts to these types of challengers. Succeeding chapters in the monograph will explain the roles SOF can play addressing this diagnosis and thus increasing the relevance of deterrence against these and similar threats.

How to Bypass the Legacy U.S. Deterrence Structure

Chapter 1 discusses the components of deterrence theory (per Secretary Kissinger, the components are capability, will, and the adversary's belief in these components). Chapter 1 also discussed deterrence theory's underlying assumptions. By re-examining the theory's components and assumptions, an adversary might formulate approaches that will thwart or bypass a deterrence operation. This section will discuss possible negation tactics, working from the discussion in chapter 1.

Negate the Defender's Deterrence Capabilities

The first component in Secretary Kissinger's deterrence formula is the defender's capability to either defeat the aggressor's prospective aggression (using deterrence by denial) or inflict unbearable pain on the aggressor and his supporting establishment (employing deterrence by punishment). There are several approaches an aggressor could pursue to negate a defender's deterrent capabilities.

The first and most obvious approach is for the aggressor to acquire relevant and sufficient defensive capabilities that are designed to thwart the capabilities the defender intends to use as a retaliatory deterrent. Defensive measures could be active, such as integrated air and missile defense systems and anti-submarine systems, or passive measures such as hardening or dispersion of critical assets. Effective defense measures such as these are typically expensive to acquire. An aggressor would normally require wealth, access to engineering talent, and the utilization of capable high-end military forces to effectively employ these approaches against a well-endowed opponent.

If the aggressor lacks wealth and high-end military capacities, he still has techniques he might employ to negate a defender's deterrent capabilities. One such approach is to refrain as much as possible from possessing assets that the defender could target with his retaliatory capabilities. If the defender cannot find anything to threaten, he might not be able to obtain coercive leverage. For the aggressor, this would mean avoiding the acquisition of fixed or visible military assets or financial accounts the defender might be able to find, sanction, or destroy. This approach would also likely require the aggressor to perpetually hide its top leaders to avoid targeting by the defender.

Chapter 1 discussed the defender's deterrence planning process. A key early step in this process is collecting information on the aggressor and forming an intelligence assessment to determine what assets and conditions the aggressor values, understanding his culture context and perspective, and discerning his decision-making process and calculus. The aggressor could attempt to thwart the defender's intelligence assessment process by taking measures to obscure the critical elements of intelligence the defender will require. The more the aggressor remains a mystery, the less confidence the defender will have in any prospective deterrence strategy.

Negate or Diminish the Defender's Will

Secretary Kissinger's second component was the defender's willingness to employ his deterrent capabilities against the aggressor and pay physical, financial, political, and moral costs for doing so. A player's will is a function of the value he assigns to a deterrence objective minus the costs he will have to pay for employing deterrence capabilities to achieve that objective.

There are a variety of measures an aggressor can employ to manipulate the value of these parameters, with a goal of reducing the defender's will to employ his coercive capabilities.

A player's will is a function of the value he assigns to a deterrence objective minus the costs he will have to pay for employing deterrence capabilities to achieve that objective.

Retaliation. An aggressor can diminish a defender's will by threatening his own retaliation in response to the defender's prospective coercion. The threat of retaliation will raise the defender's costs, and presumably his will to follow through on his deterrent coercion. During the October 1973 Arab-Israeli war, the Soviet Union threatened military intervention in the conflict in an attempt to coerce Israeli military decision-making and U.S. logistic support to Israel, which at the moment was routing the Egyptian and Syrian forces, clients of the Soviets. The United States responded by placing its nuclear forces on heightened alert, threatening high costs against prospective Soviet actions. Soviet military intervention subsequently did not occur. Raising the cost of coercion lowered the will of Soviet leaders to follow through with their coercive threat.

Ambiguous aggression. An aggressor might avoid triggering the defender's deterrent threat by disguising his aggression or implementing it in an ambiguous or deceptive manner. Students of U.S. history know how dramatic and highly visible *casus belli* such as the Confederate bombardment of Fort Sumter in April 1861, the explosion inside USS *Maine* in February 1898, the Japanese air raid on Pearl Harbor in December 1941, and al-Qaeda's attacks in September 2001, triggered public reactions and the necessity for policymakers to execute substantial military responses. By contrast, some aggressors may seek to achieve their goals in a manner that does not trigger the sharp escalation promised by a defender's deterrent threat. In these cases, an aggressor will attempt to implement his aggression below the threshold that will trigger a defender's political response.

An aggressor may have several techniques available for operating below a defender's response threshold. One method is termed "salami slicing"—the slow accumulation of small gains, each of which appears too inconsequential to trigger action (and its attendant costs), but that sum over time to a substantial geostrategic change.[46]

An aggressor may also pursue aggression by employing proxies. This technique could mask attribution of the principal aggressor. With attribution of aggression ambiguous, a defender may have difficulty achieving consensus among his policymakers or public to implement promised deterrent actions.

Negate the Aggressor's Belief or Understanding of the Defender's Deterrent Threat

Finally, an aggressor can flummox the defender's deterrence strategy by creating doubts about whether the defender's deterrent message has been understood by the aggressor. The defender may possess the capability and will to impose coercion on an aggressor. But, if the defender harbors substantial doubts about whether an aggressor understands his coercive threat, he might doubt whether he has actually deterred the aggressor. In that case, the defender might have to pay the full price of either defeating the aggressor and his strategy or of inflicting punishment on him when the aggressor acts. Deterrence would have failed to prevent conflict because all three of its required components had not been established.

An aggressor can create doubts about his understanding of a defender's threats by obscuring the identities of its leaders. If a defender never identifies the target of his coercive message, he won't have confidence the message was received and understood. An aggressor can also attempt to present a cultural context alien to the defender's frame of reference, to a degree that creates doubts about whether the defender's coercive message can effectively translate across the cultural divide.[47] Finally, the aggressor can attempt to demonstrate to the defender that he and his colleagues in the leadership are not sufficiently in control over the responses that will occur if the defender implements his coercive threats. Such would be the case if the aggressor's military forces did not operate under strict top-down command, if communication links to subordinate leaders were weak or missing, or if the aggressor's forces were purposely organized in an autonomous cellular structure.[48]

An aggressor can employ any of these technique: avoiding the defender's capabilities, threatening retaliation, creating ambiguity, and creating doubts about whether the defender's coercive message has been received, to undermine the defender's attempts to create effective deterrence. The following short case studies show how contemporary players, all current challengers to U.S. security interests, have employed these techniques to undermine the legacy U.S. deterrence structure.

U.S. policymakers should have a strong interest in fashioning a broad, comprehensive deterrence structure that will be effective across the range of military operations and potential adversaries. The alternative to creating such a deterrent structure would necessitate an engagement in a series of costly military campaigns against adversaries who are not otherwise deterred, or sacrificing important national security interests to those adversaries. As the following chapters explain, U.S. and partner SOF play important roles in building a more comprehensive and effective deterrent structure.

Case studies

The following brief case studies reveal how recent state and non-state adversaries have employed some of the techniques explained earlier in this chapter to circumvent the U.S. legacy deterrence structure. Understanding how adversaries have exploited gaps in U.S. deterrence is critical to diagnosing the problems with the legacy structure. After completing an analysis, deterrence planners will be better positioned to formulate a broader and more comprehensive deterrence structure.

Understanding how adversaries have exploited gaps in U.S. deterrence is critical to diagnosing the problems with the legacy structure.

Al-Qaeda. Al-Qaeda has employed several of the deterrence negation techniques described in this chapter. The terror organization attempted to thwart U.S. global strike capabilities by minimizing its acquisition of targetable assets and facilities. The facilities they had early on (before September 2001), such as a few small training sites in Afghanistan, were remote and difficult for U.S. military forces to find, track, and target with real-time intelligence, given U.S. military technology at the time.[49] If U.S. forces struck the training camps preemptively, al-Qaeda could have easily replaced them. And when the U.S. finally struck these camps with airpower in October 2001, al-Qaeda had abandoned them.

Al-Qaeda's financial assets were limited and its operations did not require much funding; according to the 9/11 Commission, the September 2001 attacks in the United States cost al-Qaeda between $400,000 and $500,000.[50] This made it difficult for U.S. and partner financial authorities to target the group's financial resources with sanctions, freezes, or restrictions. Al- Qaeda made use of covert third-party accounts for the few transactions it needed to perform, employed couriers, or informal money transfer arrangements such as *hawala* to transfer funds.[51]

Al-Qaeda's most important asset, and arguably its critical center of gravity, was its core leadership. The group avoided U.S. and partner deterrent capabilities by living in remote terrain and hiding among a local population friendly to them and hostile to the West. This allowed the group to avoid U.S. military reconnaissance and firepower, at least in the early years of the conflict. It would take the United States many years and a great interagency effort to build up the regional intelligence and surgical strike capabilities needed to find and kill Osama bin Laden, al-Qaeda's top leader.

By minimizing its assets and hiding the little it possessed, al-Qaeda, at least in its early years, was able to negate much of the deterrent capabilities possessed by the United States and its security partners.

Next, al-Qaeda employed secrecy to hinder the effort of the U.S. intelligence community to understand the structure and motivations of the organization. As explained in chapter 1, an effective deterrence strategy requires understanding these and other characteristics of the adversary in order to fashion a deterrent approach that will alter the behavior of the target. Al-Qaeda's secrecy, along with its professed cultural alienation, complicated the task for Western policymakers and analysts of understanding its organization and motivations.

Without this knowledge, deterrence planners faced great difficulty fashioning an approach to deterrence. After the September 2001 attacks, U.S. policymakers sought al-Qaeda's destruction, not its deterrence, and resolved to pay the cost that such a long military campaign would require. Al-Qaeda's secrecy and cultural alienation greatly diminished the prospects of developing an effective Western deterrence against the group.

Iran. Over the past three decades, Iran has employed most of the deterrence negation techniques described in this chapter. Iran's diminishment or negation of U.S. deterrent efforts has allowed it to pursue a consistent anti-U.S. strategy (to include several large-scale acts of violence against U.S. military personnel) while largely avoiding U.S. retaliation.

Since 1979, the United States has imposed economic and financial sanctions on Iran, and convinced European countries and others to join in the sanctions, to create leverage during the negotiations for the Joint Comprehensive Plan of Action that sought to limit Iran's nuclear program.[52]

But these coercive measures show a failure of deterrence in at least two respects. First, the fact that the United States and others had to apply economic and financial coercion indicates that the prior threat of imposing those measures failed to modify Iranian behavior in ways the United States wanted. Second, according to the U.S. Department of State, Iran continues to be a malevolent actor against U.S. interests (Iran is one of three countries designated by the U.S. government as a state sponsor of terrorism), another indicator that U.S. deterrent threats are not wholly succeeding.[53]

Iran has strived to improve its integrated air defenses, with a goal of increasing the costs the United States or Israel would have to pay for a prospective air campaign against Iranian assets. With a sustained effort, there is little doubt that U.S. military forces would be able to break down Iran's air defenses and thus open the way for airstrikes on targets valuable to the Iranian government. Yet by making such a prospective operation more costly, and thus giving pause to U.S. policymakers hypothetically considering such an option, Iran's efforts to improve its air defenses have likely reduced the value of coercive airpower as a means of U.S. deterrence.

Over the past three decades, Iran has taken several active and passive measures to increase the cost of a prospective adversary air campaign. For example, it has taken advantage of dispersion, concealment, and hardening of numerous facilities in its nuclear program. The Natanz uranium enrichment plant consists of three underground buildings, constructed under 70 feet of steel-reinforced concrete, while the Fordow fuel enrichment plant was built into a mountain to protect it from a bombing.[54] Dispersion, redundancy, and hardening would greatly raise the cost of a prospective air campaign, perhaps enough to dissuade policymakers from choosing such an option.

Iran has maintained and strengthened its active air defenses, presumably with the same goal in mind. The country has retained in service its fleet of F-14 interceptor aircraft, which were acquired from the United States before the Islamic revolution in 1978.[55] These aircraft are armed with the AIM-54A Phoenix missile, which despite its age, is still one of the longest-ranged air-to-air missiles in the world.[56] More recently, Iran has received the modern Russian S-300 surface-to-air missile system—a capability that will greatly complicate adversary air campaign planning.[57] Thus, Iran has taken both active and passive defensive measures in an attempt to counter adversary deterrent capabilities.

Iran has employed techniques designed to reduce the will of adversaries like the United States to employ its deterrent capabilities. It has used the threat of retaliation, presumably to be executed by terrorist proxies it is thought to control, in an effort to dissuade U.S. policymakers, and those from other adversaries, from following through on their deterrent threats.[58] Iran's capacity to employ local proxies to harm U.S. personnel abroad has affected the calculations of U.S. policymakers.[59]

Iran has employed proxy military forces in several cases to mask its identity as the principal aggressor. The use of proxy forces has allowed Iran to deliver attacks against targets of opportunity while also obscuring and delaying attribution and immediate culpability for the attack. In this manner, Iran has inflicted damage on adversaries and avoided a "Pearl Harbor" type cultural response from adversaries that would have sparked large-scale military retaliation against Iran proper. Iran has thus successfully used ambiguous attribution to negate adversary general deterrence.

