

A PERILOUS FUTURE: HIGH-INTENSITY CONFLICT AND THE IMPLICATIONS FOR SOF



EDITOR

Lieutenant-Colonel Andrew L. Brown, PhD

Special Operations Forces and
Great Power Competition



A PERILOUS FUTURE: HIGH-INTENSITY CONFLICT AND THE IMPLICATIONS FOR SOF

**Special Operations Forces
and Great Power Competition**

A PERILOUS FUTURE

**HIGH-INTENSITY CONFLICT AND
THE IMPLICATIONS FOR SOF**

EDITOR

LIEUTENANT-COLONEL ANDREW L. BROWN, PhD

Copyright © 2022 Her Majesty the Queen, in right of Canada as represented by the Minister of National Defence.



Canadian Special Operations Forces Command
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Produced for CANSOFCOM Education & Research Centre
by 17 Wing Winnipeg Publishing Office.
WPO32160

Front / Back Cover Images: CANSOFCOM

ISBN 978-0-660-43779-8 (print)

ISBN 978-0-660-43778-1 (PDF)

Government of Canada Catalogue Number D2-619/2022E (print)

Government of Canada Catalogue Number D2-619/2022E-PDF (PDF)

Printed in Canada.

1 3 5 7 9 10 8 6 4 2

DISCLAIMER

The views expressed in this publication are entirely those of the authors and do not necessarily reflect the views, policy, or positions of the Government of Canada, the Department of National Defence, the Canadian Armed Forces or any of its subordinate units or organizations, the United States Government, United States Department of Defense or any of its subordinate units or organizations, or the editors.

TABLE OF CONTENTS

PREFACE	iii
INTRODUCTION	1
	The Most Dangerous Case: SOF in Conventional Conflict with Strategic Competitors Dr. James Kiras and Captain Nicolas Provencher
CHAPTER 1	17
	Theatre Break-In Lieutenant-Colonel Andrew L. Brown
CHAPTER 2	35
	Crisis Contingencies Colonel (Retired) Peter McCabe, PhD and Lieutenant Colonel Nicholas J. Kramer
CHAPTER 3	59
	Emerging Horizons for Special Operations Lieutenant Colonel Keith L. Carter, PhD
CHAPTER 4	73
	Future Technologies for Special Operations Forces Tony Balasevicius
CHAPTER 5	87
	SOF Organizational Considerations Lieutenant Colonel C.G. Landry
CONCLUSION	107
	Never Say Never: Final Thoughts on the Implications for SOF of in High-Intensity Warfare Colonel (Retired) Bernd Horn, PhD
CONTRIBUTORS	127
GLOSSARY OF ABBREVIATIONS	131
NOTES	133
INDEX	163

PREFACE

During the period 29 August to 2 September 2021, a number of American and Canadian military practitioners, defence scientists, academics, and subject matter experts gathered at Canadian Forces Base Kingston, in Ontario, Canada, to discuss Great Power Competition (GPC) and the implications for Special Operations Forces (SOF). The assembled researchers broke into four sub-working groups, each group focusing on their assigned topic, namely the Arctic, Battle for the Narrative, High-Intensity Conflict, and the Gray Zone.

Importantly, each sub-working group was responsible for producing a volume specifically on their respective topic. Significantly, the intent was not to reproduce the reams of data that already exist on all of these topics, but rather to “operationalize” the research in such a manner that SOF teams can utilize the information to provide context and clarity to the potential challenges, risks, and tasks they may face in the respective environments.

The net result of the Canadian Special Operations Forces Command/U.S. Special Operations Command, Joint Special Operations University Research Working Group is a three-volume SOF and GPC series that deals with each of the aforementioned topics. Our intent is that each of the volumes, taken individually and collectively, will enhance the understanding of GPC in the SOF community, as well as the military and public at large.

As a final comment, it is important to note that the February 2022 Russian invasion of Ukraine occurred shortly before the publication went into production and as such it does not include substantive observations or lessons that have arisen from that conflict.

Bernd Horn
Colonel (retired), PhD
Series Co-Editor

Peter McCabe
Colonel (retired), PhD
Series Co-Editor

INTRODUCTION

THE MOST DANGEROUS CASE: SOF IN CONVENTIONAL CONFLICT WITH STRATEGIC COMPETITORS

DR. JAMES KIRAS and CAPTAIN NICOLAS PROVENCHER

Change in the national security realm is driven by several factors. They range from the most severe, including failure or catastrophe, to the trifling, in pursuit of the latest fad or ostensibly “new” idea. In other cases, change results from the decision of national leaders to depart from well-established strategy in favour of evolving national security priorities. Such was the case with the publishing of the American National Security Strategy (NSS) in 2017. The NSS and its host of subordinate documents, including the National Military and National Defense Strategies (NMS and NDS), introduced several new terms to the defence planning and policy communities, such as “principled realism” and “great power competition.” The former term put allied and partner nations on notice that the United States would place its interests first and would spur more equitable alliance cost and burden sharing. The latter term was designed to reorient the defence community away from irregular threats, including terrorist groups, to focus more on the problems presented by rising or revanchist states such as the People’s Republic of China and Russia. The NSS recognized that previously, in addressing one set of global threats, the scourge of violent extremist terrorism, the United States and its allies had overlooked a growing challenge:

Success, however, bred complacency. A belief emerged, among many, that American power would be unchallenged and self-sustaining. The United States began to drift. We experienced a crisis of confidence and surrendered our advantages in key areas. As we took our political, economic, and military advantages for granted, other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States, our allies, and our partners.¹

INTRODUCTION

In the last two decades, few organizations within the defence community could match the success of the specialized world of special operations. Special Operations Forces (SOF) responded with remarkable energy and speed to confront the challenge posed by the regional and global threat of violent Islamic extremism, whose agents killed more people in a single day, 11 September 2001, than the member states of the North Atlantic Treaty Organization (NATO) suffered in twenty years of engagement in Afghanistan.² Key among the SOF responses was the refinement and expansion of a targeting methodology, in which intelligence collection, assessment, and SOF actions worked together symbiotically to tear apart the close-knit fabric of terrorist networks.³ More importantly, the pace and intensity of SOF actions inhibited the ability of terrorist networks to heal, regenerate, and coordinate for large-scale attacks.⁴

But a complacency of a different sort has accompanied SOF success. Twenty years of successful activities across the globe has bred that a state of comfort. Western SOF, including those of the United States and Canada, settled into a routine in which success against terrorist groups was all but assured and public confidence and political support unquestioned. Terrorist opponents seldom challenged SOF skills at the point of contact. Some SOF seemingly overcame decades of marginalization, neglect, and misuse;⁵ political access, influence, and confidence remained high and SOF were the “force of choice” for national security leaders given their willingness and ability to address crises quickly and efficiently, at low cost and with minimal risk.⁶ In addition to skill, a foundational element of SOF success was a voracious appetite for resources, including support from other government departments, agencies, and ministries whose representatives rarely denied requests. Almost no task seemed beyond the ability of SOF to address, from counter-terrorism and hostage rescue to counter-proliferation and security assistance.

SOF pre-eminence, however, has been challenged by the shift in national security discourse and resource prioritization since 2017, in the recognition of first “great power” and now “strategic” competition. Shifts are necessary given budgetary instability, defence force cuts, the pursuit of technological offsets for numbers, a “procurement holiday” in conventional capabilities, and “sclerotic” capability acquisition.⁷ Conventional forces have responded to the call of competition by producing new mission and vision statements

INTRODUCTION

that outline the capabilities they wish to acquire.⁸ In addition, operating domains and environments in which the U.S. has dominated recently, such as the space and the information domains, are now the focus of energy and effort, including the creation of new organizations and the establishment of separate armed services, all in the name of “transformation.”⁹ SOF have lost their pre-eminent position in national security discussions to find themselves increasingly trapped within a policy dilemma: sustaining operations against violent extremist threats no longer at the forefront of national security priorities, while at the same time divining their role and developing capabilities to contribute to potential future conventional conflict with states like Russia and China.

PURPOSE OF THIS VOLUME

The SOF response to the challenges identified above has been a wide-ranging mix. In some cases, it has involved the rediscovery of lost or neglected missions and skillsets brought into focus by adversary actions, such as the conduct of strategic sabotage and “unconventional warfare” that paved the way for Russia’s rapid annexation of Crimea in 2014.¹⁰ Others are characterized by attempts to connect the operating environment with concepts designed to retain SOF relevance and pre-eminence such as “unconventional deterrence.”¹¹ Yet a third category seeks to rebalance and transform capabilities in the name of preparing future requirements while at the same time reducing current ones, which faces institutional and cultural resistance. Such rebalancing and transformation are necessary, given SOF is at a “strategic inflection point” and to ensure institutional capabilities and preferences are aligned with needs of the Joint Force in future conflict.¹² This book, then, seeks to support such efforts to orient SOF to the operating environment associated with the rise of great power competitors, specifically SOF’s potential role(s) in high-intensity war.

The authors of this monograph met for three days of brainstorming and discussion in a workshop on “SOF and the Great Power Competition,” sponsored by the Canadian Special Operations Forces Command (CANSOFCOM) and the Joint Special Operations University (JSOU). Their backgrounds are academic and/or operational, within the SOF and conventional communities, and reflect a range of experiences and different national perspectives. The charter for this group was to explore SOF’s “potential roles, challenges and

INTRODUCTION

requirements” for “conventional/high-intensity conflict.”¹³ Other groups at the workshop examined further aspects of SOF in great power competition, such as the Arctic, narrative struggles and grey zone competition, as part of a project to create new scholarship for the SOF community and its stakeholders. While the task set for this group was somewhat easier than for other groups, given its well-defined focus, the authors were confronted with some particular challenges. These included orienting towards the future operating environment (especially its high-intensity aspects), appreciating its key characteristics, and mapping out potential SOF tasks, roles, and requirements for different phases of conventional conflict.

During our exploration of the problem the authors settled on three overarching but interrelated objectives. The first is providing intellectual fodder for the mindset of current SOF members and leaders. This mindset is the foundation for SOF success and is based on a willingness to experiment and consider unorthodox solutions to solve challenging problems. Other factors contribute to SOF success too. For one thing, SOF remain peerless problem-solvers at the tactical level. SOF tactical action, however, must be linked to broader operational or strategic aims. In addition, most SOF roles and missions are limited in geographic space and time, as well as in combat intensity against, since 2001, non-state actors. However, most Western SOF have not faced a marginally competent, much less capable peer or near-peer state opponent in more than seventy years, including state security forces operating in brigade, divisional, or greater strength. Consequently, much of SOF training and education privileges the contemporary and most recent lessons learned, and American SOF in particular view historical experience with a somewhat dismissive or jaundiced attitude, if at all. In terms of resourcing and risk, part of SOF success is based on dealing with risk to mission and risk to force by increasing the resources allocated, including conventional force support. When SOF have run into trouble against terrorist opponents, they have been able to draw swiftly on a pool of conventional fire and manoeuvre forces. SOF combat fatalities, when they have occurred in more recent campaigns, have been limited to an average, in the case of the United States, to twenty-two per year against an average of 8,000 personnel deployed overseas.¹⁴

To assist SOF in appreciating the implications of great power competition, the authors have a second purpose: presenting an evaluation of future

INTRODUCTION

conventional conflict – or at least its primary characteristics. We are well-aware of the pitfalls associated with prediction, described in popular terms as a “fool’s errand,” given the existence of “black swan” or unanticipated events or issues.¹⁵ Rather than presenting our best guess, the authors draw upon a wide range of futures assessments from official and unofficial sources, including Chinese and Russian writings. Technological changes mean that future conventional wars will, in many ways, be fought differently than in the past. The authors seek to identify the most common attributes and characteristics identified in sources, connect them with current and emerging technology, and match them up against potential SOF tasks. Part of clarifying the future environment is defining and explaining the phases and characteristics the authors developed in the course of the teamwork.

The authors’ third and last purpose is to help answer one of the most vexing questions confronting SOF: what is their “value proposition” in conventional conflict? This question portends several considerations. They include the relevance of SOF to the Joint Force in potential future high-intensity conventional conflict. The idea that SOF should support, as opposed to being supported by, conventional forces runs counter to the experience of most serving and recently retired operators. Indeed, it is not too strong to say the notion is an anathema to them due to their more recent pre-eminence and influence. SOF have struggled in national security discussions to reassess their role, or argue for new capabilities, and can default instead to current successes and the mystique surrounding them. Taking a hard, objective look at potential future realities will encourage SOF to evaluate how they can contribute to success and, more importantly, where they cannot. Understanding their limitations in future conventional conflict will assist SOF in avoiding the twin traps into which they have fallen in the past: expected and being asked routinely to do the impossible by those unfamiliar with them, particularly civilian decision makers and senior conventional military leaders who have been accustomed to SOF success; and, identifying their limitations to better identify where they should not be used, where old capabilities might be shed, and where new ones should be developed.