Iran has employed this technique to undermine U.S. general deterrence. Iran used proxies to strike U.S. targets of opportunity and avoided U.S. military retaliation against the Iranian homeland. In 1996, a truck bomb destroyed Khobar Towers, an eight-story building in Saudi Arabia that housed U.S. Air Force personnel. Nineteen U.S. airmen were killed in the attack and another 400 people were injured. An investigation into the attack, which was hampered by disagreements between U.S. and Saudi authorities, took five years to return a U.S. criminal indictment against Ahmed al-Mughassil, a senior leader of Hezbollah al-Hijaz. In 2006, a full decade after the attack, a U.S. district court judge concluded that Hezbollah al-Hijaz was a proxy of Iran. The judge levied a $254 million judgment against the government of Iran for the Khobar Tower attack.[60] According to Kenneth Pollack, a National Security Council staff member in the Clinton administration, the confusion and delay over determining attribution for the Khobar Towers attack dissipated the political urgency for retaliation—a decision the Clinton administration ultimately avoided taking.[61]

During the U.S. counterinsurgency campaign in Iraq, Iran again employed proxy militias to opportunistically attack U.S. forces. Shiite militias, supported and in some cases directed by Iran, attacked U.S. military personnel in Iraq with rockets and improvised explosive devices. As an example, in June 2011, 15 U.S. soldiers were killed in eastern Baghdad by Iranian-supported militias. General James Mattis, United States Marine Corp, then commander of U.S. Central Command, recommended military retaliation against Iran proper. However, officials in the Obama administration's national security staff argued that U.S. military action inside Iran risked an escalating conflict and Iranian retaliation, in response to attacks whose attribution was murky. U.S. military forces took action against Iran's proxies inside Iraq, which caused attacks on U.S. forces to subside. But in the view of other officials, the lack of response against Iran proper undermined U.S. general deterrence.[62]

These two instances of Iran's use of ambiguous attribution—the 1996 Khobar Towers attack and Iran's long proxy campaign in Iraq—show how Iran obscured culpability for attacks on U.S. personnel to avoid triggering U.S. retaliation, which would have been more likely had attribution been publicly clear immediately after the attacks occurred. Iran, thus, successfully used ambiguity to negate U.S. general deterrence.

Russia. Russia inherited the vast majority of the Soviet Union's nuclear weapons and still maintains the world's largest inventory of nuclear weapons.[63] This inheritance meant that Russia and the United States would continue the mutual strategic nuclear deterrence posture that had existed prior to the Soviet Union's dissolution in December 1991.

But, in spite of the continuation of deterrence at the strategic and tactical nuclear levels, Russia has employed several of the techniques described in this chapter to execute forms of offensive operations that have bypassed or negated possible U.S. or NATO hopes for establishing general deterrence regarding security interests in Eastern Europe. As a result, Russia was able to seize portions of the Republic of Georgia in August 2008, Crimea, and portions of eastern Ukraine during the first half of 2014. Top NATO policymakers and many of its member states are now concerned about the possibility of Russia employing similar techniques against NATO members Lithuania, Latvia, and Estonia.

Top NATO policymakers and many of its member states are now concerned about the possibility of Russia employing similar techniques against NATO members Lithuania, Latvia, and Estonia.

The first and most obvious negation technique employed by Russia is the threat of retaliation should the United States or others follow through on explicit or implied deterrent threats. As mentioned, Russia retains a large and diversified nuclear weapons inventory and these weapons appear to play an increasingly important role in Russia's military doctrine. Statements by Russian policymakers about the roles of nuclear weapons in Russia's military doctrine seem explicitly designed to temper the calculations of potential adversaries.[64] The goal is to negate adversary deterrent will.

Some aspects of Russian conventional military modernization are likewise aimed at raising the costs of prospective adversary deterrent action. Examples include investments in Russia's integrated air defense systems, which are considered some of the best in the world. The advanced S-400 surface-to-air missile (SAM) system is in serial production, with 10 air defense regiments equipped with the system and three more regiments adding the system every year. The next-generation S-500 SAM will also be capable of theater ballistic missile defense and began testing in 2016.[65] Russia could threaten retaliation with its diverse conventional military forces, which include, for example, a variety of tactical land-attack cruise and ballistic missile systems, some of which have been employed in combat in Syria.[66] Raising the cost of deterrent responses with its defensive systems, or with offensive retaliatory capabilities, will diminish or negate the coercive capacity of deterrent threats from Russia's potential adversaries.

Russian gray zone operations. In spite of nuclear and conventional military capabilities, and their capacity to weaken adversary general deterrence, Russia has recently employed other negation techniques described above to execute offensive operations. Russia has employed 'gray zone' techniques that have served to at least partially conceal its culpability during the immediate crisis, provided ambiguity over what was happening and who was doing it, and carefully regulated the character and tempo of its operations to remain below a threshold that would trigger a possible deterrent response from a major power adversary such as the United States.

Special Warfare Magazine, A U.S. Army Special Operations Command publication, describes gray zone conflicts as:

> competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality, are characterized by ambiguity about the nature of the conflict, opacity of the

> parties involved, or uncertainty about the relevant policy and legal frameworks. They exist short of a formal state of war, and present novel complications for U.S. policy and interests in the 21st century.[67]

Gray zone conflict is thus a method of offensive operations that employs ambiguity, low-intensity forms of conventional and irregular military violence, information operations, and criminal proxies to achieve political goals without triggering adversary deterrent responses.

Russia employed offensive gray zone operations in August 2008 during its seizure of portions of territory from the Republic of Georgia. Russia's strategic objectives for the operation included protecting Russian ethnic populations in and around Georgia and dissuading Georgia from entering the NATO alliance. During the five-day conflict, Russia employed a combination of conventional military formations, intelligence and special operations support to local ethnic-Russian separatist guerillas, cyber denial-of-service attacks against Georgian government offices, and information and propaganda operations to enhance the ambiguity of the campaign to outside observers.[68] The combination of effective information operations, the murky character of the fighting between the separatists and the government, and Russia's careful control over the level and tempo of violence, succeeded in avoiding any vigorous Western response to the aggression. The operations concluded with Russia seizing Abkhazia and South Ossetia, formerly provinces of Georgia.[69] Russia, thus, successfully negated any general deterrence that might otherwise have protected Georgia's sovereignty.

In February 2014, Russia again employed some of these same techniques during its seizure of Crimea from Ukraine and its support to separatist guerillas in the eastern Donbas region of Ukraine. Armed men in unmarked uniforms appeared across Crimea, seizing control of the territory from Ukrainian authority. Russian President Vladimir Putin at the time claimed the men were "self-defense groups" who had bought their uniforms and equipment at local shops.[70] It later became clear that the "little green men" were Russian special operations and conventional infantry soldiers sent there on President Putin's orders.[71] A referendum of the Crimean population organized by the Russian occupation forces approved the seizure of the territory and attempted to provide a veneer of legitimacy of the operation. President Putin later justified the operation by insisting on the need to provide protection to ethnic Russians, as was the case in Georgia in 2008.

In the spring of 2014, Russia's gray zone operations spread to the eastern Donbas region of Ukraine. Ethnic Russian separatists, supported by Russian intelligence, special operations, and later conventional military forces, fought bloody battles against Ukraine military and internal security forces. According to the BBC, between April 2014 and August 2016, 9,553 people were killed, 22,137 wounded, and over 1.1 million displaced in eastern Ukraine.[72] Russian officials at first denied that their forces were involved in the fighting, but in December 2015, President Putin admitted that Russian forces were active in eastern Ukraine.[73] Russia ultimately contributed airpower, artillery, electronic warfare assets, and combat advisers in support of the insurgents in eastern Ukraine.[74]

The events in Crimea and eastern Ukraine during 2014 demonstrated Russia's capacity to undertake offensive military operations in an ambiguous and initially deniable manner. The operations were staged to appear as spontaneous local uprisings, actions that would not appear out-of-the-norm to outsiders who had become accustomed to viewing various civil wars around the world involving local militias. This context provided the Russian government with plausible deniability, at least in the early days and weeks of these crises, when the political pressure for a deterrent response would have been most intense. Russian officers and their local proxies regulated the intensity and character of the violence and calculated to keep it below the level they believed would trigger retaliation. Finally, Russia employed information operations, control over imaging, and propaganda to increase ambiguity and reinforce its initial denials of culpability.

These measures, in combination with other methods of deterrence negation described earlier, allowed the Russian government to execute these offensive operations while avoiding any military deterrent response from the West. The United States and many other governments subsequently imposed economic and financial sanctions on Russian individuals and entities. But fears of a wider war, of Russian military capabilities, and of the possibility of Russian diplomatic or military retaliation, have strictly limited other deterrent responses in support of Ukraine. For example, the United States still provides only non-lethal assistance to Ukraine's military and internal security forces.[75] Although some in the U.S. Congress have urged the provision of lethal defensive equipment such as anti-tank missiles to Ukraine, fears of retaliatory escalation by Russia have blocked such a policy.[76] Thus, Russia has succeeded in using its full range of deterrence negation tools to advance its objectives in George and Ukraine.

There are now concerns that Lithuania, Latvia, and Estonia could be the next targets of Russian aggression. From a Russian perspective, these former Soviet republics, and now NATO member states, are located uncomfortably close to key Russian centers such as St. Petersburg and Moscow. Like Georgia, Crimea, and eastern Ukraine, the three Baltic states contain substantial ethnic Russian populations, which could create the same pretext for Russian aggression as the previous cases, and, as with the other cases, could be sources for armed pro-Russian militias.

From a Russian perspective, these former Soviet republics, and now NATO member states, are located uncomfortably close to key Russian centers such as St. Petersburg and Moscow.

In response to prospective Russian gray zone action directed against the Baltics and other countries along NATO's eastern border, the United States government established the European Reassurance Initiative, later expanded and renamed the European Deterrence Initiative. The purpose of the initiative is to provide training and military infrastructure support to NATO's eastern European members, and to finance increased rotations of U.S. and NATO forces through the region, for training and presence.[77] What remains unknown is whether the addition of these deterrent capacities will be effective against the kinds of gray zone techniques Russia has employed and might employ in the Baltics or elsewhere.

China. Since 2008, China has pursued an increasingly aggressive offensive to seize maritime territory in the South China Sea, a part of its larger campaign to extend its influence in East Asia and reduce the role of the United States. However, this offensive action has occurred entirely in the gray zone, regulated by China to avoid triggering standard U.S. military deterrent responses.[78] As a result, U.S. policy responses to China's assertions have been reactive and have not deterred further Chinese action in the region.

China has designed its offensive methods in the South China Sea to bypass or negate U.S. legacy deterrent structures. For example, civilian rather than military ships and vessels have been the vanguard of its maritime activity in the area. These civilian "white hull" vessels have included China's coast guard (some of which are as large as naval destroyers and cruisers) and other maritime law enforcement vessels such as those of China Maritime Surveillance.[79] Although ostensibly civilian white-hulled vessels, these Chinese ships, overwhelming in size, number, and armament compared to those of neighboring countries, have protected other Chinese vessels as if they were gray-hull naval escorts.

Those other Chinese vessels have included mobile drilling rig platforms (some of which have drilled without permission inside Vietnam's Exclusive Economic Zone),[80] a large fleet of sand dredging vessels that have built up hundreds of acres of terrain on seven features China occupies in the Spratly Islands,[81] and China's large fishing fleets, which have effectively become a maritime militia, employed to establish China's overwhelming presence in the East and South China Seas.[82]

In April 2012, China employed these resources and methods to seize control of Scarborough Shoal from the Philippines.[83] In the Spratly chain, China used its dredging fleet to vastly expand the usable territory on the seven features it occupies. China has now built runways, aircraft hangars, wharfs, desalination plants, electrical power stations, radars, warehouses, offices, barracks, concrete emplacements, and other structures on what were previously submerged rocks.[84] These features are now ready to receive military assets such as fighter-attack aircraft, surface-to-air and surface-to-surface missiles, and naval infantry.

In spite of its "Pivot to Asia" policy,[85] the United States has not had an effective response to China's expansion in the South China Sea. There are several reasons for this. China's leaders may possess greater will over potential conflict in the South China Sea and thus may be willing to run greater risks than U.S. policymakers. The Chinese government has repeatedly stated that most of the South China Sea is Chinese territory.[86] By contrast, the United States government makes no territorial claim to the sea, and has confined its direct interests to freedom of navigation.[87] Freedom of navigation in the South China Sea, and by extension the economic security of U.S. allies and partners in East Asia, are arguably vital U.S. national interests. However, since the U.S. has no direct territorial stake in the sea, U.S. policymakers may face more difficulty marshalling political support for risky action compared to their Chinese counterparts. This differing level of direct interests could explain a differing level of will and risk tolerance.

China's employment of civilian assets as its military vanguard has appeared to successfully bypass the dramatic, visible, "Pearl Harbor"-type military event U.S. culture seems to require to be stirred to action. China's initially slow, creeping offensive action, executed for the most part out of public view and by civilian assets, occurred below the threshold that would have triggered a response by the U.S. legacy deterrent structure.[88]

Finally, the military and economic costs of prospective U.S. deterrent responses against China's gray zone aggression are rising. The rapid growth of China's military capabilities in the region have raised the potential costs and risks of U.S. military action. For now, U.S. military capabilities involved in a prospective clash concerning the South China Sea are likely dominant. Even so, U.S. policymakers would have to expect losses of personnel and equipment, possibly substantial.[89] The economic consequences of a clash would also likely be substantial, with effects on global trade extending back to the U.S. economy.[90] These risks and costs, combined with the ambiguous nature of China's aggression, its execution below America's retaliatory thresholds, and the differences in national interests and will, have combined to negate the U.S. legacy deterrence structure.

The U.S. legacy deterrence structure has effectively deterred nuclear war and major conventional military aggression in places like Western Europe and Korea that have long been high U.S. security interests. Even so, all during the Cold War and up to present day, determined adversaries have from time to time employed tactics and techniques to bypass or negate U.S. general deterrence to achieve geopolitical goals in opposition to U.S. interests.

Toward a Comprehensive Deterrence Structure

As this chapter has explained, current challengers such as al-Qaeda, Iran, Russia, and China have employed similar methods to bypass the legacy U.S. deterrent structure. These methods have included negating U.S. deterrent capabilities through active or passive means, threatening retaliation against U.S. interests, regulating offensive action to levels below the trigger point for a U.S. deterrent response, and employing ambiguity and attribution deception to forestall a U.S. reaction. These and other techniques have either thwarted legacy U.S. deterrent capabilities or undermined the will of U.S. policymakers to respond. This results in challengers slowly accumulating results toward their geopolitical objectives, often at the expense of U.S. interests and those of its security partners.

From this diagnosis we can see that the U.S. legacy deterrent structure, focused as it has been on nuclear and major conventional scenarios, has gaps that challengers are exploiting. Filling in those gaps to create a new comprehensive deterrent structure will require contributions from all the elements of national power.

Comprehensive deterrence would seek to deter aggression along a broader range of political-military operations. It would explicitly extend deterrence beyond nuclear and major conventional conflict, closing some of the gaps currently exploited by adversaries described above. Comprehensive deterrence would seek to deter adversary nation-states from employing gray zone tactics to achieve their geopolitical objectives. Comprehensive deterrence would also seek to deter hostile non-state actors from employing terrorism or other low-intensity forms of aggression against U.S. interests.

Establishing deterrence against gray zone challenges could imply possessing the capabilities and the willingness of defenders to conduct gray zone-type operations themselves. This could be the case if the United States and some of its security partners wished to establish a deterrence-by-denial framework against gray zone challenges. Deterrence-by-denial seeks to establish deterrence by convincing adversaries that they cannot achieve their objectives with their operational concepts and assets. For gray zone challenges, this implies the possession of convincing capabilities and the will of the United States and its partners to defeat adversary gray zone operations where they are happening.

Alternatively (or to supplement deterrence-by-denial capacities), the United States and some partners may find it useful to acquire their own offensive gray zone capabilities, in pursuit of deterrence-by-punishment tools and a coercive punishment framework. Future U.S. policymakers may find the need for additional military options if legacy tools such as conventional military options or special operations direct action (DA) raids alone are insufficient. Legacy tools, to include nuclear weapons, may be impractical or inadequate for generating convincing punishment leverage. If so, policymakers will desire a fuller deterrence-by-punishment toolbox.

The acquisition of some gray zone capabilities by the U.S. government could be controversial. As we have seen with the cases above, some gray zone techniques appear to violate international law, or at a minimum, skirt legality and moral standards the U.S. government would prefer to uphold rather than undermine. Acquiring and then threatening to employ some gray zone capabilities, either for deterrence-by-denial or deterrence-by-punishment, could violate norms by which the U.S. government operates.

In addition, some analysts wonder why the United States would need to operate in the gray zone, and further question whether the gray zone is a meaningful concept. These critics contend that the gray zone concept is simply ancient warfare techniques repackaged in modern—and mostly empty—terminology. By this view, U.S. policymakers and military planners are struggling with adversary gray zone techniques because they have forgotten their studies of history.[91] Critics recommend defeating gray zone competitors through escalation to adjust the battlefield to terrain that will make the best use of U.S. and coalition advantages.

There are several reasons why policymakers may wish to avoid escalating a low-intensity or ambiguous conflict, and instead oppose the aggressor on low-intensity or gray zone terms. Even if escalation would shift the conflict on to more favorable terms for the U.S. and its partners, policymakers may view escalation too risky or politically undesirable.[92] Escalation might create friction with important security partners and cause them to drop out of a coalition formed against the aggressor. Policymakers might wish to avoid the costs and commitment of prestige that escalation could require. For these reasons and others, policymakers may prefer that military commanders and planners provide them with courses of action that match the intensity, risk, and costs that the aggressor is committing with his gray zone challenge.

The United States government was once an active and successful gray zone player. However, gray zone U.S. activity and competence atrophied since the end of the Cold War. During the Cold War, the United States actively employed nonmilitary gray zone methods such as the aggressive formation of alliances and security partnerships (many with unsavory regimes), information operations, propaganda, and economic warfare against the Soviet bloc. Cold War gray zone military and paramilitary methods included the liberal employment of intelligence community covert actions and the creation and expansion of SOF. Arguably the first mission of USSOF at the beginning and through much of the Cold War was unconventional warfare (UW), the training and support of proxy forces and indigenous militias attempting to undermine governments the United States considered hostile.[93] During this period, the United States government actively employed offensive gray zone methods. More recently however, new views of legal and moral boundaries, mixed perhaps with complacency about the U.S. strategic position, has caused many policymakers to view such methods as no longer available for employment.

The sustained employment of gray zone techniques by Iran, Russia, and China, added to the ongoing threats from various non-state terror groups, may compel U.S. policymakers to once again consider many of the gray zone and low-intensity methods their predecessors once employed. The addition of such capabilities, both in deterrence-by-denial and deterrence-by-punishment roles, would patch holes in the legacy deterrence structure and help build the broader, more comprehensive deterrence framework the current and future operating environment will require.

SOF can and should make their contributions to an improved comprehensive deterrence structure. SOF can employ their capabilities and statutory missions to help patch some of the holes in the existing deterrence structure. As the next two chapters explore, SOF can contribute its traditional capabilities and missions to establish greater deterrence against hostile non-state actors. SOF can also contribute to improving deterrence against aggressive state actors that are attempting to execute offensive strategies using gray zone techniques. SOF can make important contributions to deterrence-by-denial and deterrence-by-punishment approaches, both of which will be components of a comprehensive deterrence framework.

SOF can employ their capabilities and statutory missions to help patch some of the holes in the existing deterrence structure.

If the U.S. and its security partners can establish a better and more comprehensive deterrence structure, they could prevent costly conflicts that might otherwise occur. In addition, they would prevent malicious state and non-state actors from encroaching on U.S. and partner interests. As the remainder of this monograph explains, U.S. and coalition SOF can make effective and economical contributions to improve comprehensive deterrence.

Chapter 3. SOF Contribution to Deterring Hostile Non-State Actors

Can the United States deter malicious non-state actors, especially terror groups that employ suicide attacks as a tactic? The previous chapter discussed how non-state and rogue actors have exploited gaps in the legacy deterrence framework to pursue their objectives while in some cases avoiding U.S. and partner deterrent responses. In spite of these challenges, this chapter discusses how U.S. policymakers and military planners can apply deterrent principles to hostile non-state actors. In particular, the chapter describes how SOF can employ its statutory activities to improve and extend deterrence against the threats posed by these non-state actors.

The DO JOC discussed in chapter 1 addresses the problem of deterring non-state actors, but in a manner that emphasizes the challenges more than the solutions. For example, DO JOC elaborates on the differences between deterring state and non-state actors, with a description that reveals the difficulties in deterring the latter. DO JOC reminds us that unlike most state-based adversaries, U.S. planners may struggle to identify key decision-makers inside non-state opponents—the decision makers whose behavior U.S. deterrence operations are supposed to influence. U.S. planners will face greater uncertainty understanding how a non-state actor calculates benefits, costs, and consequences (for example, some non-state actors may seek to induce a U.S. military response to bolster their prestige). Non-state actors may possess few if any assets that U.S. deterrent capabilities might hold at risk. Finally, U.S. policymakers may have greater difficulty communicating with non-state adversaries, compared to state-based opponents. For these reasons, planning deterrence operations against non-state actors will frequently be more challenging than operations against a state-based actor.[94]

How Israel has Established Deterrence Against Hostile Non-State Actors

But, in spite of these challenges, there is evidence that states can effectively design and implement deterrence operations against hostile non-state actors, even those that employ suicide attacks in their operations. For example, Graham Allison, a professor at Harvard University and former U.S. Assistant Secretary of Defense, has argued that the Israeli government has effectively established deterrence against numerous sub-state and non-state actors, including Hezbollah, Hamas, and even ISIS.[95] According to Allison, Israeli policymakers and military planners have employed the fundamentals of deterrence theory and coercive threats to establish a climate of general deterrence against these non-state adversaries.

Employing deterrence theory, Israel has communicated to its adversaries the "red lines" (such as an attack on Israeli territory or the possession of chemical weapons) that will trigger a deterrence response. Next, the Israeli Defense Force (IDF) and Israeli intelligence services have developed airpower, special operations, intelligence, and covert actions capabilities that are useful against Israel's non-state opponents and have partially revealed these capabilities so that prospective adversaries are aware of them. Finally, Israeli policymakers have achieved deterrent credibility by periodically employing these capabilities, both to display their destructive potential and also to show adversaries their will to employ them. As a result, according to Allison, groups affiliated with ISIS, one of which is located in southern Syria only a few hundred meters from Israel, have refrained from attacking Israeli targets.[96]

Over the past 25 years, Israel has employed periodic punitive campaigns against sub-state actors Hezbollah and Hamas, the cumulative effect of which has been to establish and reinforce deterrence aimed at dissuading these actors from regularly employing violence against Israeli citizens and territory. Six such campaigns, 3 each against Hezbollah and Hamas, and lasting from 7 to 50 days, employed airpower, conventional ground maneuvers, and SOF to impose costs on these adversaries and their bases of support.[97]

During this quarter-century span, a variety of Israeli leaders facing the security challenge posed by these adversaries concluded that the complete elimination of these particular threats was beyond Israel's capacity. But these leaders concluded that establishing a climate of general deterrence was possible, and this became Israel's unspoken policy.[98] Deterrence has not been perfect; during this span, rocket attacks and terror raids have occasionally occurred on Israel's northern and southern frontiers where Hezbollah and Hamas reside. But the military potential of these two groups—in particular, their inventories of rockets and missiles—far exceeds what they have employed.[99] Further, Israel's northern and southern borders are now mostly quiet. From this we can conclude that Israel, by occasionally employing its punitive capabilities, has effectively established general deterrence against two capable non-state actors that have suicide attack capability.

Since its inception in 1948, Israel has steadily established a climate of general deterrence against a shifting array of adversaries. It has built this increasingly comprehensive deterrence structure by accumulating military successes against first, state-based adversaries, and later, non-state adversaries. The cumulative effect of these military successes has been the creation of general deterrence against a broad range of potential state and non-state opponents.[100]

The first phase of Israel's construction of cumulative deterrence was the series of successful wars it waged against state adversaries between 1948 and 1982. The result of these successes was the abandonment by these adversaries of their goal of destroying the Israeli state. Instead, Egypt and Jordan signed peace treaties with Israel and the remaining Arab states have given up on military competition with Israel.[101] The second phase of Israel's cumulative deterrence approach involved conflicts against non-state terror organizations. Over several decades, Israel has employed classic deterrence methods such as denial (border fencing, arrests, special operations raids, and missile interception capabilities) and punishment (airpower and punitive ground operations) to display deterrent capabilities, will, and signaling to adversary non-state decision makers.[102] The end result of this cumulative approach to deterrence is relative quiescence for Israel regarding potentially hostile state and non-state actors in the Middle East region.

Critics of Israel's cumulative deterrence approach point out that the numerous instances of actual fighting Israel has had to execute since 1948 is hardly supporting evidence of deterrence; if deterrence truly existed, Israel would not have had to fight.[103] In truth, Israel had to fight its many wars since 1948 to firmly establish Secretary Kissinger's three factors of deterrence: capability, will, and adversary belief. Israel's cumulative deterrence approach has convinced Israel's adversaries that various coercive methods they have employed—major combat operations, low-intensity attrition, suicide terrorism, missile attacks, etc.—have all failed, due to either Israeli denial or punishing retaliation. Once the list of coercive options have all been tried and failed, general deterrence will have been established, as currently appears to be the case.

The official strategy of the IDF emphasizes the role of deterrence. Deterrence is stated as a principle of Israel's national security doctrine and as an underlying premise of the strategy's security concept.[104] According to the strategy, the IDF will employ both denial (defensive systems and disruption of enemy plans) and punishment ("a credible threat of severe offensive actions that will exact a heavy toll if we are attacked") as specific deterrent methods.[105] According to the document, current and former Israeli defense planners and policymakers believe they have established effective deterrence against Hezbollah and Hamas.[106]

Although the strategic circumstances of Israel and the United States differ, U.S. policymakers and planners can learn from how Israel has established general deterrence against its non-state adversaries. Most notably, U.S. officials should study how Israel has employed deterrence by punishment against terror adversaries and how it has used cumulative deterrence to establish the reputation of its offensive capabilities and its will to employ these capabilities.