KEY CHARACTERISTICS OF THE FUTURE CONVENTIONAL OPERATING ENVIRONMENT

Central to our inquiry here is the term “conventional.” Considerable energy has been spent developing and refining typologies of conflict and distinguishing between different and ostensibly unique forms and methods of warfare, including irregular, unconventional, and the like. Often such efforts descend into exercises in pedantry or displays of cleverness, with marginal utility at best for the planner or war fighter. The special operations community is not innocent of such efforts, some of which go to great lengths to distinguish what constitutes a “special” operation versus what is not.¹⁶ In an ironic twist, American conventional forces do not define themselves in joint doctrine. Rather, they are defined in special operations doctrine (JP 3-05), and by extension the *Joint Dictionary*, as a means of distinguishing them from SOF: “1. Those forces capable of conducting operations using nonnuclear weapons. 2. Those forces other than designated special operations forces.”¹⁷

We define conventional conflict as that involving the standing armies, navies, and air forces of at least one state against another. Further, we scope conventional conflict to that involving a state, or group of states, against another with roughly equivalent net military power and capability, or “peer” and “near-peer” states. Canadian doctrine defines the conventional adversary in the following way: “The conventional adversary will have a definitive structure and identifiable order of battle. It will likely be an extension of a political government and have a recognizable, institutional doctrine, known rules of engagement, and known intelligence assets. In other words, it will be a recognizable military force.”¹⁸

Some combatants will mirror image their opponents or think they will behave and fight according to one’s own conceptualizing, understanding, and experience of war. Nothing can be further from the truth. We concluded that conventional conflict is not normative, in the sense of a set standard or fixed pattern of behaviour but is rather relative based on an opponent’s culture and circumstances. Perhaps the best way to understand “conventional,” as it relates to conflict, is according to a set of capabilities, expectations, and preferences. Military surprise often results from subtle but important differences in capabilities, expectations, and preferences on

INTRODUCTION

a host of issues ranging from the need for formal agreement and declaration prior to hostilities to the use of “unconventional” weapons on the battlefield. Put simply, Russian and Chinese military authors view the spectrum and threshold of conflict and what constitutes “conventional” in ways that differ slightly from most Western militaries. One example illustrates this point starkly. During the Cold War, NATO forces assumed that their use of tactical nuclear weapons would automatically trigger escalation by the Soviet Union with its nuclear arsenal, or “first strike,” as it would on Soviet use. Soviet doctrine, however, distinguished between tactical or battlefield use (first use, in a limited theatre war) and strategic (first strike, or intercontinental war), based on their understanding of conflict and organizational structures.¹⁹ In the words of one scholar:

The essential difference between the Soviet and the NATO view of conventional warfare in the nuclear age has been the Russian belief throughout that offense is the best form of defense. The ability and willingness to take the offensive, in order to pre-empt the enemy’s offensive if possible, has been a consistent theme of their military thinking, training, and organization, applied equally to nuclear and conventional warfare, which, for most of the period, they have refused to regard as separate.²⁰

Another attribute identified by the workshop participants is that “conventional conflict,” in the broad Western understanding of the term, usually connotes the involvement of several nations working together. Stated simply, the participants had difficulty envisioning a scenario, involving a peer or near-peer state, where a Western nation would operate unilaterally in its military operations. Even with its military capabilities, the United States seeks to involve alliance, coalition, or other partner states, for reasons of burden and cost-sharing, as well as legitimacy. Little suggests this trend will not continue in future conventional conflict.

Forecasting the nature of future conflicts is inherently difficult and often produces inaccurate results, but nevertheless remains a necessary evil for militaries. Defence budgeting, for instance, must consider short-term predictions to ensure funds are allocated programmatically. Acquisitions in defence, while both problematic and pilloried for their glacial pace of progress, take considerable time and involve forecasting of cutting-edge

INTRODUCTION

capabilities and turning these into specified requirements for increasingly complex platforms and systems. One contemporary combat aircraft, the F-35 Lightning II fighter, runs on software comprising between eight-to-ten million lines of code and the weapon system, including its logistics, maintenance, and mission software, some 24-35 million lines, according to media reports – all to make the aircraft useful for future conflicts and situations that planners cannot fully foresee today.²¹ Within peer and near-peer states, military theorists consider forecasting a part of military science that should result from systematic study of capabilities and ongoing operations, periodically reviewed to take account of changes, to aid in the development of new forms and methods of combat.²² None of the workshop participants claim specialized knowledge in defence forecasting but their collective experience, research, and writing offered four general traits that experts, including peer competitors, suggest will characterize the future conventional operating environment.

The first characteristic is the *speed and tempo* of future warfare. Current and emerging technologies will influence speed and tempo in several ways. One is shortening decision-making cycles, with automated processes using artificial intelligence and machine learning to achieve an advantage over a competitor. Technology is already generating both massive amounts of threat and contextual information and an ability to process it all, making for rapid intelligence and operational planning cycles. Technology will also influence speed and tempo through capabilities that drastically reduce manoeuvre and fires time, such as with Russia's Zircon and the People's Republic of China's (PRC's) DF-17 hypersonic missiles.²³ Chinese military thinking views technology making the speed and tempo of war "rapider and rapider," influencing the relationship that exists between offence and defence.²⁴ Speed and tempo are not only affected by technology but also how it operates in different domains. The air, space, and cyber or informational domains, and the technologies used within them, both compress space and shorten time horizons. In the case of the cyber or informational domain, effects can be nearly instantaneous globally – and potential great power competitors recognize these factors. For example, in a recent report to Congress, the Office of the Secretary of Defense assessed that

The PLA [People's Liberation Army] argues that the implementation of 'intelligentized' capabilities will increase the speed of future

INTRODUCTION

combat, necessitating more rapid processing and fusing of information to support quick and efficient command decision making. Victory in future warfare, according to PLA strategists, will depend upon which side can more quickly and effectively observe, orient, decide, and act in an increasingly dynamic operating environment.²⁵

In order to prevent inadvertent escalation of a conventional conflict into a nuclear one, Chinese writings stress the need for controlling the conflict: “Controlling the tempo is to control the crisis’ development speed and the rise and fall of changes, avoiding the crisis going towards the edge of losing control.”²⁶ The risk inherent in not adapting to the pace of future operations can be grave indeed, which, again, potential great power challengers recognize. According to one veteran analyst of the Russian military, its theorists have concluded that “Planning tomorrow for a surprise development today (hypersonic weapons) is more than a day late, as the contemporary information environment’s impact on the [Initial Period of War] may even result in the conflict’s end before it starts, if enough capabilities/resources are destroyed or compromised.”²⁷

Future conventional warfare will also be characterized by *interconnectedness*. In its simplest terms, interconnectedness harnesses different means and technology to gather and fuse together information from a range of different systems, across domains, to ensure the most relevant, effective, and efficient application of lethal and non-lethal force. There are two dimensions of interconnectedness, related to the means of conventional conflict as well as its ways. In terms of means, the goal is to create an interlinked “system of systems” emblematic of an ongoing revolution in military affairs driven by the United States, beginning with Joint Vision 2020 (JV2020)²⁸ and most recently manifested in the concept for Joint All Domain Operations (JADO).²⁹ Ultimately faster, better sensing will lead to more accurate shooting; this point is developed more fully in the discussion of lethality and risk below.

In terms of ways, the very character of war has radically altered, according to Russian and Chinese writers, evident in United States military operations since Operation Desert Storm in 1991. These writers acknowledge the role of technology but stress another aspect: difficulty distinguishing or separating out activities across a range of formerly discrete categories. Russian General Valery Gerasimov observed “a tendency toward blurring

INTRODUCTION

the lines between states of war and peace” and the ability to achieve military objectives through non-military, or concealed military, methods.³⁰ The same interconnectedness and blending occurs throughout the depth of the battlespace, between levels of war (strategic, operational, and tactical), as well as in modes of operation (offence and defence).³¹ Paradoxically, the pursuit of the means to improve coordination and increase the efficiency of declining numbers of more capable systems on the battlefield can increase ambiguity and uncertainty by erasing the lines between the tactical, operational, and strategic.³²

At first glance *interconnected* seems to be indistinguishable from the next characteristic, *informatized*. There is a subtle but useful difference between the two, according to the authors. The former refers to the relationship of military forces to the environment, and more specifically, their ability to make sense in an effort to reduce the effects of friction, chance, and uncertainty well known in operations. Informatized, however, refers to the effect on military forces within the environment – that is, the ability to be monitored, identified, and tracked by military systems and as a result of the increasingly prevalent “internet of things.” Information technologies now make undetected and undetectable movement much more difficult.

For instance, during Moscow’s 2014 foray into Eastern Ukraine, social media and commercial satellite imagery analysis, by analysts from the Atlantic Council, pieced together the movement of Russian military forces, including mobile surface-to-air systems, from their cantonment areas into Ukrainian territory.³³ Detection and posting of information about high-risk special operations has occurred relatively recently, most famously in a series of tweets posted by Sohaib Athar during the raid that resulted in the death of Osama bin Laden on 1 May 2011.³⁴

Other implications for special operations are evident in the difficulties experienced by intelligence operatives operating in foreign countries, due to the increasing ubiquity of biometrics, smartphones, and surveillance cameras.³⁵ Future enduring operations will be confronted by the challenge of social monitoring even to the degree of China’s infamous “social credit system,” which allegedly tracks the behaviour and trustworthiness of citizens and organizations, and applies a social credit score to each.³⁶ To sum up, an informatized conventional operating environment is one in which the

INTRODUCTION

undetected massing of combat power will be extremely difficult given the transparency of future battlefields.³⁷

The fourth and final characteristic identified by the group relates to the *lethality* of the future conventional operating environment and its impact on assessments of risk. Historically, mass was an important consideration, in terms of number of forces, their concentration and density, as well as weight of fires. Quantity has given way to quality, and more specifically, to precision and accuracy. Soviet writers, and in particular Nikolay Ogarkov, identified an ongoing scientific-technical revolution in military operations in the early 1980s.³⁸ The pace of technological change since then has only increased, according to the observations and assessments of peer and near-peer competitors of U.S. and coalition military operations over the past thirty years. Gerasimov states categorically:

Frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals. The defeat of the enemy's objects [objectives] is conducted throughout the entire depth of his territory...The application of high-precision weaponry is taking on a mass character.³⁹

Other Russian writers echo Gerasimov's ideas about future warfare. Valeriy Kiselev notes a different blurring of lines between forms of war but also stresses the following:

Future war must envision how long-range hypersonic guided missiles (such as Russia's Yu-71 Glider) will work with reconnaissance and strike systems and electronic warfare systems to both uncover adversary plans and targets and then to take them out with the correct mixture of exposure, control, and destruction means.⁴⁰

Kiselev is pointing out the convergence of speed and tempo, interconnect- edness, informatized, and lethality, all of which require further study and concept development. The convergence of these characteristics has significant implications for future conventional operations, especially an emphasis on detecting and shooting first to cripple the enemy system, and setting the initial conditions for operations in your favour, while avoiding concentrated

INTRODUCTION

basing or massed forces to prevent their destruction. The implications of the characteristics are clear: the need for greater automation in decision-making and execution, the fielding of more semi-autonomous and autonomous weapons systems to collect information and generate lethal and non-lethal effects, and an increasing ability to avoid closing with the enemy in order to destroy, disable, or cripple them without incurring friendly casualties – “contactless war.”

The convergence of the characteristics of the future conventional operating environment has implications for decision-making, and more specifically, deciding to employ SOF, given different calculations of risk. Dr. Bernd Horn defines risk in rational, cost-benefit calculation terms in the following way:

Risk is influenced by the perspectives of individuals, groups and / or institutions. Through these subjective filters, risk, as perceived by a specific entity, is the probability of positive or negative consequences stemming from a given action or decision as weighed against the perceived benefit. The consequences can be in the form of a reward (e.g., fame, fortune) or damage or injury (e.g., physical harm, financial loss, damage to reputation) to individuals, groups or institutions.⁴¹

SOF have been used so frequently over the past twenty years because of their discretion, high likelihood of success, low probability of adverse or negative consequences politically, and relatively low cost in terms of resources and casualties. In short, SOF are desirable politically and strategically as a means to both mitigate and manage the risk presented by a relatively modest policy concern, terrorism, with high rewards and limited damage. However, these calculations of risk will change as the consequences, or stakes, increase dramatically.

In the chapters that follow, the authors assess how other particular aspects of the future operating environment are likely to have significant implications for SOF.

VOLUME ROADMAP

For the sake of grouping the implications of future conventional war for SOF into logical categories, the authors created several umbrella terms. These

INTRODUCTION

form the basis for this volume's chapters. The first umbrella term is *theatre break-in*, and is examined in chapter 1. The concept of breaking into a theatre is well-established in the doctrine of many advanced armed forces, including the United States, the NATO member states, Russia, and China, even if it is labelled differently. It acknowledges a core principle of conventional conflict: overcoming prepared and established defensive preparations and systems, on a national or regional scale or "theatre" or "campaign planning" level, using a variety of coordinated offensive means including firepower and movement for the purpose of seizing or threatening key objectives through manoeuvre, attrition, or both.⁴² The United States labels such actions as "joint forcible entry operations," for which there is established doctrine, in acknowledgement of the geographic position of the United States and the location of its forces and bases.⁴³ Other nations use different terms. British forces, for example, use "joint theatre entry" in a "hostile environment."⁴⁴ Generally speaking, in the development of operational plans, using the notional six-phase Western planning construct, theatre break-in equates to the overlapping activities that occur during Phases II (Seize the Initiative) and III (Dominate) illustrated below:

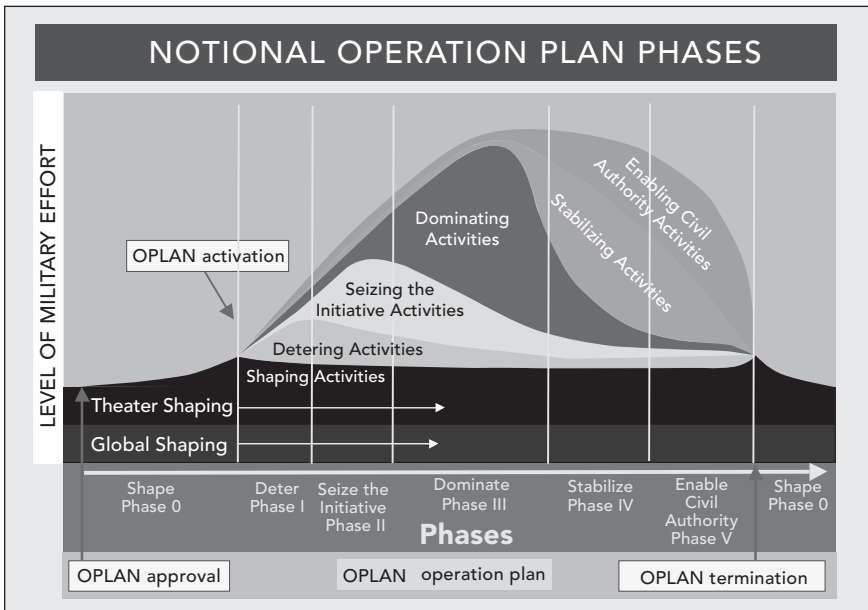


FIGURE 1: Planning Phases Versus Level of Effort⁴⁵

INTRODUCTION

In Russian military thinking, theatre break-in occurs somewhere between periods 3 (Initial conflicting actions), 4 (Crisis), and 5 (Resolution), according to the writings of General Valeri Gerasimov:

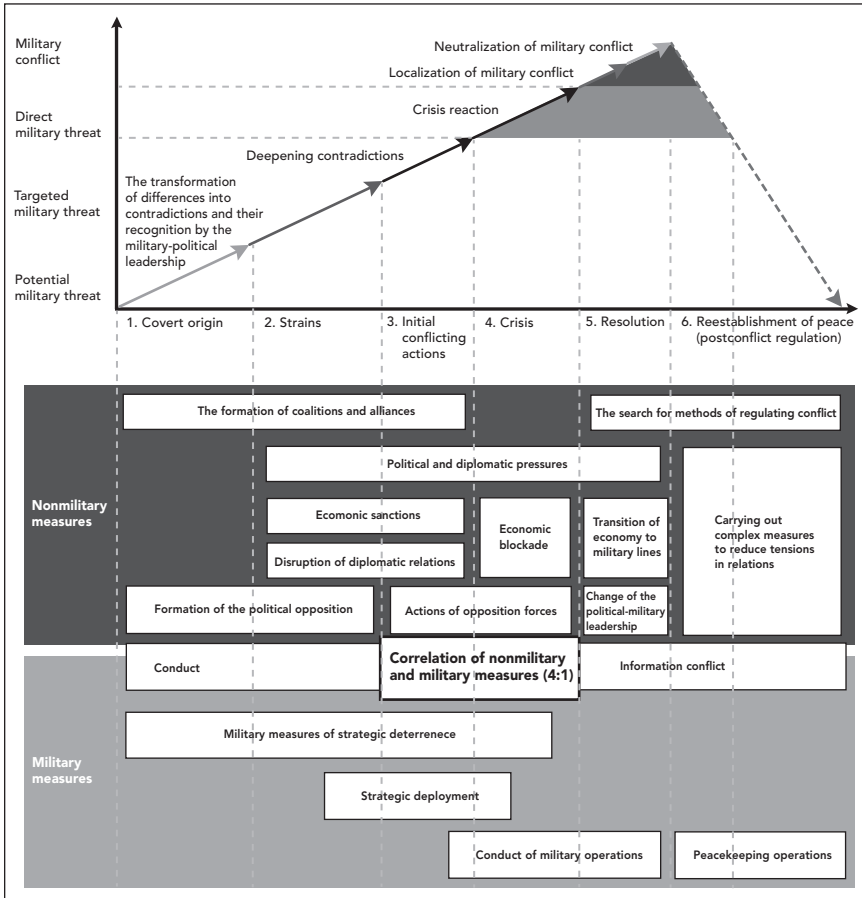


FIGURE 2: The Gerasimov Doctrine Illustrated⁴⁶

Several assumptions underpin our concept of theatre break-in for Western forces. First and foremost, it consists of military actions in response to initial aggressive, offensive actions by a peer or near-peer competitor, including through a *fait accompli* or illegitimate seizure of territory. Such actions could include a Russian invasion of the Baltic States or a Chinese invasion of Taiwan. Second, we assume that competitor has deployed defensive systems to deny others access to the ground, sea, air, space, and cyberspace to consolidate their gains and protect their own forces. In contemporary

INTRODUCTION

military parlance, the competitor has set up anti-access/area denial (A2AD) systems.⁴⁷ Third, NATO, coalition, or partner forces have resolved to respond to aggression using offensive military means. Fourth, NATO, coalition, and partner forces will take time to mobilize and deploy from bases outside of the region – a strategic reality for both the United States and Canada. Fifth, theatre break-in will be characterized by intense combat between forces across all domains, in a relatively short period of time, with significant losses on one or both sides. Sixth and last, SOF will act in a supporting and subordinate capacity to conventional force plans to assist them in accomplishing their objectives.

The next umbrella term for how conventional conflict might affect SOF is *crisis contingencies*. Examined in chapter 2, crisis contingencies consist of independent activities, whereby SOF deal with sudden, serious crises which they are well-suited to resolve and for which there is no pre-existing plan. The authors envision such contingencies occurring either in the main or peripheral states, regions, or theatres of operation. Crisis contingencies, as the modifier suggests, involve the projection of military power in response to sudden operational emergencies or requirements. Such SOF actions could consist of raids or other direct action missions against critical infrastructure or other valuable targets, securing friendly or enemy personnel or sensitive materials and recovering them, or conducting special reconnaissance to collect information, monitor, and/or direct strikes against unique targets. Crisis contingencies are characterized by their operational and strategic importance, short duration, high risk, and conduct in denied or limited access territory. Historical examples of crisis contingency SOF actions include the hastily planned and executed raid by American Rangers on Cabanatuan in 1945 to rescue endangered prisoners of war, the effort to destroy German heavy water production in Norway during the Second World War, and the “Scud Hunt” during Operation Desert Storm in 1991 – all of which are examined in chapter 2.

The third umbrella term is *emerging horizons*. Chapter 3 acknowledges that future conventional wars, fought with technologies that we see developing today, will likely have strong implications for how forces fight. This chapter assesses three areas in particular where developing technology may have especially profound impacts on SOF: social media, logistics, and human performance augmentation. The fourth umbrella term, examined in chapter 4,

INTRODUCTION

is *future technologies*. This chapter goes one step further and traces how trajectories in technological development are likely to affect information processing, weapons development, and new vehicle types.

The fifth and final umbrella term is *organizational considerations*. These are factors that may have bearing on SOF organization, training, and culture. There is every reason to believe that great power competition and the potential for conventional war will only increase demands for SOF. Non-state threat actors will not disappear, and extremist organizations will continue to threaten Western interests. How SOF contribute to combatting these persistent threats – directly or by enabling others – may necessitate difficult capacity allocation decisions and assessing what skill sets, if any, should be added, reinforced, or divested. At the same time, preparing for high-intensity conflict may entail contemplating new risk acceptance models and associated force management, preservation, and regeneration requirements.

Within each of the subsequent chapters, the authors explore how SOF might remain a highly valued instrument of national military power, in the context of future high-intensity conflict. Admittedly, this is an ambitious undertaking that cannot possibly render comprehensive solutions or give the last word on the matter. What this volume ultimately intends to do, then, is generate some informed and useful analysis for those contemplating what great power competition and the potential for conventional war means for the SOF community.

CHAPTER 1

THEATRE BREAK-IN

LIEUTENANT-COLONEL ANDREW L. BROWN, PhD

At the outset of a high-intensity conflict, how can Special Operations Forces (SOF) support the joint force's entry into a theatre of operations? The question merits consideration, given SOF's well-established role in supporting joint operations and increasing concern about great power conflict.¹ Answering it requires revisiting what SOF can or should do to fill gaps in joint capabilities. This chapter seeks to stimulate thought on the matter by proposing how SOF can provide options to the joint force commander. While continuous technological change and shifting political landscapes make it impossible here to render a comprehensive and enduring answer, it *is* possible to map out some broader concepts and contemplate in principle the contributions that SOF might bring to the joint force's theatre break-in.²

The rise and ambition of today's great power competitors make such an exercise prudent, if not necessary. Should worsening tensions with a great power initiate planning for a major offensive operation, commanders will seek SOF support to the break-in phase. And, experience shows, for SOF to render the best possible support, integrating capabilities into the joint plan will require thorough consideration. Indeed, failure to blend SOF effects into operational-level plans can result in wasted effort and undistinguished contributions. The Israeli armed forces learned this the hard way during the Second Lebanon War in 2006, when SOF operations purportedly gave little value to the overall campaign. Israeli SOF conducted up to thirty operations, including strikes against Hezbollah command and control targets, in an attempt to decapitate and demoralize the organization.³ But these operations proceeded without adequate targeting assessment, and, despite skillful tactical execution, had negligible effects on the greater Israeli effort. This experience cautions that thoroughly considered SOF input to joint planning will be crucial. Complicating this vital planning function is the anticipated nature of major operations (as described in the

introduction), particularly the speed, tempo, and lethality of high-intensity conflict. While the elevated risks associated with major operations are inescapable, SOF preservation exigencies will not change much. After all, SOF will remain a limited resource that must not be expended below critical capacity thresholds, respecting the axiom that SOF cannot be regenerated quickly because of the time required to recruit, train, and educate personnel.⁴ Nevertheless, SOF's unique capabilities have tremendous potential value to the joint force's break-in battle.

To begin, SOF can play an important role before the break-in by assisting in preparation of the operational environment. In fact, American special operations doctrine recognizes this as a core SOF activity.⁵ Preparation of the operational environment may include close target reconnaissance; reception, staging, onward movement, and integration (RSOMI) of forces; terminal guidance; and direct action, amongst other things.⁶ Given enough lead-time, and depending on the theatre in question, SOF may also be able to identify and map out resistance movements, and develop local allies to assist with theatre access for the main force and with follow-on operations. While none of these SOF roles are new, preparation of the operational environment where conflict looms with a great power competitor will bring novel challenges. At the very least, great power adversaries preparing for conflict will deploy their own resources to shape the environment, such as sophisticated technologies, covert or clandestine personnel, and ample supplies of cash to purchase influence where possible, which will complicate the challenges for friendly SOF. Russian activities in Ukraine in 2014 – including the employment of integrated proxies, information operations, and intelligence and special forces personnel – hint at the sorts of threats friendly SOF may struggle with.⁷ All of this points towards an environment in which friendly SOF engaged in operational preparation of the environment find themselves competing for influence while contending with an elevated threat of detection and severe consequences of being discovered. Mitigating these challenges, not the least through sophisticated physical and electronic concealment practices, will warrant close attention.

Advanced Force Operations (AFO) enable preparation of the operational environment and constitute another natural task for SOF.⁸ They support the senior leadership's decision-making prior to committing main body forces, often through reconnaissance and surveillance to render real-time

knowledge of the threat situation and local conditions at areas of concern. SOF can execute AFO with creative unmanned and manned information gathering methods. For instance, the emplacement of sensors for remote monitoring can allow for persistent technological surveillance of an area of interest, similar in concept to how Israeli SOF (*Sayeret Matkal*) planted sensors deep in enemy territory in the Sinai in the 1960s.⁹ Alternatively, SOF can be the sensors, providing the best-possible quality of information with close human overwatch of areas of interest. Prior to high-intensity operations, the capacity for mitigating risks to the main force, potentially through identifying targeting opportunities, may warrant the deployment of SOF elements. Teams capable of monitoring for, and calling fires on, high value targets such as missile systems, rocket batteries, and headquarters could prove invaluable to the joint break-in. AFO can also mitigate risks to the main body through other kinetic activities, such as direct action missions to disrupt the adversary's ability to respond to inbound threats.¹⁰

SOF may also play a vital role in removing enemy options just before the main force deploys. Coalition SOF activities during Operation Iraqi Freedom in 2003 highlight the potential. In the early days of invasion planning, anxiety arose at the political level about Iraqi Scud missiles in western Iraq that threatened to be a "strategic dislocator," as General Tommy Franks, the commander of United States Central Command, put it, if fired at neighbouring states or Israel. To deal with the threat, planners at first contemplated using an armoured cavalry regiment to secure Western Iraq.¹¹ But SOF advisors offered a more attractive option, one that could produce the desired effect with greater surprise: deploy SOF into Iraq before Saddam knew the war had started. After all, operations in Afghanistan had demonstrated the potential for SOF to move with remarkable speed and stealth. The concept became the plan, and eventually the Combined Joint Special Operations Task Force-West formed, comprised of American, British, and Australian elements.¹² On 19 March, when President George W. Bush ordered the invasion to commence, SOF teams bolted into Iraq before the main body.¹³ These forces, in heavily armed but agile vehicles, moved quickly and, supported with air power, struck opposing forces with disproportionate lethality.¹⁴ It worked. During Operation Iraqi Freedom, Saddam's forces fired no Scuds.

SOF may also assist in disrupting adversary systems that impede friendly forces from entering an area or operating there – frequently referred to as

anti-access/area denial (A2AD) systems. These pose a major potential obstacle to the joint force's break-in and lodgement.¹⁵ At the outset of a high-intensity conflict, joint forces preparing to force their way into a theatre of operations may have to expose themselves to elevated risk and casualties. Some of the most threatening A2AD capabilities comprise powerful combinations of long-reaching missiles. For instance, Russian standoff weapons designed to disrupt theatre access by air, land, and sea include an array of short-range ballistic, surface-to-air, land-attack cruise, and surface-to-surface anti-ship cruise missile systems.¹⁶ Aside from missiles, A2AD measures can also include things like coastal and shallow-water smart mines, cyber capabilities, and so on. None of these are limited to guarding an adversary's homeland and may be deployed to expeditionary theatres and their adjacent areas. Russia, for example, has deployed missiles to Syria and their reach extends over the Eastern Mediterranean.¹⁷ In any event, A2AD systems pose serious challenges to conventional forces at sea, in the air, and on the ground. SOF, however, are insensitive to many A2AD platforms – or at least can be, given that these are designed largely to detect and attack large physical objects. If SOF can enter a theatre discretely, they may be capable of helping disrupt A2AD systems.

Generally speaking, interfering with A2AD systems entails multiple active countermeasures. These can include mitigating missile fire by deploying decoy targets, radiating electronic jamming signals, and attacking the missiles themselves. Forces can also achieve disruption by targeting critical components of an A2AD system, for instance by attacking firing units, target acquisition and engagement radars, support vehicles, and personnel.¹⁸ A2AD systems can also be suppressed by saturating target acquisition and engagement systems with potential targets, as when they face swarm attacks.¹⁹ Such countermeasures fundamentally seek to break or disrupt any link in a system's kill chain, that is, its ability to find a target, track it, and engage it. Attacking just one of part of the chain can be enough to render an entire weapon system ineffective.²⁰ Plausibly, SOF can attack such key parts through kinetic or electronic means.