The DO JOC presents in appendix B an illustrative example of how the deterrence precepts in the publication would be applied against a non-state adversary.[107] The illustration relies heavily on deterrence-by-denial methods. Examples of recommended methods of deterring a non-state actor include financial sanctions against the actor, targeting the actor's leadership, intercepting and disrupting the actor's communications, and hardening U.S. and coalition facilities against the adversary's attack capabilities.

These are all direct or indirect methods of denying the non-state adversary the capacity to achieve his goals. Deterrence by punishment, by contrast, is not mentioned. The non-state actor appendix in DO JOC makes no mention of "a credible threat of severe offensive actions that will exact a heavy toll if we are attacked," that is explicitly discussed in the IDF's official doctrine.[108]

Israel's numerous punitive campaigns against Hezbollah and Hamas imposed costs on the military forces and governing structures of these adversaries, but also made life difficult for the underlying civilian populations behind these groups, putting at risk the organizations' continuing political legitimacy and authority.[109] Israel's 2006 war against Hezbollah is an example. The IDF received much criticism in the aftermath of the war for being unprepared for Hezbollah and its hybrid warfare tactics. The war cost the IDF 114 of its soldiers killed in action and 10 percent of the army's main battle tanks committed to the conflict. Hezbollah struck 901 Israeli cities and towns with 3,709 rockets and missiles during the 34-day conflict. Even so, the IDF killed over 600 Hezbollah fighters and reduced the group's military capacity by half. The war also killed more than 1,000 Lebanese civilians, wounded another 4,000 and inflicted over $4 billion in losses to Lebanese infrastructure and buildings.[110]

The costs inflicted on the Hezbollah organization and its homeland caused Hassan Nasrallah, Hezbollah's leader, to regret the war, which began when Hezbollah fighters kidnapped two Israeli soldiers in northern Israel on 12 July 2006. "We did not think, even one percent, that the capture would lead to a war at this time and of this magnitude," Nasrallah said in August 2006 in an interview on Lebanese television after the war. "You ask me, if I had known on July 11 … that the operation would lead to such a war, would I do it? I say no, absolutely not."[111] After these campaigns, Israel's northern and southern frontiers were relatively peaceful. It is reasonable to infer that Israel's punitive campaigns, techniques not discussed in U.S. doctrine for deterring non-state adversaries, have contributed to deterrence.

This deterrence has applied against not only Hezbollah and Hamas, but other hostile non-state actors also. In addition to warring against the Iraqi government, the United States, and Western Europe, ISIS has also declared its hostility to Israel. But, it has not attacked Israel. According to a German journalist who in 2014 embedded with ISIS, "The only country ISIS fears is Israel. They told me the Israeli army is too strong for them."[112]

After several years of enduring U.S. and coalition airpower and the support the United States has provided to Iraqi security forces fighting to remove ISIS from Iraqi territory, it may be the case that ISIS decision-makers and foot soldiers may now also fear the United States and its partners. For U.S. policymakers and military planners hoping to establish general deterrence against prospective hostile non-state actors, creating such a deterrent reputation—composed, per Secretary Kissinger, of capability, will, and adversary belief—should be an explicit goal of U.S. policy. U.S. policymakers should use Operation Inherent Resolve—the U.S. and coalition campaign against ISIS—as a component of cumulative deterrence, a building block of establishing a reputation for deterrent capability and will that other potential adversaries will believe and understand. That is a second lesson from Israel's experience that U.S. policymakers can apply to U.S. security challenges.

The Role for SOF in Deterring Hostile Non-State Actors

Title 10, Section 167 of the United States Code lists military activities assigned to USSOF. These activities are:

1. DA;
2. Special reconnaissance;
3. UW;
4. Foreign internal defense (FID);
5. Civil affairs (CA);
6. Military information support operations;
7. Counterterrorism;
8. Humanitarian assistance;
9. Theater search and rescue; and
10. Such other activities as may be specified by the President or the Secretary of Defense.[113]

USSOF, alone and in cooperation with partner forces, could, in some circumstances, employ these Title 10 authorities to enhance and extend the U.S. deterrence framework against current and prospective hostile non-state actors. Each of the statutory SOF activities could be a potential deterrent capability, the first factor in Secretary Kissinger's capabilities-will-belief deterrence equation.

For SOF activities to be valuable as deterrent tools, policymakers will have to fashion these activities to meet all three factors of Secretary Kissinger's equation. The activities will have to be real and exercised capabilities, that are useful for either deterrence-by-denial or deterrence-by-punishment courses of action. Second, U.S. policymakers and military commanders must be willing—and demonstrate their willingness—to employ the SOF activities against prospective adversaries. Finally, prospective adversaries must understand the capabilities and believe that the U.S. might employ these capabilities against them. That means that the capabilities have to be at least partially overt and publicly demonstrated in combat against other adversaries in a manner that increases their credibility.

Policymakers and planners intending to employ the statutory SOF activities in deterrent roles should begin with the deterrence operations planning process presented in the DO JOC doctrinal publication and discussed in chapter 1 of this monograph. To review, that planning process consists of five steps:

1. Determine the objectives of the deterrence operation;
2. Assess the target's interests and decision calculus;
3. Select variables inside the target's decision calculus to be influenced by deterrent effects;
4. Develop deterrent courses of action designed to influence the selected variables; and
5. Execute the deterrent operation and evaluate its effectiveness.[114]

By completing this planning process, the planner will then be able to determine which, if any, of the statutory SOF activities might be useful as deterrent capabilities against the target under consideration.

The next section discusses how USSOF can employ some of these statutory activities to deter current and prospective non-state adversaries.

DA and Counterterrorism. Since 2001, U.S. and coalition SOF have conducted thousands of DA raids against a wide variety of hostile non-state actor targets.[115] The vast majority of these raids occurred in support of the larger political-military campaigns in Iraq and Afghanistan. However, USSOF raids in Libya, Yemen, Somalia, Syria, and on the high seas in the Indian Ocean have also been revealed to the public. The most globally famous SOF DA raid from this period was Operation Neptune Spear, the raid on Osama bin Laden's residence in Pakistan in 2011.[116]

The cumulative effect of these raids, and the global public knowledge of particularly dramatic cases such as Operation Neptune Spear, would seem to support the three-factor Secretary Kissinger axiom for deterrence. U.S. and coalition SOF have repeatedly demonstrated raiding capabilities against a wide variety of targets. The thousands of such examples, including difficult cases such as the decision to raid Pakistan to get at bin Laden, have demonstrated the will to use the capability. Finally, U.S. policymakers have been willing to partially reveal these DA capabilities so that prospective adversaries can understand the threat they could face, and thus believe it.

USSOF DA raiding has focused on denying non-state actors their capabilities for offensive action against U.S. and partner targets and interests. The objectives of USSOF raids have almost always been high- and mid-level personnel, intelligence-gathering, and the seizure or destruction of adversary weapons, financial resources, or other assets.

The theory behind such targeting is to disrupt and destroy the adversary's capacity for action. In other words, the goal for the vast majority of these raids has been denial, not punishment. USSOF' raids may have been painful for the targets, but it has not been a U.S. aim to deliberately inflict pain on organizations like al-Qaeda or ISIS with the goal of changing the behavior of the organizations' decision-makers. Instead, the U.S. theory is to employ DA to disrupt or destroy such organizations by killing or capturing their leaders and eliminating the ability of such organizations to function. Deterrence, whether by denial or punishment, infers living with the adversary while deterring its potential malicious actions. For declared adversaries like al-Qaeda and ISIS, destruction, not deterrence, is the U.S. theory of success.

Even so, it is possible that the examples the U.S. sets with DA raiding against al-Qaeda and ISIS could establish effective deterrence against other prospective non-state actors whose leaders, after viewing such examples, will be deterred from malicious activity against the United States and its interests. It will be very difficult to prove whether spectacular USSOF DA such as Operation Neptune Spear function as deterrents against future potential adversaries. Chapter 1 discussed this conundrum—the inability to prove why an act did not occur, which is what deterrence is about, preventing acts from occurring. Even though establishing such proof is challenging, policymakers and military commanders should be willing to at least partially publicize USSOF DA successes, with a goal of strengthening deterrence against prospective adversaries.

UW and FID. In a lecture delivered at the Naval Postgraduate School in 2008, Admiral Eric Olson, U.S. Navy, then commander of U.S. Special Operations Command, said, "Direct action is important, not decisive; Indirect Action is decisive."[117] UW and FID are two special operations activities that aim to develop friendly indigenous military forces (irregular in the case of UW, state-controlled in the case of FID) to achieve the political and military goals of both the United States and the partner receiving UW and FID assistance. UW and FID thus constitute an indirect application of U.S. military power.

But, although indirect methods, successful UW and FID campaigns are likely to be more powerful and effective deterrents to current and prospective hostile non-state actors than DA raids. Unlike raids, successful UW and FID campaigns offer the prospect of long-term change to the underlying geopolitical conditions of a conflict, to the detriment of an adversary non-state actor. It is for this reason that Olson defined indirect actions such as UW and FID as decisive examples of SOF activity.

Operation Inherent Resolve, the current campaign against ISIS, has FID and UW lines of effort that, if successful, should deliver a decisive blow to ISIS. The FID line of effort is the assistance U.S. and coalition SOF and conventional forces are providing to Iraq's security forces, which are clearing ISIS forces from western and northern Iraq. A simultaneous UW line of effort, conducted by U.S. and coalition SOF and intelligence personnel, is assisting Syrian irregular militias in their campaign to defeat ISIS forces in eastern Syria. According to the combined-joint task force responsible for the campaign, "Ultimately, the military victory over Da'esh [ISIS] will be accomplished by the indigenous forces, we will accomplish our mission with those indigenous forces, and we will attain improved regional stability *through* those partners [emphasis in the original text]."[118]

Should Operation Inherent Resolve's FID and UW lines of effort succeed as designed, local indigenous forces would defeat ISIS, the hostile non-state (or proto-state) actor in the case. This form of defeat could be especially crippling for a movement such as ISIS because it would come from the hands of those in the local region it had hoped to lead, convert, or control. Much more than the loss of material assets, which in theory could be replaced, defeat by local indigenous forces would constitute a political, ideological, or theological rejection—an outcome likely to be more consequential and long-lasting.

This form of defeat could be especially crippling for a movement such as ISIS because it would come from the hands of those in the local region it had hoped to lead, convert, or control.

Such an outcome could serve as a powerful deterrent to other prospective non-state actors, and likely a more powerful deterrent than the consequences of DA raids. These prospective adversaries would observe that this defeat was organized and supported by U.S. and allied SOF, along with other whole-of-government efforts. The deterrent lesson for other non-state actors would be to avoid antagonizing the United States or threatening its interests to a degree that would spark another such U.S.-sponsored FID or UW campaign directed against that non-state actor.

It is too late to deter ISIS; Operation Inherent Resolve aims to thoroughly defeat the movement through the specific application of indigenous military power, support by U.S. FID and UW campaigns and airpower. However, the example set by successful outcomes of these two lines of effort could provide a powerful deterrent against future prospective non-state adversaries. The Deterrent Conundrum—the inability to prove that adversaries did not act because of deterrent coercion—will make it difficult to determine whether a successful outcome for Operation Inherent Resolve increased general deterrence against prospective non-state actors. Even so, U.S. policymakers and military planners should promote and publicize such successes in languages and manners easily accessible to prospective non-state adversaries, in the hope of transmitting effective deterrent messages.

CA and Military Information Support Operations. U.S. policymakers and planners have long recognized that to prevail against hostile non-state actors, the United States and its security partners will have to desiccate the recruitment of new terrorist foot soldiers and their supporters. It will also be necessary to discredit terror organizations, with the goal of reducing their public support, financing, sanctuaries, and recruiting. The U.S. government has long attempted to employ "whole of government" lines of effort and programs to assist other countries with weak institutions that are struggling to battle terror groups with global reach that may have found sanctuaries inside their borders. CA and military information support operations (MISO), both SOF statutory activities, are examples of actions U.S. and coalition SOF can undertake to support beleaguered security partners that are attempting to discredit and dry up support for hostile non-state actors.

For example, the United States government could sponsor propaganda campaigns inside partner countries that aim to discredit hostile non-state groups. Second, the U.S. government could implement overt or covert actions and programs that support friendly rivals and alternative organizations in opposition to the hostile groups the United States and its partners seek to diminish.[119] Finally, the United States government can encourage and support the reform of government institutions and security forces of security partners in an effort to remove some of the possible grievances driving support for violent non-state groups.[120]

These lines of effort—propaganda, support to alternative groups, and institutional reform, among others—are almost always performed by broad interagency task forces of the U.S. government. For example, the U.S. Department of State would likely have leading roles regarding public diplomacy and information operations while other agencies would lead efforts to support alternative groups. That said, USSOF would have its roles to play for all of these lines of effort through its CA and Psychological Operations (PSYOP) organizations and teams.

When these lines of effort are successful in one context, such an example could deter other prospectively hostile non-state actors. As with the threats posed by well-functioning UW and FID campaigns, hostile non-state actors will very likely fear information and clandestine actions that are effective at discrediting these groups and shutting down support among their core supporters. Effective SOF-organized CA and MISO campaigns against one hostile non-state actor could deter other such actors from attacking U.S. interests, lest they receive the same unwanted attention from SOF CA and PSYOP operators.

The Deterrent Role of Punitive Campaigns Against Non-State Actors

U.S. policymakers and military planners may encounter a hostile non-state actor they are not able to completely eradicate as an enduring threat. DA raiding by SOF might degrade such an actor's capabilities but not eliminate the threat. Similarly, United States and coalition partners may not have the option of developing local indigenous military forces through UW or FID lines of effort to eliminate the hostile non-state actor. In such cases, the United States and its security partners may be forced to tolerate the hostile actor's existence for an open-ended period. Deterring the hostile group from aggressive and violent acts against the United States and its interest would then be the only remaining option.

Although an undesirable outcome, Israel's experience with Hezbollah and Hamas indicate that establishing stable deterrence against hostile and implacable non-state or proto-state actors can be feasible. As mentioned earlier, Israel achieved these outcomes through punitive military campaigns against these adversaries, campaigns that resulted in the delivery of deterrence-by-punishment messages that have since resulted in a stable peace on Israel's northern and southern borders, across which Hezbollah and Hamas reside.

Israel's 34-day military campaign against Hezbollah in the summer of 2006 is instructive regarding the establishment of a deterrence-by-punishment condition. The Israeli military campaign was designed to be a denial line of effort, but punishment was the ultimate, an initially unintended result, and also the enduring deterrent consequence. When the Israeli campaign began on 12 July 2006, the day after a Hezbollah force kidnapped two Israeli soldiers inside Israel, Israeli Prime Minister Ehud Olmert stated that the goals of the operation were to compel Hezbollah to return the two captured Israelis and permanently drive Hezbollah's military forces out of southern Lebanon.[121] Israel was unable to achieve these goals. Even so, its campaign against Hezbollah that summer was a success, for reasons unexpected at the beginning of the war.

Israel's political and military leaders were at first highly reluctant to employ ground maneuver forces in the campaign. This limited Israel's response during the first three weeks of the campaign to fixed wing aircraft, attack helicopters, and long-range artillery and rockets. By the end of the campaign these forces delivered over 24,000 bombs and missiles from the air and 173,000 artillery shells and battlefield rockets from the ground.[122]

In accordance with a denial strategy, the targets of these munitions were at first Hezbollah's leadership, its command and control facilities, and its fielded forces—especially its surface-to-surface rocket and missile forces. Indeed, Hezbollah's response to the rapidly escalating Israeli air campaign were rocket attacks against Israeli towns and cities, attacks that extended throughout the war. The suppression of these Hezbollah rocket units became a primary focus of Israel's air campaign.

Israel's targeting theory was strictly denial, but the effect of the campaign accumulated by the end into punishment inflicted on the wider Lebanese population, economy, and society. This punishment effect occurred as a result of Hezbollah's tactics for concealing its leadership, command and control elements, and its rocket forces from Israeli intelligence efforts and airpower. For example, Hezbollah's main leadership compound was located in the densely populated Harat Harik neighborhood in Beirut. After warning the civilian population to evacuate, the Israel air force repeatedly struck the compound with 2,000-pound bombs during the war.[123]

Israeli attacks on Lebanon's infrastructure delivered a grievous blow to Lebanese society. Israel considered these infrastructure sites as dual-use for both civilian and military purposes and were thus legal and legitimate targets. According to Israeli officials, nominated targets underwent a legal and command review process similar to that employed by U.S. and coalition command staffs in the U.S. Central Command region.[124] After these reviews, the Israeli air force cratered the runways of Beirut's main airport, destroyed Hezbollah's television transmitters, destroyed 71 bridges in Lebanon (and all the bridges crossing the Litani River in Hezbollah's southern heartland), closed the highway between Syria and Lebanon, and destroyed many telecommunication and cellular telephone towers and facilities.[125] After a cruise missile attack on an Israeli coastal corvette, the Israeli air force destroyed most of Lebanon's coastal radars and imposed a naval blockade on the country. Israel then added Beirut's and southern Lebanon's electrical grid to the target list.[126] By the end of the conflict, over 750,000 Lebanese, one in six of the population, were refugees.[127]

Perhaps the most punishing aspect of Israel's long-range fires campaign was its attempt to suppress Hezbollah's rocket and missile fire targeting Israel's towns. Hezbollah routinely attempted to hide its truck-mounted rocket launchers in and near civilian houses and apartments. When Israeli reconnaissance assets located these launchers, firepower was usually directed at these sites, since they were considered valid and legal targets.[128]

During and after the conflict, the Israeli government received heavy condemnation for its firepower tactics, which at the time appeared to give Hezbollah a propaganda windfall.[129] However unpleasant, Israel's seemingly disproportionate response to the kidnapping of two of its soldiers undoubtedly changed the calculations of Hezbollah's leadership. Prior to the 2006 war, Hezbollah rocket attacks and raids into Israel were frequent occurrences.[130] After Israel's initially-unintended punitive campaign, there have been eleven years of peace along the Israeli-Lebanese border. Israel did not plan to build a deterrence-by-punishment condition against Hezbollah. But, a combination of Hezbollah's miscalculation regarding the kidnapping, Israel's preferred standoff firepower strategy, and Hezbollah's attempted but failed use of human shields to protect its rockets and commanders, resulted in punishment that Hezbollah's leaders have chosen not to risk again. Since

2013, Hezbollah has fought in the Syrian civil war in support of the Assad government, its critical ally. But it continues to refrain from employing its massive rocket arsenal against Israel, evidence of effective Israeli deterrence.

Should U.S. policymakers face a hostile non-state or proto-state actor they could not eliminate, a short, punitive campaign, aimed to create deterrence-by-punishment, may be the least-bad course of action. Such a campaign would naturally have to conform to accepted laws of warfare and norms governing the employment of U.S. military power.[131] But as Israel's 2006 campaign against Hezbollah shows, it is possible to change the decision calculous of determined and well-armed adversaries through punishment accumulated by striking legal and valid targets.

For such a prospective punitive campaign, military commanders and planners would task U.S. and coalition SOF on DA and special reconnaissance missions that targeted enemy leadership, command and control, special weapons, long-range and guided munitions, and intelligence collection. As with Israel's 2006 campaign, such activities would seek to deny the adversary their military capacities. But, the cumulative and long-term consequence of the campaign could be punitive, with favorable changes in the adversary's post-conflict perceptions and calculations regarding future conflict aimed at the United States and its interests.

Conclusion

The U.S. preferred approach to non-state actors that become hostile is to destroy them. Although the mission statement of the DOD begins with the concept of deterrence, in the post-9/11, al-Qaeda era, deterrence against hostile non-state actors was dropped as a useful theory, and replaced with the "4D" concept: "defend, diminish, deny, and defeat."[132]

As we have observed over the past decade and a half, U.S. and coalition SOF will have central roles to play executing direct and indirect lines of effort to deny, defeat, and destroy such adversaries. DA, special reconnaissance, and, more decisively, UW and FID are basic SOF activities that will continue to be employed against hostile non-state actors.

But like Israeli leaders and its public have learned, the United States may someday face hostile non-state adversaries that may prove impractical to completely eradicate. Policymakers and the public will then have to accept deterrence rather than destruction as the least bad method of attaining a stable peace. U.S. military planners and SOF commanders would do well to learn from Israel's experience dealing with well-armed and determined adversaries like Hezbollah and Hamas. U.S. and coalition SOF should be prepared to execute denial campaigns that employ some of the basic SOF activities mentioned above against non-state actors that cannot be destroyed.

U.S. military planners and SOF commanders would do well to learn from Israel's experience dealing with well-armed and determined adversaries like Hezbollah and Hamas.

The DOD's Law of War Manual and the ethical norms governing the employment of U.S. armed forces would likely result in a campaign designed around deterrence-by-denial principles. In practice however, we should not be surprised if the outcome of such a campaign, at least from the non-state adversary's perspective, is deterrence-by-punishment. Such an approach, even if unintended, has worked for Israel, and may also have to work for the United States.

Chapter 4. SOF Contribution to Deterring State Actors Operating in the Gray Zone

Even while U.S. and coalition SOF have spent the past decade and a half (and more) focused on the threats posed by hostile non-state actors (especially those in the Central Command area of responsibility), the growing challenges presented by state competitors and adversaries will require focused attention from policymakers and military planners. These policymakers and planners will call on SOF to participate in the responses to these state-based challenges.[133]

Chapter 2 discussed how some of these state challengers, such as Iran, Russia, and China, are employing 'gray zone' techniques to achieve their goals at the expense of U.S. and allied interests. These gray zone techniques are specifically tailored to avoid the competitive advantages of the United States and its security partners. Legacy U.S. deterrence concepts have proven effective over many decades at deterring overt conventional military aggression. But that is why these state competitors are now employing gray zone techniques, tactics the U.S. and its security partners are struggling to deter.

This chapter will discuss how U.S. and partner SOF can contribute their particular competencies and expertise in response to the challenges the United States and its partners increasingly face from these great power and regional state-based challengers. As is the case with non-state actors (examined in the previous chapter), success thwarting an adversary state's gray zone actions would provide an example that could deter other prospective state-based gray zone challengers.

Defending Against Gray Zone Aggression

The United States and its security partners will have an interest in defending against gray zone aggression for the same reasons they would have for defending against other forms of aggression. Gray zone aggression, whether against the maritime and air commons in the western Pacific or against allies in Eastern Europe, can threaten the legal rights, sovereignty, and economic prospects of the United States and its security partners. As with any aggression, policymakers will presumably have an interest in defending threats to their interests. For gray zone threats, the problem is developing effective, realistic, and sustainable responses to adversary methods that will likely be ambiguous, slow-moving, or difficult to define to domestic and international audiences.

After understanding the gray zone threat and making the decision to counter it, policymakers and planners will then have to formulate courses of action that respond to the gray zone challenge. These responses are likely to fall into the denial or punishment categories described throughout this monograph. Denial responses would seek to directly block the adversary from achieving the goals of his gray zone activities, usually by disrupting or thwarting the adversary gray zone activities themselves. Punishment responses would attempt to dissuade the leaders of the state employing the gray zone actions by imposing costs on that state, its leaders, or other assets and conditions that are valued by the state and its leaders.

Table 1 provides a taxonomy of the responses U.S. and partner policymakers could employ in response to state-based gray zone aggression, and common examples of each.

Table 1. Responses to state-based gray zone aggression

	Denial Responses	**Punishment Responses**
Orthodox Responses	Security Force Assistance	Sanctions
Overt Escalation Responses	Major Combat Operations	Coercive Military Reprisals
Gray Zone Responses	CA, MISO, Covert Action, UW (inside contested zone)	Covert Action, UW (outside contested zone)

The available courses of action will each possess benefits, costs, and risks. Policymakers evaluating the available courses of action will have to weigh the comparative advantages of the players and what those advantages imply for the benefits, costs, and risks of each option.

A threshold question for U.S. policymakers confronting a gray zone challenge will be whether to respond to the challenge with orthodox responses; to escalate the conflict out of the gray zone and on to terms that would allow the United States and its partners to bring familiar tools, such as direct military power into the bargain; or to respond with their own gray zone activities. The following sections will discuss these categories of responses and the roles U.S. and coalition SOF might play for each.

Orthodox Responses to Gray Zone Aggression

The United States and its major security partners have orthodox and familiar responses to misbehaving states. Indeed, U.S. and partner policymakers are currently employing many of these orthodox measures in response to gray zone actions recently executed by Iran, Russia, and China. As noted in table 1, these orthodox responses fall into both the denial and punishments categories.

Orthodox punishments employed against misbehaving states include well-known actions such as diplomatic demarches, travel bans for leadership figures in the offending state, and economic and financial sanctions that can target individuals, select companies, or an entire economy. The United States and many other countries employed economic and financial sanctions against Iranian individuals, companies, and the Iranian economy, and the United States still maintains many such sanctions, in response to Iran's ballistic missile program and its support for terrorism.[134] Similarly, the United States and most of its security partners in Europe have imposed diplomatic, political, and targeted financial sanctions on individuals and entities in Russia in response to Russia's gray zone aggression against Ukraine.[135]

Of more interest to SOF commanders and planners are orthodox denial activities policymakers have called for in response to adversary gray zone activities. Orthodox denial responses typically center on assisting the security forces of friendly states who are harmed by adversary gray zone aggression. Security force assistance to partners resisting gray zone aggression can take many forms. Policymakers have tasked USSOF to assist with the training of partner conventional military forces, SOF, and internal security units—all of which could be called on to disrupt an adversary's hostile employment of infiltrators, guerrilla militias, proxy forces, intelligence officers on covert actions missions, malicious information operations, and other forms of low-intensity and non-attributable gray zone activity.

A current example of security force assistance applicable to countering gray zone aggression is the recent deployment of USSOF to the Baltic states (Lithuania, Latvia, and Estonia) to assist the training of security forces in those countries to counter possible gray zone activities from Russia.[136] Such assistance would resemble FID, one of the Title 10 statutory SOF activities. However, when assisting the security forces of a friendly country to resist gray zone aggression, FID might be a more appropriate term for this SOF activity.[137]

Indeed, this tasking—FID activities that assist partners under siege from gray zone aggression—will be the most common request SOF commanders and planners will receive from policymakers responding to active gray zone threats. It will be the most common because it is an accepted, orthodox response and because orthodox punishment approaches such as sanctions have usually failed to modify adversary behavior.