To be sure, air forces play an obvious and major role in the joint counter-A2AD plan, although SOF and other forces may have much to contribute as well.²¹ If viable staging areas exist close to the theatre of operations, SOF may be within striking range. For instance, as the authors of a 2019

assessment of Russia's A2AD capabilities argue, to assail Russian systems in Kaliningrad, SOF could conceivably attack from Poland or Lithuania, as could army rocket artillery units. Thus, SOF can form part of a joint force's array of counter-A2AD capabilities. As the aforementioned authors put it, "in a pre-planned operation it is possible to orchestrate a multitude of assets – surveillance, jammers, decoys, long-range missiles, artillery, special forces, stealth assets, and so on – to achieve good effects with acceptable levels of risk."²² Others agree with the concept. One authority on the Chinese People's Liberation Army (PLA) Rocket Force, which has undergone recent expansion and modernization, proposes the feasibility of using SOF in conjunction with other forces to neutralize the serious Chinese missile threat.²³

These proposals for a SOF role in countering A2AD systems warrant closer consideration. Potentially, SOF can assist in suppressing A2AD networks by fielding sensors to locate systems, disrupting them with electronic means, or destroying them by vectoring fires. Prior to, or in the early stages of, a break-in effort – before hostile missile batteries light up their engagement radars, making them vulnerable to aerial attack – SOF may be able to assist in identifying battery locations. This would open possibilities for attacking them with long-range rocket artillery or guided ordnance released from aircraft far from the target.²⁴

Electronic warfare (EW) monitoring constitutes another potential SOF role in the early stages of a break-in effort. Activation of A2AD systems triggers intensified activity in the electromagnetic spectrum and therefore can be detected through EW monitoring.²⁵ Ground-based forces may prove well-suited for conducting such activity, provided they possess the appropriate technology. Ascertaining exactly what can be done, and how exactly to do it, may require thorough studies of the systems in question to determine where and how A2AD assets are vulnerable to SOF effects and active countermeasures.

Special reconnaissance (SR) represents another traditional SOF task that can potentially support the joint force's break-in.²⁶ Because SR fundamentally concerns the collection or verification of information of operational or strategic importance, through capabilities distinct from those in conventional forces, it could prove especially valuable prior to the commitment of joint forces to major operations.²⁷ Although the joint force will have various

information gathering capabilities that do not require placing human collectors at risk, such as overhead imaging and signals intelligence, a requirement will probably exist for SR to complement or even stand in for other platforms. After all, weather can frequently obscure overhead imaging, especially in temperate climates. Terrain features, such as wooded areas and man-made structures, can block overhead observation too. Such problems frustrated Western forces during the North Atlantic Treaty Organization (NATO) bombing campaign against the Federal Republic of Yugoslavia (FRY) in 1999, when prolonged poor weather hindered operations and forested, variegated terrain impeded overhead collection.²⁸ Furthermore, in a conflict with a well-resourced adversary, the joint force may not have sufficient control of the airspace to guarantee collection by overhead intelligence, surveillance, and reconnaissance (ISR) platforms.

What is more, SOF observation of a target renders particular value because humans are less likely to be fooled by decoys and ruses.²⁹ Potential adversaries certainly recognize the effectiveness of such tricks. During NATO's bombing campaign against the FRY, for example, Serbian forces famously employed clever camouflage, concealment, and deception methods to diminish the effectiveness of high-level bombing. Shrewd passive air defence methods included dispersing troops and equipment and hiding it all from overhead observation.³⁰ When Canadian armoured reconnaissance forces entered Kosovo after the bombing stopped, they saw that NATO had overestimated the damage done to Serbian armoured units.³¹ The Canadians saw very few destroyed tanks. They did, however, see extremely effective camouflage, such as M-80 tanks concealed under mounds of garbage, and decoys such as mock tanks built of plywood. These efforts proved very effective at blunting the effectiveness of NATO aerial attacks.³² One important lesson coming out of the war, then, was the requirement for better discernment between decoys and genuine targets.³³ SOF could potentially fill an important role here. As Alastair Finlan, professor War of Studies at the Swedish Defence University, argues, automated information gathering systems cannot replicate a highly-trained SOF operator's direct observation and information-processing procedures. "Unquestionably," he asserts, SR "is the gold standard of battlefield intelligence."³⁴ It also renders a quality of surveillance that technical platforms often cannot match.

British SR achievements during the Falkland Islands war exemplify the value SOF can provide to joint forces before they enter a theatre. To support campaign planning, G Squadron of the Special Air Service (SAS) received orders to conduct surveillance of likely enemy areas.³⁵ Patrols thus deployed to East Falkland long before the invasion force and acted as dependable, all-weather, persistent sensors. They inserted by helicopter at night, miles from their objectives, followed by careful approaches and painstaking efforts to avoid detection. For the entire weeks-long surveillance effort, patrols had no resupply or medical evacuation except for the most exceptional situations. They provided both negative information (such as areas clear of an enemy presence) and positive information (locations of enemy troop concentrations). These SAS patrols, operating deep in enemy held territory, provided invaluable information and remained effective for weeks on end, despite dreadful weather of bitter wind, rain, and sleet.³⁶ Meanwhile, the Special Boat Service (SBS) carried out reconnaissance of potential landing sites for the invasion force.³⁷ Campaign planners required high-quality assessments of locations that had the topography suitable for landing thousands of troops. They needed to know where landing craft could approach the beach and which landing zones included defensible terrain. Obtaining this critical information was particularly sensitive work that required highly skilled operators, as detection would have drawn Argentine attention and exposed the landings to serious risk.

Admittedly, while demonstrating the exceptional value SR can bring to joint planners preparing the break-in, the Falkland Islands case has limited value when considering future high-intensity conflict. Providing similarly useful SR support in a military contest with a great power will entail challenges that did not exist in the Falklands. The operating area may be much more densely inhabited than thinly populated East Falkland. And the *interconnected* nature of a great power's armed forces, and the *informatized* environment that makes concealing forces extremely difficult, as described in this volume's introduction, could pose significant challenges for SR efforts.

A great power facing high-intensity conflict with U.S.-led forces will not waver in deploying throughout its territory every sensor at its disposal. Aerial ISR, fixed ground-based observation instruments, and monitoring of the electro-magnetic spectrum will make for a thick surveillance blanket that

covers even seemingly remote terrain. Tightly-networked internal security personnel, probably in plain clothes, maintaining close scrutiny will add density to the array of technical sensors. Indeed, it may be all but impossible to conceal a physical presence. All this will have serious implications for the potential for compromise and, by extension, for risk management and acceptance. That said, risk mitigation may benefit from innovative procedures for conducting SR in a densely populated region under an internal security microscope.

SOF's potential for excelling at operational deception may also prove invaluable to the joint force's break-in. By executing feints (distracting an enemy by seeking contact, but without decisive engagement) or demonstrations (shows of force intended to deceive an adversary), SOF may prod an adversary to divert or dissipate combat power, to the benefit of the main force's theatre entry.³⁸ Operational deception can induce an adversary to deploy forces to an area they have been deceived into believing faces a serious threat. It can make the main friendly effort appear as a secondary or even diversionary effort. And it can persuade an adversary to withhold combat power by creating uncertainty about where major blows may land. It thus assists the main body to enter a theatre against reduced opposition and, during the initial period of vulnerability, buys time for building up combat power.

Again, SOF achievements in the Falkland Islands provide a useful conceptual model for what is possible. Before the amphibious landings at San Carlos, staff had ascertained that the landing force required a full day to dig in and prepare defences, free from enemy air and ground interference, so that it could withstand anticipated counter attacks.³⁹ Thus, planners designed a sophisticated deception plan to keep Argentine forces away from the beach for as long as possible. This included convincing the Argentines that British forces would land on the south shore of East Falkland at a location, far from San Carlos, where the topography suited amphibious landing. The deception effort included radio transmissions, air activity, nighttime naval shelling of land targets – plus an SBS patrol that went ashore to spread disinformation amongst the locals. These activities gradually intensified right up to the night of the real landings. Furthermore, when British forces pushed ashore at San Carlos, G Squadron of the SAS conducted a diversion at Darwin/Goose Green.⁴⁰ The Argentine garrison there posed a serious risk to the landings, especially if it attacked the landing site before British forces reinforced

the beachhead. G Squadron's task was to prevent the force from leaving its garrison. To achieve this, the squadron conducted a feint attack, designed to pin down the Argentines by convincing them that they were about to face a major assault. The ruse included pouring small arms fire on an enemy outpost and making a big show of things to make it seem that a large force was pressing in.⁴¹ It worked. The Argentines believed that a major landing had occurred somewhere and that Darwin/Goose Green was under attack. The SAS effort contributed to a larger successful plan that encouraged the enemy to remain in place instead of rushing forces towards the vulnerable beachhead at San Carlos.

Creating a similar effect in a future conflict with a highly lethal, *interconnected* enemy would surely prove difficult, but probably remains feasible. Above all, operating in terrain controlled by a great power adversary may require creativity and high risk tolerances. Still, SOF may be ideal for turning the adversary's dense and hypersensitive surveillance network against them. Feeding misinformation to the adversary's sensors could induce the desired reaction – a distraction, the husbanding of forces, or the deployment of forces away from the break-in area.

The methods used to achieve such effects may or may not look anything like G Squadron's dramatic kinetic demonstration outside Darwin/Goose Green. Conceptually, however, a kinetic demonstration of some type may be plausible, perhaps by proxy forces organized in advance of major operations or by SOF operators who aggregate suddenly to conduct the demonstration and then, just as quickly, disaggregate and disappear. What is more, experience demonstrates that forces can achieve deception very effectively through non-kinetic means. Consider, as a conceptual model, the Allies' successful deception in the Second World War to convince the Germans that the invasion of Northwest Europe would occur in the Pas-de-Calais, not Normandy.

Allied planners executed a clever deception plan, called Operation Bodyguard, to mask the location and timing of the landings in France.⁴² By early 1944, the buildup of forces in southern England signaled clearly to the Germans that an invasion was coming, and the Allies knew that Hitler and his high command would make plans to push it back into the sea. The deception plan, then, aimed to obscure the invasion's time and place. To achieve

CHAPTER 1

this, the Allies schemed to convince the Germans that amphibious forces would cross the channel between Dover and the Pas-de-Calais, the shortest route across the water. Operation Bodyguard achieved this aim largely through non-kinetic means, in part by feeding the German intelligence system misinformation about the buildup of the First U.S. Army Group (FUSAG) in southeast England.

To the Germans, FUSAG seemed a formidable force, one million strong, preparing for a tremendous thrust toward the Pas-de-Calais. But it was a complete fiction. Yet, thanks to how the Allies fed the enemy's intelligence system, the Germans thought it was very real. To deceive German overhead collection, the Allies fabricated fake camps across southeast England, complete with phony headquarters, tanks made of rubber, and landing craft made of wood and canvas. Misinformation fed through double agents divulged FUSAG's organization and warned of American units crossing the Atlantic for the buildup. FUSAG radio transmissions added to the hoax, as did real messages that referred to the massive force. By May 1944, the Germans assessed that the Allies had 79 divisions in England, when there were just 47. The Allies even managed to convince the Germans that a diversionary attack would occur at Normandy, to explain German intelligence about the buildup of the real invasion force, so that they would not rush the actual landings with overwhelming forces. It worked. When the Allies drove ashore at Normandy, the Germans kept powerful forces at the Pas-de-Calais where an anxious Hitler expected the main blow to land. In fact, the deception worked so well that he did not send formations from the Pas-de-Calais to Normandy until late July, seven weeks after the initial landings, which bought the Allies much-needed time to consolidate.

In a future conflict with a great power competitor, SOF could be a potent tool in achieving, or helping to achieve, a similar deception. While the techniques will require novel approaches tailored to the situation, the aim would fundamentally be the same as in 1944: feed the adversary disinformation to encourage decisions that favour the break-in operation by minimizing potential opposition. And, like in 1944, sustaining the deception effort after the initial theatre break-in, for as long as possible, could buy time for forces to secure the entry.

Direct action, yet another SOF core activity, may also prove invaluable to the joint force's break-in. A series of sudden raids and ambushes, for instance, could seize vital ground, confuse the adversary's command and control, disrupt lines of communications, create confusion, and paralyze ability to react. SOF demonstrated both the feasibility and value of such activities during the opening moves of the 2003 invasion of Iraq. Just before the main assault began, two SAS squadrons and a squadron of the Australian Special Air Service Regiment (SASR) pushed into western Iraq and sped towards two airbases, H-2 and H-3.⁴³ At H-2, operators directed air strikes that defeated local Iraqi forces, then drove onto and seized the airfield unopposed. The British and Australian soldiers soon handed the site over to American and British follow-on forces.

At H-3, which was defended by an Iraqi battalion with plenty of anti-aircraft weaponry, British, Australian, and American SOF teams used laser designators to bring down precision airstrikes for twenty-four hours.⁴⁴ Those Iraqis who survived the onslaught abandoned the site, allowing SOF to seize it as well. SAS, SASR, and American Delta teams also cut escape routes along major highways to interdict fleeing high value targets of Saddam Hussein's regime.⁴⁵ And according to one account, Delta operators even infiltrated Bagdad to intercept and cut Iraqi communications and search for regime officials.⁴⁶ These examples demonstrate, at least at the conceptual level, that direct action missions can lend valuable support to the joint force's break-in.

Indeed, direct action may be a powerful tool for helping frustrate an adversary's decision-making. One forward-looking defence policy expert argues that the Chinese People's Liberation Army (PLA) uses exceedingly centralized command arrangements and therefore may struggle to deal with a prolonged, complex, and high tempo crisis – a problem that western forces could exacerbate by causing numerous concurrent emergencies through physical, electronic, and cyber attacks.⁴⁷ Surely, SOF could assist in such an effort. That said, deploying multiple SOF teams to conduct direct action in hostile territory could stress risk thresholds. The lethality of large-scale conflict against a great power adversary – one with far greater ability to detect and pounce on threats than Iraq had in 2003 – suggests that the risks to both missions and forces will be higher than anything experienced to date. Mitigating those risks may pose a significant planning challenge.