However, when both categories of orthodox responses fall short of success, policymakers will need to explore some of the other options on table 1. The next section discusses overt escalation and the roles SOF might be called on to perform under these approaches.

Responding to Gray Zone Aggression with Overt Escalation

Competitors that select gray zone activities—such as subornation of target leaders, information and cyber operations, non-attributable militias, and civilian and law enforcement assets such as coast guard vessels performing military missions such as territorial seizure—are simply selecting a lower space on the continuum of escalation, with an intent to avoid the adversary's more powerful military forces and responses.[138]

Thus, Russia, instead of employing its armored brigades, seized Crimea with "little green men," who it claimed were pro-Russian Ukrainians who bought their uniforms and rifles from local stores and suddenly self-organized to protect ethnic Russians under threat from Ukrainian nationalists.[139] Another example is China, which in April 2012 seized Scarborough Shoal from the Philippines using fishing boats and a coast guard cutter instead of an amphibious assault by the PLA Navy.[140] In each case, the state competitor accomplished its territorial acquisition while avoiding an employment of military force that by normal standards would have constituted a casus belli.

Naturally the defender, at least in theory, has the option of overt escalation, responding by shifting the crisis to a space on the escalation continuum that may be more favorable to his competitive advantages. For example, during his confirmation hearing in January 2017 to be the U.S. Secretary of State, Rex Tillerson hinted at the possibility of overt escalation to counter China's territorial encroachments in the South China Sea. "We're going to have to send China a clear signal that, first, the island-building stops," Secretary of State Tillerson told the senators. “And second, your access to those islands also is not going to be allowed.”[141] Although Secretary of State Tillerson did not explain how the United States would block Chinese access to the features it occupies in the South China Sea, his statement implied the employment of U.S. naval and air power to prevent Chinese air and maritime access to the features.

If so, that would be a clear example of overt escalation by one player in a conflict, by shifting the conflict to a mode that that player believes is more favorable for the capabilities and advantages he possesses. In the case of his testimony, Secretary of State Tillerson appeared to presume that overt escalation by the employment of U.S. air and naval forces in a blockade of China’s South China Sea features would favor U.S. military capabilities versus those of China, in that theater of operations. Overt escalation could be used for denial, employing military power to directly disrupt or defeat the adversary’s gray zone activities. Overt escalation, in the form of coercive military reprisals against targets outside the contested zone, could also be used to impose costs or threaten to inflict punishment should the adversary not desist from his gray zone actions.[142]

In practice, U.S. policymakers have frequently employed overt escalation during recent foreign policy crises, in an effort to shift the crisis playing field to terms more favorable for U.S. competitive advantages. For example, U.S. policymakers purposefully escalated U.S. military activity in the early years of the Vietnam War, during the Persian Gulf crisis of 1990-1991, and against Iraq in 2003—each time to take advantage of what these decision-makers believed were U.S. military advantages. Even the 1962 Cuban Missile Crisis, which is held out as an example of the successful use of negotiated crisis “off ramps,” saw U.S. decision-makers first organize a large buildup of U.S. military power near Cuba in order to create negotiating leverage. U.S. policymakers used overt escalation in these cases, both to directly deny the adversary his objectives and—during the Vietnam War and the NATO air campaign against Serbia in 1999—as punishments, in the hope of compelling new behavior from adversary leaders. U.S. policymakers have thus recently employed overt escalation and may find occasion to do so again in the future.[143]

United States and coalition SOF will have familiar, yet important, roles to play when policymakers opt for overt escalation and the employment of joint and combined conventional military forces. SOF would support major combat operations when these operations are employed for either immediate deterrence or in a kinetic response. SOF activities in such cases would include special reconnaissance, to support the targeting of adversary leadership, command and control capabilities, adversary special weapons capabilities, and access-denial nodes and capabilities, such as adversary surface-to-air missile assets.[144] Commanders may task SOF to undertake DA raids on any of these and other target sets to support theater access and operations by conventional air, naval, cyber, and ground forces, and protect U.S. and allied space forces.[145] In cases where policymakers choose overt escalation in response to adversary gray zone activities, SOF will have critical, albeit supporting, roles inside a larger military response.

Fighting Inside The Gray Zone

Needless to say, overt escalation will not always be a feasible response against well-armed and well-positioned state adversaries. Depending on the stakes at risk and an assessment of the relative competitive advantages of the players, U.S. and coalition policymakers may not be willing to bear the risks and possible costs overt escalation could require. In that case, policymakers will ask commanders and planners for responses that are less risky, make fewer reputational commitments, allow for an easier withdrawal from the conflict if necessary, and that are likely to be clandestine. Courses of action with these characteristics describe "blue's" gray zone activities. Thus, policymakers may wish to fight an adversary state's gray zone actions with friendly and partner gray zone activities of their own.

Once again, friendly gray zone responses could take the form of either denial or punishment actions. Denial actions in the gray zone would employ clandestine, proxy, or low intensity actions including non-kinetic activities that would thwart the adversary's gray zone actions. Punishing gray zone actions would seek to impose costs on the adversary, with the goal of coercing a change in the adversary's behavior. These "blue" cost-imposing gray zone activities could occur either in the theater the adversary is attacking or elsewhere where the adversary has interests that might be exposed to coercive action.[146]

Employing SOF to Execute Gray Zone Denial Actions

Information operations, UW, and clandestine operations by USSOF would likely be the most common activities employed by the United States and partner policymakers should they choose to employ gray zones techniques to deny adversary gray zone aggression. The goal of "blue" gray zone activities would be to directly disrupt and block the adversary's gray zones actions within the contested area. A successful display of denial gray zone actions would demonstrate these capabilities and the will to employ them, and could thus provide the basis for deterring other prospective adversaries.

UW is a fundamental statutory activity of USSOF and could be a powerful gray zone denial technique. With this approach, U.S. and partner SOF would support, train, and equip local indigenous resistance forces that could directly counter an adversary's gray zone aggression, and do so without the involvement of conventional U.S. and allied military forces.

One prospective example of this could occur in eastern Ukraine, where SOF could assist pro-Kiev militias resisting separatist militias that are assisted by Russian gray zone activities. U.S. Army Special Forces personnel from the 10th Special Forces Group are frequently in Ukraine training Ukrainian SOF and other local military forces.[147] Such training of regularly-constituted government security forces is an example of orthodox security force assistance, described in an earlier section.

However, should U.S., partner, and indigenous SOF then employ their SOF training and assets beyond basic FID and into a clandestine UW campaign inside the gray zone contested area, such a campaign would fall into gray zone denial activity. The SOF-led UW effort in this case would support a resistance movement opposing militias supported by the aggressor state's gray zone actions.

In the case of Ukraine, U.S., partner, and Ukrainian SOF would form a combined SOF task force to support pro-Kiev militias in eastern Ukraine opposing separatist militias supported by Moscow. Another example of "blue-green" gray zone denial could occur in Yemen, where a coalition SOF task force, likely led by Saudi Arabia, could support friendly Yemeni forces opposing Iranian-backed Houthi proxy forces.

Another form of gray zone denial U.S. and partner SOF might execute, would be preemptive UW. The goal of preemptive UW would be to organize, train, and equip resistance groups and guerrilla forces of a partner facing either a gray zone or conventional threat. An adversary contemplating the conquest and occupation of a territory, the population of which has already prepared to resist, may be deterred from attacking, knowing the presumed high cost of pacification the aggressor would have to pay.

For example, the Estonian Defense League has organized 25,400 civilians (over four times the size of the country's regular army) into insurgent teams. These teams regularly practice patrolling, fieldcraft, combat medicine, and insurgency tactics such as improvised explosive devices. Weapons, ammunition, and supplies for a prospective guerrilla resistance are deployed and hidden throughout Estonia.[148] U.S. and partner SOF could be greatly beneficial to similar preparations in other threaten locations.

In the maritime realm, U.S. and partner maritime SOF (for example, U.S. Naval Special Warfare and U.S. Marine Corps SOF) could expand the training and capabilities of local maritime SOF, naval forces, and civilian maritime security forces. Such training and support could be expanded from orthodox maritime security force assistance by extending such assistance to "maritime militia," civilian fishing fleets and other craft that are organized (as does China) into flotillas that pursue or counter maritime territorial objectives.[149] In the East and South China Seas, friendly maritime militias, trained and supported by coalition maritime SOF, would counter China's use of its maritime militia as a gray zone technique.

UW is a fundamental SOF mission and would be a key tool in campaigns that employed gray zone techniques to counter adversary gray zone aggression. USSOF would thus have a central role should policymakers choose to counter adversary gray zone actions with their own gray zone activities that focused on directly denying the adversary's actions.

Employing SOF to Execute Gray Zone Punishments

Punishment strategies threaten to, or actually impose, costs that will compel an adversary to alter his aggressive behavior. As discussed in chapter 1, punishment strategies require a player to thoroughly understand what assets and conditions the adversary values. The player then requires a capability to hold those assets and conditions at risk, and the will to employ those capabilities, even when they are likely to result in painful consequences for the player that employs them.

Employing punishment with gray zone methods will come with advantages and drawbacks, when compared to overt and orthodox techniques. Policymakers may find punishments they inflict through the gray zone appealing because they are likely to be covert and thus deniable. Policymaker may be more ready to employ covert and deniable actions since they will not have to publicly explain and defend such actions. In addition, proxies and auxiliaries that execute the punishment methods may have specialized capabilities and authorities the principal player lacks, but which will be critical for the strategy's effectiveness.

On the other hand, there are drawbacks to employing punishment methods through the gray zone. Ethical questions avoided early on may return later, creating legal and political problems. More fundamentally for deterrence theory, players have more freedom to stop and withdraw covert and deniable threats and actions since these actions have not required any public commitment of prestige. If a player can easily withdraw from such a course of action, it will be a less credible and therefore less powerful coercive lever against an adversary. Policymakers may enjoy the greater variety of options available when including covert measures, but should not be surprised if they are not as coercive as hoped.

With those caveats, policymakers and planners should understand the wide variety of gray zone punishment techniques available, even if only to understand what adversaries could inflict on a player not planning to employ them himself. Gray zone punishments are likely to employ horizontal escalation, the extension of the conflict to new geographical areas or to involve new players as combatants. Gray zone punishments may also involve vertical escalation that will bring new classes of targets, assets, and interests under threat or actual attack.

Policymakers could call on SOF to employ its various offensive capabilities in clandestine and deniable ways. Such actions, when employed as coercive punishment designed to modify adversary behavior, could involve opening new operational fronts to pressure the adversary (horizontal escalation) or result in offensive action against new classes of assets and conditions most highly valued by the adversary (vertical escalation).

There are a wide variety of cost-imposing actions policymakers can impose that might employ all forms of national power: diplomatic, informational, military, and economic. Players can employ cost-imposing actions to weaken an adversary or to force him to divert scarce resources away from areas of interest to the player. For deterrence, a player would execute (or threaten to execute) cost-imposing actions in response to actions an adversary took, which the player warned (either generally or specifically) the adversary not to take.

For example, in the case of China's gray zone aggression in the East and South China Seas, cost-imposing actions the United States and its security partners in the region might take include highly-visible and frequent reports itemizing China's gray-zone activities, issued by government agencies and government-related institutions; greater security cooperation among countries in the region and greater involvement in security activities by friendly countries from outside the region; banning China and its companies from activity in the "strategic sectors" of allied countries, along with prohibitions on technology transfers to China; banishment of China from international organizations such as the G-20; the imposition of travel and security restrictions on Chinese citizens (including students) involved in security-related sectors; and United Nation-sponsored tribunal reviews of China's gray zone activities.[150] Information operations aimed at discrediting China's leaders and institutions by, say, exposing the wealth and corruption at the highest levels of the Chinese Communist Party, would be an even more aggressive example of a gray zone punishment response.[151]

Policymakers will hope these examples of nonmilitary courses of action would create coercion sufficient to alter the behavior of state-based adversaries. If insufficient however, even more aggressive military-based gray zone coercion could be required. U.S. and partner SOF would have important roles to play creating such gray zone coercion.

For instance, policymakers could call on SOF to execute an UW campaign somewhere outside the contested zone, employing horizontal escalation to impose costs on the adversary and draw away his resources. In the case of China, for example, policymakers could call on U.S. and partner SOF to support resistance movements in Tibet and Xinjiang province that oppose rule by the Chinese Communist Party.[152] SOF could also employ DA and special reconnaissance operations to target valuable leadership targets such as key commanders, command hubs and data networks, and key economic targets, especially those owned by top political leaders, their families, and close associates.[153] Finally, horizontal escalation could also extend to Chinese political and economic interests elsewhere in world, such as the assets of

Chinese state-owned enterprises in Africa and Latin America, which could be vulnerable to SOF DA and UW.[154]

As with China, Russia and Iran also have interests and assets that could be vulnerable to gray zone information operations, covert action, and perhaps UW. Policymakers could call on SOF to develop courses of action to hold these assets and interests at risk with a goal of applying coercion through clandestine means on key leaders.

According to classic deterrence theory, policymakers are likely to prefer denial courses of action because these actions act directly against the adversary's strategy and thus do not rely on other possibly unreliable linkages to be effective.

That said, there may be cases when effective denial courses of actions won't be available. In such cases, punishment and cost-imposing actions may be the only options remaining. As this section has explained, SOF will have a leading role in formulating and executing punishment and cost-imposing actions in the gray zone. The goal of these actions will be to coerce adversary leaders into more favorable behavior and policies. Operating in the gray zone may give the United States and its partners a wider variety of coercive options. SOF' skills, expertise, and statutory activities will be important assets for policymakers contemplating coercive actions in the gray zone.

Conclusion: Preparing SOF for Comprehensive Deterrence Operations

Deterrence remains the U.S. Department of Defense's principal method of preventing conflict; the department's mission statement and its main strategy documents make that clear. The department's practice of deterrence has successfully prevented major power wars for many decades. But, the DOD's legacy concept and execution of deterrence has frayed. Many state and non-state challengers have learned how to bypass the legacy deterrence framework, by crafting their strategies to avoid U.S. capabilities, or by operating in a murky gray zone, outside the traditional actions and mechanisms that would energize U.S. will and trigger a forceful response.

It now falls on U.S. and partner policymakers and planners to thoroughly understand the future operating environment and fashion new approaches to deterrence. A new comprehensive deterrence framework will encompass the deterrence-avoiding methods employed by recent and presumably future challengers. U.S. and partner SOF will have critical roles to play filling the gaps in the legacy deterrence framework exploited by hostile non-state and state actors that operate in the gray zone.

SOF will not have to learn new activities to play its expanded roles in a more effective and comprehensive deterrence framework. The statutory activities assigned to USSOF by Title 10 of the U.S. Code are relevant and sufficient for the tasks SOF will need to perform. The only change required is for policymakers and planners to shape and apply these statutory activities into tools that can deny hostile non-state actors and states operating in the gray zone their objectives. Policymakers and planners can also apply SOF activities to create coercive punishments that will convince adversary leaders and foot soldiers to desist from actions that harm U.S. interests. SOF' denial and coercive capabilities will add to a larger toolbox that includes all elements of national power. When the United States and its security partners demonstrate these capabilities and the will to employ them, they will increase the prospects for general deterrence, the DOD's principal method of preventing conflict, maintaining stability, and defending U.S. interests.

Chapter 3 showed cases from Israel's experience that demonstrate that hostile and well-supported non-state and proto-state actors can be deterred. Although it may appear that certain hostile non-state actors, especially those employing suicide tactics, cannot be deterred, Israel's experience shows this conclusion is likely a myth. Many of these groups do, in fact, have assets and interests a defender can hold at risk. The leaders of these groups have goals and interests that the defender's instruments of national power can deny the group from achieving. Perhaps most notably, Israel's several punitive campaigns against Hezbollah and Hamas have resulted in long periods of relative peace on Israel's frontiers with these groups. This supports the notion that coercion can work against even the most hardened and capable enemies. For these approaches against hostile non-state actors, SOF' DA, special reconnaissance, counterterrorism, information warfare, and UW skills will be crucial to a successful combined and joint campaign.

When policymakers decide to employ gray zone methods against adversary nation-states themselves operating in the gray zone, SOF will likely have leading roles in those campaigns. Major powers like China and Russia are bypassing the legacy deterrence framework through the use of gray zone techniques in Ukraine, the Baltics, and the East and South China Seas.

In order to prepare for these challenges, USSOF (for example, the 1st and 10th Special Forces Groups from the U.S. Army) will need some relief from commitments to the Central Command area, to allow training time and relationship-building for operations in east Asia and eastern Europe. To counter China's gray zone activities, U.S. and partner SOF will need to prepare for an adversary with high-end capabilities and large missile inventories designed to prevent access to the theater by U.S. and partner military forces. USSOF will need to deepen their knowledge of East Asia's languages and cultures, including those in Tibet and Xinjiang province. Much of the current gray zone challenge is in the maritime realm, which means that U.S. and partner SOF will require mastery of maritime special warfare and irregular warfare techniques.[155]

UW will likely be a critical technique for either denial or cost-imposition in the gray zone, so USSOF will have to be ready for such missions. Conducting UW against major or regional powers such as Russia, China, or Iran will require the training and skills to operate successfully in denied areas. SOF and the logisticians that support them in such challenging circumstances will need to master advanced techniques for gaining access to denied areas and then sustaining operations inside denied areas in spite of sophisticated adversary access barriers. SOF operators, logisticians, and planners should prepare for stealthy aerial and subsurface resupply, resupply tunneling, and acquiring advanced equipment and supplies that would reduce resupply requirements for operations inside denied areas.[156] Completing these preparations will make UW a more feasible option. That, in turn, will benefit deterrence, when potential adversaries understand that the United States and its security partners possess such capabilities, even in denied areas.

This monograph has explained the many capabilities SOF can add to an improved, comprehensive deterrence framework. Displaying, at least partially, these capabilities to potential adversaries will help those challengers understand how the United States and its partners can either thwart an adversary's strategy or impose painful costs in response to misbehavior. Current operations against ISIS and in support of Ukraine, give U.S. and partner SOF an opportunity to display these capabilities and demonstrate to others the will of the United States and its allies to employ them. Policymakers and SOF should take advantage of these opportunities to strengthen the building-blocks of deterrence. Doing so will prevent future conflicts, sustain security, and protect U.S. interests.

Endnotes

1. U.S. Department of Defense home web page, accessed 8 March 2017, https://www.defense.gov/.
2. U.S. Department of Defense, "The National Military Strategy of the United States of America 2015," 6, accessed 8 March 2017, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
3. U.S. Department of Defense, "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms," as amended through 15 February 2016, 67, accessed 8 March 2017, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
4. U.S. Department of Defense, *Deterrence Operations Joint Operating Concept* (Washington, D.C.: U.S. Department of Defense, 2006), accessed 3 January 2017, http://dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.
5. Ibid, Approval.
6. Ibid, 7.
7. Ibid.
8. Ibid, 4.
9. Ibid, 7.
10. Ibid, 9.
11. Ibid, 62-66.
12. The Fiscal Year 2017 National Defense Authorization Act, signed into law by President Obama on 23 December, 2016, authorized $59.5 billion for Overseas Contingency Operations such as Operations Inherent Resolve, the U.S. effort to support the Iraqi government's campaign against ISIS. See, House Armed Services Committee, "S. 2943 – The National Defense Authorization Act for Fiscal Year 2017 Summary," accessed 4 January, 2017, https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/wysiwyg_uploaded/NDAA%20final%20passage%20Summary%20FINAL.pdf.
13. The Obama administration requested $3.4 billion in fiscal year 2017 for the European Reassurance Initiative. See, Terri Moon Cronk, "European Reassurance Initiative Shifts to Deterrence," DOD News, Defense Media Activity, 14 July 2016, accessed 4 January 2017, https://www.defense.gov/News/Article/Article/839028/european-reassurance-initiative-shifts-to-deterrence.
14. *Deterrence Operations Joint Operating Concept*, 8.
15. The White House, "President Bush Delivers Graduation Speech at West Point," Office of the White House Press Secretary, 1 June, 2002, accessed 4 January 2017, http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html.

16. Ibid. Indeed, President George W. Bush in his seminal 2002 West Point speech, explained why in some cases deterrence would not be an appropriate concept.
17. Lawrence Freedman, *Deterrence* (Cambridge, United Kingdom: Policy Press, 2004), 110.
18. Ibid, 37-8.
19. Ibid, 38-9.
20. "Foreign Policy under President Eisenhower," U.S. Department of State, Office of the Historian, accessed 6 January 2017, https://history.state.gov/departmenthistory/short-history/eisenhower.
21. Freedman, *Deterrence*, 40-1.
22. "REFORGER," Globalsecurity.org website, 7 April 2011, accessed 7 January 2017, http://www.globalsecurity.org/military/ops/reforger.htm.
23. Freedman, *Deterrence*, 40-2.
24. Henry Kissinger, *The Necessity for Choice: Prospects of American Foreign Policy* (New York: Harper & Row, 1960), 12.
25. Thomas Shelling, *Arms and Influence* 2008 edition (New Haven, CT: Yale University Press, 2008), 92-9.
26. George H.W. Bush and Brent Scowcroft, *A World Transformed* (New York: Alfred A. Knopf, 1998), 490-2.
27. "Draft Memorandum from McNaughton to Robert McNamara, 'Proposed Course of Action re: Vietnam' (draft) 24 March 1965," Source: *The Pentagon Papers* Gravel Edition, Volume 3, pp. 694-702, accessed 9 January 2017, https://www.mtholyoke.edu/acad/intrel/pentagon3/doc253.htm.
28. Diane Pfundstein Chamberlain, *Cheap Threats: Why the United States Struggles to Coerce Weak States* (Washington, D.C.: Georgetown University Press, 2016), Introduction.
29. Alex Weisiger and Keren Yarhi-Milo, "Revisiting Reputation: How Past Actions Matter in International Politics," *International Organizations* 69, spring 2015, 473-4.
30. Robert McNamara, "Statement Made on Saturday 5 May by Secretary McNamara at the NATO Ministerial Meeting in Athens," 5 May 1962, National Security Archive – George Washington University, accessed 8 January 2017, http://nsarchive.gwu.edu/nukevault/ebb236/background%20doc%202.pdf.
31. Eric Schmitt, "U.S. Lending Support to Baltic States Fearing Russia," *The New York Times*, 1 January 2017, accessed 8 January 2017, http://www.nytimes.com/2017/01/01/us/politics/us-baltic-russia.html?_r=0.
32. *Deterrence Operations Joint Operating Concept*, 16.
33. Ibid, 15-6.
34. Ibid, 11.
35. Ibid, 12.

36. Ibid, 46-8.
37. Ibid, 47.
38. Ibid.
39. Ibid, 47-8.
40. Freedman, *Deterrence*, 28-32. See also chapter 3.
41. *Deterrence Operations Joint Operating Concept*, 29.
42. Ibid, 29-44.
43. Todd Harrison and Evan Braden Montgomery, "The Cost of U.S. Nuclear Forces: From BCA to Bow Wave and Beyond," Center for Strategic and Budgetary Assessments, 4 August 2015, 5, accessed 11 January 2017, http://csbaonline.org/publications/2015/08/the-cost-of-u-s-nuclear-forces-from-bca-to-bow-wave-and-beyond/.
44. *Deterrence Operations Joint Operating Concept*, 18, 65-6.
45. Ibid, 62-4.
46. Shelling, *Arms and Influence*, 66-9.
47. Freedman, *Deterrence*, 27-9.
48. *Deterrence Operations Joint Operating Concept*, 15-9.
49. "The 9/11 Commission Report," National Commission on Terrorist Attacks Upon the United States, 22 July 2004, 210-2, accessed 9 March 10, 2017, http://govinfo.library.unt.edu/911/report/911Report.pdf.
50. Ibid, 169.
51. Ibid, 171-3.
52. "Iran Sanctions," U.S. Department of the Treasury, Resource Center, updated 9 March 2017, accessed 9 March 2017, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx.
53. U.S. Department of State, *Country Reports on Terrorism* (Washington, D.C.: U.S. Department of State Publication, 2016), 300-1, accessed 19 January 2017, https://www.state.gov/documents/organization/258249.pdf.
54. "Nuclear Iran Uranium Enrichment," Institute for Science and International Security website, undated, accessed 19 January 2017, http://www.isisnucleariran.org/sites/by-type/category/uranium-enrichment/.
55. International Institute for Strategic Studies, *The Military Balance 2016* (Milton Park, United Kingdom: Routledge, 2016), 330.
56. "F-14 Tomcat," GlobalSecurity.org website, accessed 19 January 2017, http://www.globalsecurity.org/military/systems/aircraft/f-14.htm.
57. "Russian S-300 air defence missiles 'arrive in Iran,'" BBC News website, 11 April 2016, accessed 19 January 2017, http://www.bbc.com/news/world-europe-36013847.
58. Nazila Fathi, "Iran Threatens Retaliation if Attacked," *The New York Times*, 27 April 2006, accessed 19 January 2017, http://www.nytimes.com/2006/04/27/world/middleeast/27iran.html.

59. Michael Crowley, “Iran might attack U.S. troops in Iraq, U.S. officials fear,” Politico website, 25 March 2015, accessed 19 January 2017, http://www.politico.com/story/2015/03/could-iran-attack-us-troops-in-iraq-116365.

60. David Kirkpatrick, “Saudi Arabia Said to Arrest Suspect in 1996 Khobar Towers Bombing,” *New York Times*, 6 August 2015, accessed 21 January 2017, https://www.nytimes.com/2015/08/27/world/middleeast/saudia-arabia-arrests-suspect-khobar-towers-bombing.html?_r=0.

61. Kenneth Pollack, *The Persian Puzzle: The Conflict Between Iran and America* (New York: Random House, 2002), 278-302.

62. Greg Jaffe and Adam Entous, “As a general, Mattis urged action against Iran. As a defense secretary, he may be a voice of caution.” *Washington Post*, 8 January 2017, accessed 21 January 2017, https://www.washingtonpost.com/world/national-security/as-a-general-mattis-urged-action-against-iran-as-a-defense-secretary-he-may-be-a-voice-of-caution/2017/01/08/5a196ade-d391-11e6-a783-cd3fa950f2fd_story.html?utm_term=.a4f1902c28ad.