CHAPTER 1

Experience shows that calling down fires is another SOF activity that can assist the joint campaign. The capacity to penetrate sensitive areas potentially allows SOF to attack throughout an adversary's depth by directing strikes from operational or strategic level assets. Russian SOF in Syria suggested as much by pinpointing targets for cruise missile attacks.⁴⁸ During the Falkland Islands war, British operators demonstrated how SOF can shape an adversary with fires while joint forces manoeuvre into position. SAS and SBS patrols penetrated deep into Argentine-controlled territory and established observation around the capital of Stanley.⁴⁹ As the main ground force approached the town, SOF teams began targeting Argentine forces by calling down joint fires, including air, artillery, and naval gunfire strikes. The Argentines suffered both physical and psychological damage, just as British joint forces prepared for the final series of ground battles.

Similarly, SOF can also assist the joint effort by providing real-time post-strike assessments based on direct observation. In the opening days of the 2003 invasion of Iraq, American joint forces launched sixty-four Tomahawk Land Attack Missiles at a terrorist training camp along the eastern border with Iran. American Special Forces (SF) observed the strikes and provided battle damage assessments (BDA) (in preparation for an SF attack on the camp, in conjunction with air and Kurdish Peshmerga forces).⁵⁰ In a conflict with a great power competitor, such direct observation of strikes may prove vital when contested airspace or obscuring meteorological conditions render aerial or remote BDA impractical. This was precisely the case during NATO's air campaign against the FRY, when staff struggled to produce quality BDA in real-time to support tactical decision-making.⁵¹

In fact, NATO's experience in Kosovo suggests yet another way that SOF may in future play a critical role in directing aerial fires: addressing collateral damage concerns. The potential for killing non-combatants caused a great deal of concern amongst NATO political leaders, which Serbian forces exacerbated by using human shields. As it was, NATO aircraft were already flying at relatively high altitudes (over 15,000 feet) to avoid Serbian air defences, which made viewing targets difficult. And, inclement weather often obscured visibility, adding to the burden of avoiding unnecessary casualties. As a result, stringent efforts to avoid collateral damage probably degraded the effectiveness of bombing.⁵² In the future, SOF operators might reduce such problems with direct, all-weather observation of potential

targets. One of the key lessons of the NATO air campaign in Kosovo suggests as much: the factors that made targeting so difficult – poor weather, flying at higher altitudes to avoid air defence, and the adversary’s use of decoys and ability to hide in closed terrain – probably typify future air campaigns more than conflicts like the Gulf War, where targets sat exposed and vulnerable in the open desert.⁵³

While it is clear, then, that SOF have the potential to provide valuable support to the joint force’s break-in, it is equally clear that operations against a great power adversary will bring significant challenges. Contested airspace stands out as a particularly difficult problem. Potential great power adversaries possess sophisticated, layered air defence systems that may complicate the joint force effort to achieve air superiority. Consequently, SOF may not possess the aerial freedom of manoeuvre that they have enjoyed for decades. Projecting force by rotary wing aircraft may necessitate revisiting mitigation measures or accepting higher risk thresholds. It may even prove impossible if risks are too high. The same applies to sustaining or recovering deployed elements. Aerial medical evacuation may not be feasible either, heaping on more risk and mitigation requirements for commanders to consider.

Concealing forces in contested or enemy-held areas may also prove especially challenging. Peer or near-peer adversaries will soak battlespaces with state-of-the-art ISR coverage. Because completely evading such collection may prove difficult or impossible, SOF may consider adopting physical and electronic profiles that mimic local patterns of life and do not appear out of the norm to ISR sensors. In other words, seek not to cloak, but to blend in. What is more, quite aside from the hostile ISR problem, the adversary’s security services may prove especially difficult to evade. After all, potential great power challengers have long maintained very capable internal security agencies to crush any sign of political or popular opposition. Iran provides a useful illustrative example.

The regime in Tehran maintains a dense network of internal security forces. Since 1979, they have carefully guarded the revolution from internal threats. To this day, the country’s leadership believes that America and its allies constitute an active threat to the Iranian regime and the nation’s interests.⁵⁴ Consequently, Iran maintains several overlapping domestic security agencies that detect and subdue anti-government activities.⁵⁵ The Islamic

Revolutionary Guards Corps and its *Basij* militia, multiple law enforcement agencies, the Ministry of Interior, and the Ministry of Intelligence and Security form a legion of agencies that maintain tight internal security, watching for and suppressing anti-regime groups or actions. In fact, the regime has used violence to suppress outbursts of unrest that manifest from time to time. Iran has a long record of abusing human rights, with brutal and sometimes lethal treatment of political dissenters.⁵⁶ In short, Iranian authorities take seriously the business of scrutinizing the population and cracking down hard and fast as necessary. They are very good at it and are no doubt sensitive to detecting activity out of the ordinary. The Iranian case shows that, for SOF, entering spaces where authorities keep a close watch on the population and evading security services' attention will require a great deal of skill, intensive planning based on a thorough understanding of the threat, and risk management.

The potential for hostile actors to detect SOF elements suggests that survivability constitutes another potential challenge. After all, as this volume's theme of the lethality of future high-intensity operations emphasizes, great power adversaries possess means to strike threats rapidly with devastating firepower. For instance, in recent years, Russian artillery upgrades have produced a formidable capability that includes heavy long-range artillery – and Russian forces have already demonstrated its potential. In 2014, artillery in the Donbas region of southeast Ukraine caused a surprising eighty percent of casualties, suggesting that, in any future contest, Russian forces will wield artillery as a sledgehammer to pound threats immediately upon detection.⁵⁷ Russian artillery in Ukraine demonstrated adroit responsiveness, with fires cued by a system of target-spotting unmanned aerial vehicle (UAVs) and forward observers.

Today, every Russian artillery brigade now includes a UAV company that finds targets, adjusts fire, and performs BDA.⁵⁸ And Russia is hardly unique in this regard. According to *Janes*, the Chinese PLA probably prefers using UAVs to facilitate targeting with artillery and rocket forces.⁵⁹ Chinese special forces also now use small UAVs with greater frequency to identify and strike targets. Looking ahead, because adversaries will seek targets by dispatching UAVs, searching for electromagnetic signatures, or employing cyber techniques, mitigating the threat of hostile artillery may require camouflaging one's physical, electromagnetic, and cyber profiles.⁶⁰ Excellence in this

regard may prove essential for avoiding the severe consequences of detection, which could include devastating sledgehammer blows.

Finally, while this chapter has focused on potential SOF roles during the break-in, it should also acknowledge the value that SOF could bring if Western forces find themselves in an opposite scenario, countering an adversary's attempted break-in. After all, SOF may be well-placed to serve in an anti-access role, making it costly for a great power to attack a Western ally. Fundamentally, potential SOF tasks to support a joint force's defensive campaign mirror many of those for offensive campaigns, even if their higher purpose is to prevent the adversary from establishing or consolidating a bridgehead. For example, as part of pre-crisis contingency planning, preparation of the operating environment could prove invaluable, such as organizing local resistance, placing sensors, or preparing surveillance positions and ingress/egress plans. Once an invasion begins, SOF could aid in short-circuiting the adversary's orientation and decision-making processes by conducting multiple direct actions in rapid succession. Disrupting lines of communication and executing terminal guidance on high-value targets of opportunity throughout the adversary's depth are but two examples. Gathering intelligence for the joint force through surveillance could prove indispensable. While the adversary would possess the initiative at the operational level, SOF and the joint force would enjoy the advantages of fighting on the defence, such as intimate knowledge of the terrain, infrastructure, and population. Planning to exploit such benefits well in advance will be crucial. Similarly, if enough warning occurs before the adversary commences operations, SOF may have the lead-time to establish vital safe areas, lines of communication, and support arrangements.

Several conclusions arise from this chapter's contemplation of potential SOF roles during the initial phase of major operations. Above all, a requirement exists to consider, on a continuous basis, the question posed at the beginning: in a high-intensity conflict, how can SOF support the joint force effort to break-in to a theatre of operations? Constant shifts in the strategic landscape, especially in the political and technological domains, necessitate revisiting the question frequently. For contingency and targeting planning, databases and understanding of potential adversaries' weapons, command and control, and sustainment systems require continuous updating. Similarly, templates of adversary A2AD schemes and vulnerabilities require

ongoing refinement as technology improves and new equipment proliferates. Internal security agencies merit close and ongoing study too, if SOF are to operate proximate to these very capable forces without being discovered. Remaining oriented to the problem is also essential for, amongst other things, buying time to develop, procure, and field special equipment and technologies. Planners probably cannot accomplish any of these things thoroughly at short notice.

Of course, planning for the break-in must be a joint effort. With individual services now paying closer attention to potential high-intensity conflict with peer or near-peer adversaries – with some forces having spent much of the post-9/11 era combatting terrorism and insurgency in relatively clear arid climates – refining and updating joint campaign designs will be necessary to fuse the services' latest capabilities. Assuredly, prevailing in high-intensity conflict will require execution of well-planned joint efforts that include the best-possible integration of SOF resources.

Inculcating enduring joint culture, however, takes effort and, in the face of strong service identities, may fall short. For example, concern arose recently that the American armed forces have experienced an erosion of joint capability, owing to, amongst other things, diluted joint education and shortened postings to joint billets.⁶¹ Such a trend would be troublesome when joint collaboration should be galvanizing and a requirement exists for acknowledgement in all quarters that interservice bickering and parochial attitudes must not undermine joint readiness.

Furthermore, joint planners, including SOF representatives, should possess a comprehensive appreciation of the interservice dependencies between SOF and the joint force. To this end, U.S. Special Operations Command's fifth SOF truth, that "most special operations require non-SOF support," surely portends the reality of high-intensity conflict. In short, delivering the best-possible SOF support to the break-in requires a genuine commitment to joint planning.⁶²

Lastly, contemplating *how* SOF should contribute to the joint force's break-in should include considering *how much*. After all, SOF is a low-density resource that cannot regenerate quickly. Yet, in a world in which militaries must prepare plans for high-intensity conflict, the demand for SOF will

CHAPTER 1

climb, for several reasons. For one thing, recent and current requirements for SOF – for counter-terrorism, capacity building, counter proliferation, and so on – will not abate and these mission sets will remain as important as ever. Furthermore, because the U.S. and its allies face more than one great power competitor, they could find themselves facing multiple serious threats. To state just one possibility, should western forces find themselves conducting major operations against a hostile power, another power could decide to exploit the situation while western forces have their hands full.

Finally, requirements will remain to preserve some SOF capacity for contingencies. All these competing demands require reconciliation before committing SOF resources to joint plans. Because demands may outstrip resources, precisely how much SOF to commit to the break-in battle, and how much to preserve for other requirements, will require strategic decisions and risk management.

Fundamentally, none of the roles discussed in this chapter are new. What *is* new is the requirement to adapt to highly capable adversaries and to the speed, tempo, and lethality of high-intensity operations. Failure to do so thoroughly risks undermining SOF's value in contests of the highest national importance.

CHAPTER 2

CRISIS CONTINGENCIES

COLONEL (RETIRED) PETER MCCABE, PhD
and LIEUTENANT COLONEL NICHOLAS J. KRAMER

As popularized in the 1968 movie, “The Devil’s Brigade,”¹ the use of Special Operations Forces (SOF) in a conventional war – specifically in a crisis contingency – is not a new idea. The movie depicts the true story of the creation of the First Special Service Force (FSSF)² in 1942 and its assault on a seemingly impenetrable defensive position that sat high atop a mountain surrounded by steep cliffs, blocking the route to Cassino, Italy. The FSSF was a joint Canadian-U.S. force of three small regiments and a service battalion. While the force fought in numerous battles in World War II, the movie focuses on the one operation that conventional forces were unable to conquer.

Between 3 and 9 December 1943, in the dead of winter, the FSSF wiped out the vital enemy defensive position called Monte la Difensa. Monte la Difensa was part of the Bernhardt Line defences on the Camino Hill mass located near the ancient town of Rocca d’Evandro, roughly ten miles (16 kilometres) southeast of Cassino. The German position dominated the Mignano Gap, which was key to the U.S. Fifth Army’s route to Cassino. Previously, conventional U.S. and British forces had suffered high casualties in futile attempts to take the important target.³ After five days of hard fighting, the FSSF cleared the mountain top and paved the way for the U.S. Fifth Army to restart its stalled offensive to Cassino. This example illustrates one possible crisis contingency operation for SOF in a conventional war – an assault of a hard target.

The purpose of this chapter is to describe how SOF will likely be utilized to address crisis contingencies in a future conventional war. There is no definition for a crisis contingency operation in either U.S. or Canadian SOF doctrine, but there are numerous examples of crises to which SOF have responded in conventional war that are worthy of study. Lacking a doctrinal definition, the authors define *crisis contingency* as an operation conducted in

response to a rapidly developing situation of strategic, or national, importance for which there is no pre-existing plan. Crisis contingency operations can take many forms – from liberations to assaults to search and destroy missions – but the common denominator to all these operations is the immediacy of the situation, the lack of an existing plan, and the level of import. What follows in the remainder of the introduction is a discussion of how the authors arrived at this definition as well as the limitations of SOF in these kinds of operations.

According to U.S. Joint Publication (JP) 3-0, *Joint Operations*, a crisis is defined as an incident or situation involving a threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national objectives.⁴ JP 3-0 posits that responses can range from an independent, small-scale, non-combat operation, such as support of civil authorities, up to a supporting component of extended major non-combat and/or combat operations.⁵ Additionally, JP 3-0 describes a crisis response or contingency operation as occurring separately or as part of a campaign or major operation.⁶ For the purposes of this chapter, crisis contingencies will assume to occur during major combat operations. According to U.S. (JP) 5-0, *Joint Planning*, a contingency is defined as a situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect United States interests.⁷ Therefore, while *crisis contingency* is not a doctrinal term, it describes a situation where a military response is required to address a problem where a pre-existing plan does not exist.

United States Special Operations Command's (USSOCOM's) and Canadian Special Operations Forces Command's (CANSOFCOM's) role in crisis contingencies is not clearly delineated in guiding documents. For example, JP 3-05 touches on special operations in a crisis, but focuses on what SOF can do before a crisis emerges and less on what role SOF has during a crisis. The following JP 3-05 excerpt illustrates the point:

[Special Operations] SO are most effective during crisis when SOF has had enough time (months to years) to conduct pre-crisis activities, build relationships, and build [host nation/partner nation] HN/

CHAPTER 2

PN SOF capacity as part of shaping operations (Phase 0) of theater campaign and contingency plans. Longer term preparations for SO provide options for decision makers in times of crisis that would otherwise not be available. Also, pre-crisis SO preparations may provide situational awareness that permits identification of a potential crisis prior to requiring a US military response, thus allowing a whole-of-government solution be applied to de-escalate the situation by dissuading, deterring, or disrupting the parties involved or through mediation.⁸

Therefore, the exact role of SOF in crisis contingencies is not outlined in guiding documents. According to JP 3-05, if SOF does not have a presence pre-crisis, their utility could be less optimal. If SOF are employed in such a scenario, they are usually utilized independently or with conventional (general purpose) forces. This will be evident in the historical examples identified in the next section.

There are limitations to employing SOF in a crisis contingency operation. For example, joint forces possess significant raiding capabilities. So why use SOF? Frequently, as in the case earlier when discussing Monte la Difensa, SOF are called to accomplish what conventional forces might be unable to do because of a perception that SOF can overcome the hardest of missions due to specialized capability and high *esprit de corps*. However, SOF may not be the suitable tool to apply against the operational problem. For instance, SOF operate in small teams and do not retain the same weight of firepower or protection that conventional combat arms units possess. On 30 January 1944, for example, the 1st and 3rd Ranger Battalions were decimated when they were ordered to assault the German-held town of Cisterna in Italy.⁹

Sometimes SOF are called because senior leaders are left with few options to nebulous problems and SOF appear to be the most versatile and lowest risk solution. During the past twenty years and two wars in Iraq and Afghanistan, the U.S. shifted from large-scale counter-insurgency (COIN) missions to a lighter-footprint counter-terrorism (CT) strategy. That approach placed an extremely high premium on small, skilled units that could conduct raids or support friendly forces fighting the Islamic State or al-Qaeda. As SOF delivered results, policymakers leaned more heavily on them; the budget of USSOCOM roughly tripled between 2001 and 2017 and its personnel

increased from 43,000 to 70,000.¹⁰ But with this increase in resources came the expectation that SOF would answer the call no matter the situation, potentially with insufficient thought as to whether they were the right fit to meet a given crisis. In a future crisis, it is likely that policymakers will turn to SOF regardless of their suitability for the mission.

Incidents involving SOF employment because of their skill with host-nation groups are likely to be one of the more apt applications of SOF in future crises. Looking toward the future operating environment, SOF will need to be prepared to enter a denied area and operate for an extended period working with host-nation groups against a belligerent or occupying power. General (retired) Charles T. Cleveland, who commanded the U.S. Army Special Operations Command from 2012-2015, identified tension between direct action and unconventional warfare: “this idea between the indigenous centric war fighting and the hyper-conventional raid, bringing those two halves together at the campaign level to say this is what a SOF campaign looks like, and then educating leaders as they move up the chain to be able to command those campaigns, which are very complex.”¹¹ It is SOF’s unique and specialized skill in unconventional warfare that is likely to be the prized and applicable asset in a future crisis contingency.

The remainder of the chapter proceeds in three sections. The next section discusses three historical examples to illustrate how SOF have been used for this purpose in the past. The subsequent section considers how SOF could be utilized in crisis contingencies in a future operating environment. And, finally, the chapter concludes with the implications of the four themes of future conventional war for SOF in future crisis contingencies (as articulated in this volume’s introduction) and suggestions for USSOCOM and CANSOFCOM to consider for what can be done now before employing SOF in crisis contingency operations during a future conventional war.

HISTORICAL VIGNETTES OF CRISIS CONTINGENCY OPERATIONS

The authors have chosen three vignettes of crisis contingency operations, varying their type – liberation, interdiction, and search and destroy – and varying the reliance on partners – none, partially reliant, and wholly reliant. While not necessary for success, a local partner does increase its chances

in a crisis contingency operation. Two of the crisis contingency operations occurred during World War II while the third occurred during the 1991 Gulf War. The first vignette, the 6th Ranger raid on Cabanatuan, illustrates the added capability even partial employment of a local resistance force brings to the operation and the speed at which such a force allows SOF to act in a crisis. The second vignette is the effort to destroy the heavy water plant at Vemork, Norway, which exemplifies how crisis contingencies can be nearly independently executed by a capable resistance force to great success. The third and final vignette, the Great Scud Hunt during the 1991 Gulf War, demonstrates the difficulty of executing a crisis contingency operation without a local partner's information and the perils of relying solely on the most sophisticated surveillance technology of the day.

THE U.S. ARMY RANGER RAID ON CABANATUAN, 30 JANUARY 1945

The rescue of 512 prisoners of war (POW) from the Japanese camp at Cabanatuan in the Philippines in January 1945, is an important example of a crisis contingency operation. Several other rescue operations could be used to illustrate a crisis contingency operation during wartime – the German rescue of Benito Mussolini and the Son Tay Raid come to mind – but the U.S. Army 6th Ranger raid has significant implications for SOF in the future operating environment. First, the raid demonstrates the importance of intelligence networks and local partners for acting quickly. Furthermore, the raid illustrates the speed at which decisions and actions need to take place to be successful. Additionally, it exemplifies the necessity of conventional forces' support to special operations. And, finally, while this operation did not require the integration of new technology, it did require adaptation and flexibility throughout execution.¹²

The raid on Cabanatuan was conducted during the retreat of Japanese forces during the U.S. Sixth Army's advance on Luzon island, in the Philippines, and its purpose was to rescue the POWs who had endured the Bataan death march.¹³ U.S. Sixth Army leadership credibly believed that the withdrawing Japanese forces would execute the remaining POWs rather than risk withdrawing with them.¹⁴ Of the roughly 6,500 Americans who had surrendered at Bataan, survived the Bataan death march, and arrived at Camp Pangatian, only 512 remained in 1945 after enduring brutal conditions of captivity.¹⁵

CHAPTER 2

Saving these survivors was a matter of national honour and military morale.¹⁶ Lieutenant General Walter Krueger, commander of U.S. Sixth Army and leading the effort to retake the Philippines, deemed the mission critical and assigned it to the 6th Ranger Battalion, a unit formed previously out of a field artillery unit with just such an operation in mind.¹⁷

In preparation for the raid, the 6th Ranger Battalion was dependent on intelligence from local networks and Captain Juan Pajota's guerrillas for detailed planning. Pajota had trained in the 45th Infantry Philippine Scouts prior to the fall of Bataan. After the Japanese occupation of the Philippines, then-lieutenant Pajota and another member of the scouts formed, in the Luzon Central Plains, a guerilla unit made up of Filipino military to harass the Japanese. Pajota was promoted to Captain and led the eighty-person guerrilla group that would be vital for the success of the Rangers' raid.¹⁸

The timeline to execute the operation was short – the commanding officer, Lieutenant Colonel Henry Mucci, and the 6th Rangers received the mission on 27 January and began moving to the objective the following morning.¹⁹ The force conducted no rehearsals before departing and completed the plan at the objective rally point during infiltration to the POW camp.²⁰ Lieutenant William Edgar Nellist, a scout officer tasked to reconnoitre the camp but unable to because of the timeline and unpromising infiltration routes, and a Filipino guerrilla questioned locals near the objective and obtained detailed information on the POW camp's pattern of life and layout from people who had been there.²¹ The rescue force was even able to tailor loads – food and water, weapons and ammunition – based on the intelligence provided by Captain Pajota's local networks.²²

Captain Pajota's Filipino networks and guerrillas were crucial during the Rangers' infiltration. The Filipinos acted as guides for the Rangers, ensuring they stayed on safe routes to avoid compromise and made stops in friendly villages.²³ The Filipino guerillas and networks secured the objective rally point for the Rangers as they made final preparations for the rescue, and provided food and water along the route and at the objective rally point.²⁴ All the while, the local informants monitored the objective for changes in enemy force numbers and patterns of life.²⁵ Pajota and his guerrillas' timely information led Mucci to delay the operation by twenty-four hours to allow

CHAPTER 2

an enemy force resting in the camp and the surrounding area to leave, thus avoiding a larger force that could have spoiled the operation.²⁶

The 6th Battalion Rangers executed a textbook raid, isolating the objective from reinforcing enemy forces, suppressing the enemy on the objective with supporting fire while attacking with a separate assault force, and conducting a deliberate, planned withdrawal. The Rangers had precise intelligence from reconnaissance by the Alamo scouts, guerrillas, and informants about the layout of the camp, enemy force concentrations, and POW locations.²⁷ Because of that information, the Rangers were able to be precise with where and how they concentrated fire during the attack. Further, Pajota's forces acted as a blocking element, isolating the objective for the Rangers, destroying Japanese reinforcements, and covering the withdrawal of the Rangers and POWs.²⁸ Pajota's men killed an estimated three hundred Japanese attempting to reinforce the camp.²⁹

After securing the camp and the POWs, the Rangers were in the hands of the Filipino guerrillas to make their way back to friendly lines. The local networks kept the Rangers and POWs on safe routes to avoid retreating Japanese forces.³⁰ Despite the Rangers' knowledge of the poor health of the POWs and preparing as much as possible, the withdrawal still required local help to evacuate everyone.³¹ Locals supplied water and food along the way, and ox carts to speed the Rangers' movement back to friendly lines.³² Airplanes covered the withdrawing element's route and trucks moved to the link-up point to aid the evacuation efforts.³³ The 6th Ranger Battalion's raid on the camp at Cabanatuan resulted in the liberation of 512 POWs and considerable destruction of enemy forces, with only two friendly casualties.³⁴ It remains a textbook example of a raid and an important event in the history of special operations.

For modern-day SOF, the raid on Cabanatuan holds an important lesson to keep in mind for crisis contingencies in the future operating environment. The speed and tempo of a crisis contingency operation depends on information, the best of which may come from local informants and networks. Without high quality information, the Rangers could not have conducted the raid as quickly as they did, with as few preparations and without rehearsals, and expect to be as successful as they were. In fact, when future USSOCOM Commander Admiral William H. McRaven interviewed former

6th Battalion Rangers who participated in the raid, to an individual they credited the success of the operation with good intelligence.³⁵

OPERATION GUNNERSIDE AND THE SINKING OF THE D/F HYDRO, 1942-1944

An equally significant example of a crisis contingency operation is Operation Gunnarside – the effort to destroy the Norsk Hydro heavy water production plant at Vemork, Norway during World War II. Unlike the 6th Ranger Battalion raid to liberate POWs at Cabanatuan, this operation was to prevent an adversary from achieving a new capability that could prove decisive, or at the very least devastating. Ultimately, Operation Gunnarside was just one of four attempts to prevent or delay Nazi development of an atomic weapon. The successful sabotage of the heavy water production plant was achieved entirely by, with, and through local partners with the British and Americans acting in supportive roles. Norwegian local networks collected information on the facility and the enemy forces in the area, prepared support for the operation, and eventually formed the team of saboteurs – albeit trained and infiltrated into Norway by the British Special Operations Executive (SOE) – to carry out the operation. The local network and saboteurs brought to bear language skills, knowledge of the local area, survival skills for the backwoods of Norway, and special knowledge of the plant in Operation Gunnarside. Furthermore, they continued to monitor the facility after the success of the initial operation, which led to follow-on operations.

After the outbreak of war, the British established the SOE to oversee espionage, sabotage, and reconnaissance networks in Nazi-occupied Europe and eventually Asia. The SOE began training Norwegian exiles and running intelligence networks in Norway, specifically around the heavy water plant at Vemork. A key Norwegian leader at the SOE was Leif Tronstad, a chemistry professor who had helped design the heavy water production facilities.³⁶ From the Norwegian resistance fighters in Britain and Norway willing to participate in subversive activities, the SOE and Norwegian government in exile created the Norwegian Independence Company, known as *Kompani Linge*.³⁷ In Scotland, the SOE trained Norwegian resistance fighters in marksmanship, explosives, hand-to-hand combat, parachute operations, communications, surveillance, morse code, and survival skills.³⁸

Through the Norwegian resistance that comprised locals from around Vemork and workers at the plant, the British eventually had detailed architectural designs, which even included door openings, guard shift schedules and locations, infiltration and withdrawal routes, and specifics of how to disable the heavy water production.³⁹

In June 1942, the British War Cabinet put forth plans to conduct a raid on the heavy water plant based on intelligence of the Nazi regime's desire to increase production.⁴⁰ In response, the British infiltrated four members of the Norwegian Independence Company into the Vidda – a mountainous area around the plant – under the codename Grouse to collect information and report back to the British SOE and British intelligence.⁴¹ Initial planning had the Grouse team acting as an advanced party for thirty British sappers that would infiltrate into the area using gliders in a mission to destroy heavy water production, under the name Operation Freshman.⁴² However, during the infiltration, the planes and the towed gliders faced harsh winter weather and subsequently crashed in Nazi-occupied Norway.⁴³ Operation Freshman was a complete failure resulting in several dead and the injured survivors being captured, interrogated, and eventually executed by the Nazis.⁴⁴ In the debris the Nazis found a map with the words Grouse Group labeled around the plant.⁴⁵ The threat to the local British-supported resistance, pressure on the Norwegian intelligence networks, and the urgency to disrupt the Nazis' heavy water production created the immediacy for Operation Gunnerside.⁴⁶