63. Hans Kristensen and Robert Norris, “Status of World Nuclear Forces,” Federation of Atomic Scientists website, 2017, accessed 23 January 2017, https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/.

64. Amy Woolf, “Nonstrategic Nuclear Weapons,” Congressional Research Service, 23 March 2016, 18-21, accessed 23 January 2017, https://fas.org/sgp/crs/nuke/RL32572.pdf.

65. *The Military Balance 2016*, 168.

66. Christopher Cavas, “Russian Submarine Hits Targets in Syria,” Defense News website, 8 December 2015, accessed 24 January 2017, http://www.defensenews.com/story/breaking-news/2015/12/08/submarine-russia-kalibr-caliber-cruise-missile-syria-kilo/76995346/.

67. Philip Kapusta, “The Gray Zone,” *Special Warfare Magazine*, Oct-Dec 2015, 20, accessed 9 March 2017, https://www.dvidshub.net/publication/issues/27727.

68. Nathan Freier, Project Director, *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: U.S. Army War College Press, 2016), 44.

69. “Georgia profile – Timeline,” BBC News website, 7 December 2016, accessed 25 January 2017, http://www.bbc.com/news/world-europe-17303471.

70. Vitaly Shevchenko, “Little Green Men or Russian Invaders?” BBC Monitoring website, 11 March 2014, accessed 25 January 2017, http://www.bbc.com/news/world-europe-26532154.

71. “Ukraine Crisis: What’s going on in Crimea?” BBC New website, 12 August 2016, accessed 25 January 2017, http://www.bbc.com/news/world-europe-25182823.

72. Ibid.

73. Shaun Walker, “Putin admits Russian military presence in Ukraine for first time,” *The Guardian*, 17 December 2015, accessed 25 January 2017, https://www.theguardian.com/world/2015/dec/17/vladimir-putin-admits-russian-military-presence-ukraine.

74. International Institute for Strategic Studies, *Strategic Survey 2015: The Annual Review of World Events* (Milton Park, United Kingdom: Routledge, 2015), 161-71.

75. Vincent Morelli, "Ukraine: Current Issues and U.S. Policy," Congressional Research Service report, 3 January 2017, 37-41, accessed 25 January 2017, https://fas.org/sgp/crs/row/RL33460.pdf.

76. Ibid, 40-1.

77. Terri Moon Cronk, "European Reassurance Initiative Shifts to Deterrence," DoD News, Defense Media Activity, 14 June 2016, accessed 26 January 2017, https://www.defense.gov/News/Article/Article/839028/european-reassurance-initiative-shifts-to-deterrence.

78. Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), 80-1.

79. U.S. Naval Institute and AFCEA WEST 2013 Conference, "Chinese Navy: Operational Challenge or Potential Partner?," 31 January 2013, accessed 26 January 2017, http://www.usni.org/events/2013-west-conference-exposition. Video: http://www.youtube.com/watch?v=nLrO1GI8ZIY&list=PLWX4R7nG6a8moZ0bIUtkBBIqaOkbr85zb&index=9, 21:02.

80. Mazarr, *Mastering the Gray Zone*, 84.

81. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016* (Washington, D.C.: U.S. Department of Defense, 2016), 13-20.

82. Andrew Erickson, "The South China Sea's Third Force: Understanding and Countering China's Maritime Militia," Testimony before the House Armed Services Committee Seapower and Projection Forces Subcommittee, 21 September 2016, accessed 26 January 2017, http://docs.house.gov/meetings/AS/AS28/20160921/105309/HHRG-114-AS28-Wstate-EricksonPhDA-20160921.pdf.

83. Mazarr, *Mastering the Gray Zone*, 85.

84. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016*, 13-20.

85. U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, D.C.: U.S. Department of Defense, 2012), 2.

86. "The World Factbook – China," United States Central Intelligence Agency, Transnational Issues tab, accessed 27 January 2017, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html.

87. Ben Dolven, Mark Manyin, and Shirley Kan, "Maritime Territorial Disputes in East Asia: Issues for Congress," Congressional Research Service report, 14 May 2014, 3, accessed 27 January 2017, https://fas.org/sgp/crs/row/R42930.pdf.

88. Robert Haddick, "Salami Slicing in the South China Sea," Foreign Policy website, 3 August 2012, accessed 27 January 2017, http://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/.

89. Eric Heginbotham, et al, "An Interactive Look at the U.S.-China Military Scorecard," RAND Corporation Project Air Force, 14 September 2015, accessed 27 January 2017, http://www.rand.org/paf/projects/us-china-scorecard.html.
90. "The World Factbook – China," United States Central Intelligence Agency, Economy tab.
91. Adam Elkus, "50 Shades of Gray: Why the Gray Zone Concept Lacks Strategic Sense," War on the Rocks website, 15 December 2015, accessed 30 January 2017, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.
92. Michael Mazarr, "Struggle in the Gray Zone and World Order," War on the Rocks website, 22 December 2015, accessed 31 January 2017, https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/.
93. Freier, *Outplayed: Regaining Strategic Initiative in the Gray Zone*, 67-8.
94. *Deterrence Operations Joint Operating Concept*, 18-9.
95. Graham Allison, "Why ISIS Fears Israel," The National Interest website, 8 August 2016, accessed 14 February 2017, http://nationalinterest.org/feature/why-isis-fears-israel-17286.
96. Ibid.
97. Ron Tira, "Israel's Second War Doctrine," *Strategic Assessment*, Vol. 19, No. 2, July 2016, 143-6.
98. Ibid.
99. Allison, "Why ISIS Fears Israel."
100. Doron Almog, "Cumulative Deterrence and the War on Terrorism," U.S. Army War College *Parameters*, Winter 2004-5, 6, accessed 15 February 2017, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/04winter/almog.pdf.
101. Ibid, 11-12.
102. Ibid, 13-14.
103. Ibid, 7-8.
104. Gadi Eisenkot, "IDF Strategy," August 2015, English translation from the Belfer Center for Science and International Affairs website, Harvard University, 4-5, accessed 15 February 2017, http://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf.
105. Ibid, 24-5.
106. Ibid.
107. *Deterrence Operations Joint Operating Concept*, 65-7.
108. Eisenkot, "IDF Strategy," 24-5.
109. Tira, "The War Doctrine Israel Does Not Talk About."
110. Timothy McCulloh and Richard Johnson, *Hybrid Warfare* (Tampa, FL: Joint Special Operations University Press, 2013), 20-5.

111. Rory McCarthy, "Hizbullah leader: we regret the two kidnappings that led to the war with Israel," *The Guardian*, 27 August 2006, accessed 16 February 2017, https://www.theguardian.com/world/2006/aug/28/syria.israel.

112. Allison, "Why ISIS Fears Israel."

113. "10 U.S. Code §167 – Unified combatant command for special operations forces," Cornell University Law School, Legal Information Institute website, accessed 16 February 2017, https://www.law.cornell.edu/uscode/text/10/167.

114. *Deterrence Operations Joint Operating Concept*, 46-8.

115. For example, from May 2010 through April 2011, U.S. SOF in Afghanistan conducted 2,245 counterterrorism missions. See Jim Thomas and Chris Dougherty, *Beyond the Ramparts: The Future of U.S. Special Operations Forces* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2013), 18-9.

116. On May 2, 2011, U.S. President Barack Obama delivered a live address from the White House, revealing that U.S. personnel had raided a compound in Abbottabad, Pakistan and killed Osama bin Laden during a firefight. See "Osama bin Laden Dead," Obama White House Archives, May 2, 2011, accessed 8 June 2017, https://obamawhitehouse.archives.gov/blog/2011/05/02/osama-bin-laden-dead. In 2013, Columbia Pictures Industries, Inc. released *Zero Dark Thirty*, a dramatic film portrayal of the hunt for and raid on Osama bin Laden. The film was released to the public in 62 countries. See, http://www.imdb.com/title/tt1790885/releaseinfo?ref_=tt_dt_dt, accessed 8 June 2017. For former Secretary of Defense Leon Panetta's comments on Operation Neptune Spear, see "Panetta: U.S. Remains Focused on Pursuit of al-Qaida," accessed 18 August 2017, http://archive.defense.gov/news/newsarticle.aspx?id=116122.

117. Thomas and Dougherty, Beyond the Ramparts, 6.

118. "Our Mission," Combined Joint Task Force – Operation Inherent Resolve Fact Sheet, undated, accessed 18 February 2017, http://www.inherentresolve.mil/Portals/14/Documents/Mission/Mission.pdf?ver=2016-03-23-091705-717.

119. Adam Lowther, "Deterring Nonstate Actors," *Thinking about Deterrence: Enduring Questions in a Time of Rising Power, Rogue Regimes, and Terrorism*, Adam Lowther, editor (Montgomery, AL: Air University Press, 2013), 208.

120. Ibid, 210-1.

121. Benjamin Lambert, *Air Operations in Israel's War Against Hezbollah: Learning from Lebanon and Getting it Right in Gaza* (Santa Monica, CA: The RAND Corporation, 2011), xiii.

122. Ibid, xviii, xxi.

123. Ibid, 35.

124. Ibid, 158.

125. Ibid, 30-3.

126. Ibid, 36-8.

127. Ibid, 175.

128. Ibid, 158-162.

129. Ibid, 157-8, 176.

130. Ibid, 18-9.

131. See "Department of Defense Law of War Manual," Office of General Counsel, U.S. Department of Defense, June 2015, accessed 20 February 2017, https://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf.

132. Almog, "Cumulative Deterrence and the War on Terrorism," 14-5.

133. David Ellis, Charles Black, Mary Ann Nobles, "Thinking Dangerously: Imagining United States Special Operations Command in the Post-CT World," *Prism*, Vol. 6, No. 3, 2016, 115-6.

134. "U.S. Relations with Iran," U.S. Department of State, U.S. Bilateral Relations Fact Sheets, Iran, undated, accessed 2 March 2017, https://www.state.gov/r/pa/ei/bgn/5314.htm.

135. "U.S. Relations with Russia," U.S. Department of State, U.S. Bilateral Relations Fact Sheets, Russia, 20 December 2016, accessed, 2 March 2017, https://www.state.gov/r/pa/ei/bgn/3183.htm.

136. Eric Schmidt, "U.S. Lending Support to Baltic States Fearing Russia," *New York Times*, 1 January 2017, accessed 2 March 2017, https://www.nytimes.com/2017/01/01/us/politics/us-baltic-russia.html?_r=2.

137. Thomas and Dougherty, *Beyond the Ramparts*, 71.

138. Neil Hollenbeck and Benjamin Jensen, "Seeing Gray in the Next World War," War on the Rocks website, 21 February 2017, accessed 26 February 2017, https://warontherocks.com/2017/02/seeing-gray-in-the-next-world-war/.

139. Shevchenko, "Little Green Men or Russian Invaders?"

140. Geoff Dyer and Demetri Sevastapulo, "US strategists face dilemma over Beijing claim in South China Sea," *Financial Times*, 9 July 2014, accessed 1 March 2017, http://www.ft.com/intl/cms/s/0/b2176dea-0732-11e4-81c6-00144feab7de.html%23axzz3AkKMjTAs.

141. Michael Forsythe, "Rex Tillerson's South China Sea Remarks Foreshadow Possible Foreign Policy Crisis," *The New York Times*, 12 January 2017, accessed 27 February 2017, https://www.nytimes.com/2017/01/12/world/asia/rex-tillerson-south-china-sea-us.html?_r=0.

142. Shelling, *Arms and Influence*, 141-53.

143. Robert Haddick, *Fire on the Water: China, America, and the Future of the Pacific* (Annapolis, MD: Naval Institute Press, 2014), 206-7.

144. Thomas and Dougherty, *Beyond the Ramparts*, 66-70.

145. International Institute for Strategic Studies, *The Military Balance 2017* (Milton Park, United Kingdom: Routledge, 2017), 12.

146. See Joseph Votel, Charles Cleveland, Charles Connett, and Will Irwin, "Unconventional Warfare in the Gray Zone," *Joint Forces Quarterly* 80 (1st Quarter,

January 2016), accessed 26 April 2017, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

147. Geoffrey Pyatt, "Helping Ukraine Defend Itself," U.S. Embassy Kyiv Blog, 25 January 2016, accessed 3 March 2017, https://usembassykyiv.wordpress.com/tag/special-operations-force/.

148. Andrew Kramer, "Spooked by Russia, Tiny Estonia Trains a Nation of Insurgents," *New York Times*, 31 October 2016, accessed 4 March 2017, https://www.nytimes.com/2016/11/01/world/europe/spooked-by-russia-tiny-estonia-trains-a-nation-of-insurgents.html.

149. See Erickson, "The South China Sea's Third Force: Understanding and Countering China's Maritime Militia."

150. Ross Babbage, *Countering China's Adventurism in the South China Sea* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2016), 58-9.

151. Ibid, 60-1.

152. Robert Haddick, Challenges in the Asia-Pacific Theater for U.S. and Partner Nation Special Operations Forces (Tampa, FL: Joint Special Operations University Press, 2014), 66-7.

153. Ibid, 68-9.

154. Ibid, 67.

155. Ibid, 70-1.

156. Robert Haddick, *Improving the Sustainment of SOF Distributed Operations in Access-Denied Environments* (Tampa, FL: Joint Special Operations University Press, 2016), 57-63.