Once Operation Freshman had failed, the SOE immediately sought to infiltrate a team of five Norwegian resistance fighters, codenamed Gunnerside, to destroy production of heavy water at the Norsk Hydro plant.⁴⁷ The Gunnerside team was led by Joachim Ronnenberg with Knut Haukelid as his second-in-command, both members of the Kompani Linge and trained by the SOE.⁴⁸ The decision was made to insert the team by parachute – a much easier and validated infiltration method than gliders – but inclement weather delayed the team by three months and caused one insertion attempt to abort.⁴⁹ In the meantime, the SOE communicated to the four-man team still on the ground (now named Swallow, after the compromise of Grouse) to prepare to receive the Gunnerside team and continue to collect on the heavy water plant, as the Nazis would likely harden their defences after the failed Operation Freshman.⁵⁰ On the night of 16 February 1943, the Gunnerside team finally parachuted into the Vidda and linked up with the

Swallow team.⁵¹ At a hunting cabin in a remote area outside of Nazi patrols and control, the nine-man team made final preparations for the sabotage mission, to include reconnoitring the most discreet route to the plant.⁵² As it turned out, Nazi defences had in fact been hardened and additional guards brought to the Norsk Hydro plant.⁵³

On the night of 27 February, the Gunnerside team made their way to the plant to carry out their mission.⁵⁴ The team infiltrated via a gorge, crossed a frozen river, and scaled a 500-foot cliff to arrive at the plant undetected.⁵⁵ Once through the fence surrounding the plant, the team split up into a four-man demolitions team and a five-man security team.⁵⁶ The demolitions team was unable to enter the plant through an outside door as planned but gained entrance through an unguarded access tunnel.⁵⁷ While entering the room where the heavy water production cells were located, the team encountered a plant worker.⁵⁸ Dressed in British uniforms, but speaking perfect unaccented Norwegian, the team quickly interrogated him to determine if he was a threat and then ushered him out of the area after helping the elderly night engineer find his glasses.⁵⁹ The demolition team placed two strings of explosives on seven of the nine heavy water production cells and set the fuses for thirty seconds.⁶⁰ To divert Nazi scrutiny from the Norwegian resistance and local Norwegians, the team leader left a British parachutist patch in the room as the team quickly exfiltrated.⁶¹

The demolitions team exited the plant and reconnected with the security team. As the force withdrew from the plant, they heard muffled explosions from inside the production room, confirming success.⁶² The nine-man team withdrew via the infiltration route but split up once arriving at the mountainous plateau in the Vidda.⁶³ Four members of the Gunnerside team, including the team leader Ronneberg, skied roughly 200 miles (322 kilometres) to the border with Sweden and crossed into the neutral country through an unguarded crossing.⁶⁴ Meanwhile, Knut Haukelid, the second-in-command of the Gunnerside team, and the Swallow team split up to separate cabins in the plateau and continued to collect intelligence on the plant and Norway's Nazi occupiers.⁶⁵ Despite Nazi attempts to find the saboteurs, none of the nine-man team were captured.

Operation Gunnerside was a success and even General Nikolaus von Falkenhorst, the head of German forces in Norway, referred to the mission

as “the most splendid coup” upon his inspection of the damaged plant.⁶⁶ Nazi heavy water production dropped off significantly, hampering Nazi experiments and progress toward a functioning nuclear reactor.⁶⁷ An estimated 600 to 700 kilograms of heavy water had been destroyed – the equivalent of four months’ worth of production.⁶⁸ However, the results were temporary. The Nazis would need roughly ten to twelve months to return heavy production back to pre-sabotage levels, delaying supplies of heavy water for twelve to fourteen months.⁶⁹

The Nazis rebuilt the heavy water production cells, repaired the damaged plant, and were operating it again by May 1943.⁷⁰ On 16 November, 140 United States bombers conducted a raid on the Norsk Hydro plant that resulted in negligible damage and several civilian casualties.⁷¹ The operation was undertaken without prior coordination with or notification to the exiled Norwegian government in Britain or the Norwegian resistance.⁷² But the strike did convince the Nazis to cease production at the plant, as they considered it too easily bombed, too costly to rebuild, and its work force too vulnerable.⁷³ Instead, the remaining heavy water of varying concentrations was to be removed and transported to Germany along with the high concentration cells.⁷⁴

On 29 January 1944, Tronstad at the SOE became aware that the Nazis intended to disassemble and remove the high concentration cells from the plant for transportation to Germany along with the remaining stockpiles of heavy water.⁷⁵ Tronstad messaged the Swallow team to confirm and report if action against the transport was possible.⁷⁶ After the success of Gunnerside, the Swallow team had stayed in the area to continue to report on the goings-on at the heavy water plant and were well-positioned to gather the needed information for the SOE.⁷⁷

It was not until 6 February 1944 that the Norwegian resistance learned that the Nazis would move the stocks of heavy water within the week by ferry – not enough time to create a detailed plan and gather needed supplies, assemble a team, rehearse, and execute an operation.⁷⁸ Haukelid, the Swallow team, and the local Norwegian resistance considered several options to avoid civilian casualties, but eventually decided on sinking the ferry and its contents as the best chance at success.⁷⁹ Haukelid reconnoitred the ferry at port in Mael and determined that an explosion at the bow of the vessel

would cause it to sink quickly.⁸⁰ On 20 February, the Norwegian resistance sank the ferry D/F *Hydro* transporting the Norsk heavy water supplies, thus ending the Nazis' heavy water ambitions in Norway.⁸¹

Success in disrupting heavy water production at the Norsk Hydro plant at Vemork was heavily dependent on local intelligence networks and resistance fighters. The operation that eventually disrupted production, if only for a year, was completely Norwegian-led and executed, as was the operation to end Nazi heavy water ambitions with the sinking of the ferry. Both British and American attempts failed, but even the impetus to act in these two instances was dependent on local Norwegian intelligence networks' information. Like the 6th Ranger raid on Cabanatuan, local networks and assistance was a necessary component of this series of crisis contingency operations both in terms of the immediacy to act and the execution. The local networks allowed the British to react with speed and accuracy. Additionally, the local networks allowed the British and Americans to follow-up with additional operations as necessary.

THE GREAT SCUD HUNT DURING THE 1991 GULF WAR

The Great Scud Hunt of the 1991 Gulf War illustrates the difficulty in achieving an operation's objectives without a local partner supplying detailed information. This vignette highlights the pitfalls of relying solely on sophisticated surveillance technology to direct operations. The Iraqi Scud crews used tactics, techniques, and procedures, and low-cost decoys, to routinely defeat the most modern surveillance technology available to the U.S. Air Force and SOF. Once launchers were identified, speed was the key to success, but the time lapse from target identification to bombs on target was usually too long to destroy Iraq's transporter-erector-launchers (TELs). This vignette has obvious implications for the targeting of an adversary's dispersed capability exclusively with technological surveillance and no informants, such as the targeting of weapons of mass destruction (WMD) and their associated delivery vehicles during a war with a WMD-capable adversary.

In August 1990, Saddam Hussein's Iraq invaded the Arabian Gulf nation of Kuwait. In response, the George H.W. Bush administration put together a coalition of forty nations, including several Arab partners, to expel Saddam's

armies from the small, oil-rich state.⁸² Saddam wagered that he could fracture the coalition by drawing Israel into the conflict, cleaving off the Arab nations – who had a contentious relationship with Israel – from the provisional coalition.⁸³ Saddam’s tool of choice was Iraq’s Scud missile arsenal. Iraq had experience with missile warfare during the eight-year Iran-Iraq War that had just concluded in 1989. Iraq had first attacked Iran with missiles in what became known as the “War of the Cities.” While inaccurate, Saddam’s Scuds were a useful psychological weapon of terror and could pressure the Israeli government to retaliate.⁸⁴ On 18 January 1991, Saddam fired the first of eighty-eight missiles that would be launched at Israel, Saudi Arabia, and Bahrain during the war.⁸⁵ In the first week alone, Saddam launched twenty-six missiles at Israel, causing little damage but rousing much fear.⁸⁶

In 1990, when Saddam invaded Kuwait, Iraq operated two types of Scuds – the al-Hussein (600-650 km range) and the al-Abbas (750-900 km range).⁸⁷ The Iraqis had modified the Soviet Scud by decreasing the payload weight and increasing the burn rate of the fuel, which made the missiles less accurate but gave them greater range.⁸⁸ Augmenting the Scuds, the Iraqi army operated two types of TELs – the Soviet-made, eight-wheeled MAZ-543, and the Al Waleed, a modified civilian Saab-Scania tractor-trailer.⁸⁹ Iraqi forces also had twenty-eight fixed launchers at five missile complexes in western Iraq and several training launchers in other parts of the country.⁹⁰ Iraq’s Scuds were not militarily effective but, Saddam knew from experience, they were a useful weapon of terror. Iraq had fired 203 Scuds at targets in Iran during the Iran-Iraq War, creating panic among Iranians while developing experienced, trained, and dedicated missile crews in the Iraqi army.⁹¹

At first, the U.S. attempted to keep Israel out of the war through reassurance by redeploying two Patriot batteries from Saudi Arabia to defend Israel, but these had little success shooting down incoming Scuds.⁹² Next, the U.S. turned to aerial surveillance to locate Saddam’s TELs and employing orbiting aircraft to destroy them. The air war against Iraq’s TELs began the night of 16-17 January.⁹³ The opening salvo included B-52s, F-117 stealth fighters, and Tomahawk missiles to destroy the twenty-eight fixed Scud sites, storage areas, and factories.⁹⁴ In fact, the vast majority of the war’s opening sorties flew against Scud targets and ultimately 2,500 sorties would be flown in Scud hunting missions throughout the war.⁹⁵ Despite the initial air

CHAPTER 2

effort, however, Saddam fired more missiles at Israel and Saudi Arabia on 18 January.⁹⁶

The intelligence picture of Saddam's Scud arsenal and mobile TELs was incomplete. The intelligence community underestimated the number of TELs and lacked knowledge of their locations.⁹⁷ Infrared scanners were used to identify TELs but operators could not distinguish between a TEL and a truck or Iraq's decoys, and in some instances even mistook goat herds for missile launchers.⁹⁸ On the few occasions at night when aircraft spotted Scud launches, they were only able to target the TELs twenty percent of the time.⁹⁹ After three weeks of the failing air operation to destroy Iraq's TELs, and sensing that the Israelis were eager for results, the Bush administration turned to SOF to find, fix, and finish Iraq's mobile launchers. The desire to keep Arab states part of the coalition, and the credibility the Arab partners brought with them, pressured the Bush administration to act immediately.

On 7 February, the first U.S. SOF patrols entered Iraq.¹⁰⁰ The British Special Air Service (SAS) had already infiltrated Scud hunting teams into western Iraq starting on 20 January.¹⁰¹ U.S. SOF and the SAS divided a large swath of Iraq's western desert known as "Scud Alley" into two smaller but still vast sectors.¹⁰² SOF teams in four-wheel drive vehicles flew by helicopter into western Iraq from Saudi Arabia in darkness, moved into hidden sites, conducted reconnaissance patrols at night, and called in circling aircraft on targets.¹⁰³ As one SAS staff sergeant said about identifying Scud sites,

Scuds were usually launched at night and gave a huge signature, a great big ball of light. You could see the fireball at the base of the motor from thirty miles away across flat open desert, and that gave us an indication of where to look. The launcher would be moved immediately after firing.¹⁰⁴

Missions typically lasted for ten days.¹⁰⁵ Both SAS and U.S. SOF destroyed missile facilities and sabotaged fibre optic cables relaying orders.¹⁰⁶ Joint Terminal Attack Controllers (JTACs) from the U.S. Air Force accompanied the SAS and U.S. SOF teams to talk aircraft onto targets.¹⁰⁷ JTACs called in strikes from A-10s and F-15Es when TELs were identified.¹⁰⁸ Coalition aircraft equipped with sensors like Low Altitude Navigation and Targeting Infrared System for Night (LANTIRN) were used to identify Iraqi TELs.¹⁰⁹

However, aircraft typically took fifty minutes to respond while waiting for targeting data to be relayed and sensors on aircraft routinely mistook decoys or trucks for TELs.¹¹⁰

Iraq's Scud crews were well-prepared to survive the aerial targeting and frequently escaped. Crews made great use of high-fidelity East German decoys and similar looking fuel trucks as well as wadis, overpasses, bridges, and other infrastructure to obscure and hide missiles and mobile launchers.¹¹¹ Beyond use of decoys and terrain, Iraqi teams also developed a quick procedure for setup and teardown of their TELs.¹¹² Under Soviet training, the typical time to erect and fire a Scud was sixty to ninety minutes, which the Iraqi Scud teams had reduced to just thirty minutes.¹¹³ Further, the Iraqi teams had reduced the teardown time from thirty minutes to just six.¹¹⁴ These techniques coupled with the inadequacy of U.S. surveillance technology resulted in few confirmed TEL kills.

The outcome of the Great Scud Hunt by coalition SOF left much to be desired. Operating behind enemy lines and deep into Iraq for long periods came with substantial risk.¹¹⁵ Teams in hidden sites were at constant risk of compromise such as what occurred with the now well-known SAS team Bravo-Two Zero, resulting in one member killed, two dead from exposure, and four captured and tortured.¹¹⁶ Another U.S. SOF patrol was forced to hastily evacuate by helicopter after calling in air strikes on an Iraqi mechanized unit.¹¹⁷ Additionally, three were killed in a helicopter crash when an MH-60 crashed into a sand dune at night.¹¹⁸ Ultimately forty-two Scuds were fired at Israel during the course of the war resulting in two civilians killed but caused the later death of fifteen more and damage to hundreds of homes.¹¹⁹ The most U.S. casualties during the war attributable to one incident occurred when a Scud attack killed twenty-eight Pennsylvania National Guardsmen in Dhahran, Saudi Arabia.¹²⁰ Even though Iraq's firing rates declined after the first week of the war, they increased again in the war's final week, demonstrating that Iraq's capability had not been greatly impacted by coalition efforts.¹²¹

The Great Scud Hunt is unlike the other two vignettes presented earlier. Coalition SOF had no local partners and were entirely reliant on the most sophisticated surveillance technology of the day and their own senses to find and destroy Scuds in the vast western desert of Iraq. Iraqi surveillance

countermeasures and launch procedures proved too clever and quick to permit the TELs to be acquired and destroyed in sufficient numbers. The reaction time for coalition SOF, from identification of the TEL to bombs on target, was well outside of the Iraqi missile operators' teardown time. Ultimately, however, the employment of SOF and the dedication of the most sophisticated U.S. aircraft demonstrated enough determination to reassure Israel and prevent it from entering the war, despite no real change to Iraqi missile launch rates.¹²² In that regard, SOF's mission was a success even though the operation failed to have a tactical or operational impact. Furthermore, the Great Scud Hunt sheds light on the complexity and potentially low probability of success of SOF employment against an adversary's dispersed and mobile WMD capability in a future war. SOF is likely to encounter similar difficulties without a vast local network to provide timely information.

FUTURE OPERATING ENVIRONMENT

Most experts agree that the future operating environment will be different than the recent past (2001-present), although assessments of what that means for SOF vary.¹²³ The 2017 National Security Strategy (NSS) directs a change in focus with the introduction of "great power competition." Specifically, the NSS describes the competitions and rivalries the U.S. and its allies face from China and Russia: "they are determined to make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence."¹²⁴ The NSS also addresses North Korea and Iran as states "determined to destabilize regions, threaten Americans and our allies, and brutalize their own people."¹²⁵ While the NSS does mention transnational threat groups (non-state actors), the focus is on those state entities that threaten U.S. interests. This change in focus from non-state actors to states is the most obvious change in the SOF future operating environment since 2001.

Another change to consider is how SOF will operate in this new environment. Instead of direct action (DA) and CT, SOF may need to focus instead on unconventional warfare (UW). General Cleveland describes it as follows:

Now, if you think about UW, it's the orchestration of subversive efforts, of sabotage, of confidence targets, knowing when to increase the tempo of certain operations, knowing when to pull back,

having the discipline to wait when forces in the field aren't ready. It takes somebody that frankly understands all that to orchestrate it properly.¹²⁶

Cleveland and many others have recognized the atrophy of SOF UW skills over the last twenty years. As SOF look ahead, how do they operate in this new operating environment – one that challenges SOF to operate with more than a DA and CT focus? During a conventional war, SOF will be called on to address crisis contingencies and will need to draw on and build from how they operate in the so-called “Gray Zone.”¹²⁷ SOF and how they need to operate in the Gray Zone will be addressed in another volume of this “SOF and Great Power Competition (GPC)” series but a short summary follows. The Gray Zone is characterized by political, economic, informational, and military competition that is more intense than normal diplomatic relations but short of conventional war.

This way of operating across a broad spectrum of mission types has been accomplished in the past. The Cold War (1947-1991) was a period of great power competition between the U.S. and the Soviet Union and their respective allies (western versus eastern bloc). While the post-Cold War period saw the U.S. focus on CT, states such as Russia, China, and Iran began to use Gray Zone operations to advance their interests at the expense of America's. For example, in 2014, Russia's use of “little green men” (masked Russian soldiers in unmarked uniforms) in Ukraine led to the annexation of Crimea by Russia. Meanwhile, since 2013 China has been building artificial islands in the South China Sea, turning them into military and logistical bases. Iran's Gray Zone activities include using indirect means (damaging ships with mines) and foreign proxies (Hezbollah) to provide deniability and avoid direct confrontation. The U.S. response to these Gray Zone activities has been less than decisive. Many call for a U.S. foreign policy strategy of organized political warfare to counter Gray Zone operations of adversarial states.¹²⁸

A strategy of organized political warfare would entail “the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures...and ‘white’ propaganda to such covert operations as clandestine support of ‘friendly’ foreign elements, ‘black’ psychological warfare and even encouragement of underground

resistance in hostile states.”¹²⁹ This chapter’s authors support the idea. Such a strategy would serve SOF well in a conventional war when conducting crisis contingencies. It would allow SOF to work closer with other elements of the U.S. government as well as allies and partners to address crisis contingencies. Whether SOF are conducting reconnaissance, raids, or sabotage; working with proxies or resistance forces; or engaging in a counter-SOF situation, they will be of particular value to integrating the efforts of organized political warfare by planning and executing operations with the assistance of others.

One of the more obvious SOF roles in a future conventional war is to strike at high value targets of operational (and possibly strategic) importance. A crisis contingency mission would involve SOF conducting raids, assaults, ambushes, and sabotage missions against high-value targets, as the historical vignettes illustrated. For instance, while in some scenarios, conventional forces will be forced to adopt a defensive posture in an anti-access/area denial area of operation (for instance, in the Indo-Pacific region), SOF can provide agile forces to strike the enemy’s most important assets where they are most vulnerable.

Many of the SOF roles in crisis contingencies during a high-intensity conflict that have been addressed here are echoed in a recent RAND study titled, “Countering Russia: The Role of Special Operations Forces in Strategic Competition” (November 2021). In this study, RAND concludes that SOF can “help build partner capabilities for resisting foreign invasion and occupation, thus increasing deterrence.”¹³⁰ While the applicability of the RAND study is limited since it deals only with U.S. Army SOF and one adversary (Russia), the conclusions can be (in most cases) extrapolated to the other services and allied SOF, and the threats posed by China.

Working with proxies or resistance forces will be critical for mission success in the future operating environment. SOF success in crisis contingencies lies in the future value of alliances. Indeed, SOF provides the U.S. military with the ability to have a virtual or physical presence in areas deep in enemy territory normally denied to other forces. But that is generally only possible if SOF work with partner forces or through a resistance movement. Working by, with, and through a partner or resistance force is a skill that SOF need to keep sharp. Since successful resistance relies on pre-crisis preparations

of the environment, SOF need to develop resistance requirements and to support planning and operations with willing partners. Opportunities exist. For example, Latvia recently called for a permanent U.S. military presence to guard against Russian threats.¹³¹ Russia's annexation of Crimea in 2014 and outright invasion of Ukraine in 2022 has alarmed the Baltic countries and the rest of NATO. The *Resistance Operating Concept*, published by the Joint Special Operations University (JSOU), argues that "when national resistance planning is integrated with allies and partners committed to the ideals of national sovereignty, territorial integrity, and self-determination, it can become a powerful message against a potential adversary."¹³² Unfolding world events are indicative of the need for SOF to maintain and enhance traditional UW skills, but those skills must be assessed in the context of modern resistance movement dynamics.¹³³

Finally, another potential crisis contingency for SOF in a future conventional war is against an enemy SOF's activities and operations, or counter-SOF for short. An adversary's SOF could trigger a crisis contingency operation through its harassment and disruption of friendly force operations, sabotage of key infrastructure or military capability, and disruption of national capability, among other operations. Hostile SOF operations could provoke a response that bears the characteristics of a crisis contingency operation – the target is of strategic importance, there is an immediacy to respond, and there is no pre-existing plan. Although conventional forces are more numerous and first to be tasked with vital point or rear area security, if unable to stymie adversary SOF, friendly SOF would likely be tasked to assist operationally or as advisors.¹³⁴

A recent example of a counter-SOF crisis contingency operation occurred on 3 January 2020, when U.S. SOF carried out a drone strike against Qassem Suleimani and Abu Mahdi al-Muhandis – the Iranian Quds force commander and a proxy commander respectively – disrupting an alleged series of attacks against U.S. forces in Iraq that could have resulted in hundreds of U.S. personnel killed.¹³⁵ Further, adversarial SOF – Russian SOF specifically – are currently working on counter-irregular warfare, designed specifically to neutralize the West's ability to conduct effective UW.¹³⁶ In the same vein, U.S. SOF is exercising the ability to defend vital points such as remote radar sites that would become targets of adversary SOF.¹³⁷

CHAPTER 2

The growing capability of both Russian and Chinese SOF presents a unique challenge to coalition militaries and SOF in a future conventional war. Russian SOF is particularly adept. As Christopher Marsh, an expert on Russian SOF, notes, “Russia is now emulating U.S. models when it comes to special operations.”¹³⁸ Russia’s use of *spetsnaz* (special designation troops) and the recent creation of Russian SOF (SSO) and the Special Operations Command demonstrate an organized and proven capability. While *spetsnaz* units perform deep reconnaissance, interdiction, intelligence gathering, and act as a rapid reaction force, Russian SOF units are “proper combat units themselves and can operate independently. They are ready for rapid deployment across a spectrum of counter-terrorism and combat missions, on Russian territory and abroad.”¹³⁹

Recent Russian SOF experience in Syria further illustrates this point. As one expert on Russian special operations puts it, “The roles in which SSO units are based in Syria include target acquisition and designation for air strikes, eliminating rebel leaders on the front line and behind enemy lines using ambushes, and storming heavily defended facilities.”¹⁴⁰ Additionally, acting as agitators, saboteurs, trainers and mentors, and potentially directly as combatants, Russian SOF seemingly paralyzed Ukrainian military and law enforcement with their ubiquitous presence during the dismantlement of the Ukraine in 2014 and is a recent example of the significant roles adversarial SOF can play.

China’s SOF presents a less tested and proven challenge, however. According to Dennis Blasko, an American intelligence officer:

Chinese SOF units are much younger than U.S. forces, organized and supported differently, and have minimal real world operational experience. Nonetheless, at the individual and small team level they have proven themselves to be tough and technically competent in international competitions. Their abilities in larger, more complex joint operations remain untested in actual combat.¹⁴¹

China’s SOF do not cover the full range of U.S. SOF roles but instead focus on direct action, special reconnaissance, and counter-terrorism. They will be integrated with the main military force, the People’s Liberation Army, and have less independence than their Russian counterparts. “Although quite

numerous, they were established relatively recently, do not have much real combat experience, and have yet to come into their own.”¹⁴² Much like the Russian *spetnatz* and SSO, Chinese SOF primary roles will focus on military and deep reconnaissance as well as commando and sabotage operations. In both cases, Russian and Chinese SOF are likely to provoke a crisis contingency operation in response to their activities and coalition SOF are likely to be called upon.

Clearly, however, the employment of SOF on defensive tasks is not ideal, particularly since U.S. and coalition SOF capacity will be stretched during major combat operations. The previously discussed missions (reconnaissance, raids, and sabotage on high value targets) will strain the limited SOF assets available. Countering enemy SOF would only add to the already demanding mission sets. That said, should joint forces demand assistance to deal with hostile SOF threats, the similarity in roles between coalition and adversarial SOF could make coalition SOF an effective foil; SOF understand the tactics, techniques, and procedures (TTPs) that are used and are thus well-suited to act as a counter in a crisis contingency.

CONCLUSION

In this chapter the authors have tried to demonstrate that in past major combat operations SOF were highly dependent on local networks to succeed in crisis contingency operations and proposed that this dependency will be the case in a future conventional war in a variety of different scenarios. Also, the four characteristics of future conventional war identified and defined in the introduction to this volume – speed and tempo, lethality and risk, informatized, and interconnectedness – hold significant implications for SOF in a future crisis contingency. Furthermore, technology in a future conventional war will likely cut both ways for SOF, in that raising and maintaining a resistance force and local networks – critical for success in a crisis contingency operation – will be both more difficult and, if the resistance force is viable, more effective. USSOCOM and CANSOFCOM can ensure future success in a crisis contingency by experimenting with and integrating emerging technology now.

The building blocks of the technologies of a future fight are already present in ubiquitous technical surveillance – the combining of biometrics, facial

recognition, voice recognition, internet surveillance, drones, street cameras, and artificial intelligence (AI) – and will likely make raising and maintaining resistance forces and underground networks exceedingly difficult. In fact, current technology infrastructure, as nascent as it is, is doing just that as Russian and Chinese counter-intelligence agencies capture spies and break up intelligence networks in their respective countries.¹⁴³ Terrorism scholar Thomas Hegghammer noted in a recent article in *Foreign Affairs* magazine that the last twenty years of counter-terrorism efforts have only made states more capable in surveillance, and will have obvious impacts for developing resistance movements.¹⁴⁴ The increasing *informatized* world will only make running underground, subversive networks – like the Norwegian resistance in Nazi-occupied Norway or Captain Pajota’s guerrillas in the Philippines – harder to keep undetected. (Chapter 1 deals with the same challenge as it relates to SOF support to theatre break-in efforts.) However, ubiquitous technical surveillance is unlikely to be of the same quality and applied to the same level universally as in Russia and China, and coverage even in those countries varies widely geographically, but one only must look at Xinjiang (Uyghur autonomous region) as an example of what could be constructed in an occupied territory. The challenges such ubiquitous surveillance infrastructure would present to local support of SOF in a crisis contingency would doubtlessly be substantial.

However, the technologies used in technical surveillance do have biases and limitations that can be exploited, and the same technology that makes up technical surveillance infrastructure can be used to avoid that surveillance.¹⁴⁵ U.S. SOF and CANSOF will need to develop TTPs that are exportable to local partners and integrate new technology – also exportable to partners – to defeat adversaries’ detection methods and technologies. Further, and as other authors in this volume propose, SOF will need to integrate with the Joint Force and other defence entities like never before, working with cyber forces and others to avoid, disrupt, or defeat detection. In future crisis contingencies, evading adversary detection for both SOF and their local resistance forces will likely be a significant undertaking.

The technology available in a future fight will likely also make SOF more lethal while lowering risk to force in a crisis contingency. Specifically, *interconnectedness*, as defined in the introduction, can play a large role in increasing precision while increasing standoff and thus reducing risk.

A scenario could exist where SOF are called upon to destroy a certain adversary capability like in the Vemork heavy water plant vignette. Instead of relying on saboteurs to place explosives, perhaps SOF will use a local resistance group to infiltrate individual components of a simple autonomous robot that is then built and employed by resistance fighters against the adversary's capability. This is not so far-fetched and is allegedly what Israeli networks in Iran did on 27 November 2020 in the targeted killing of Mohsen Fakhrizadeh, the alleged chief of Iran's nuclear program.¹⁴⁶ Interconnected "systems of systems" could greatly lessen the risk to force for both SOF and their partnered resistance forces in a crisis contingency operation, while also enhancing lethality. To that end, SOF should experiment with such technology and ensure it is as simplistic as possible to make it suitable for resistance forces, perhaps even creating an entire production line for partner use.

Finally, technology in future warfare, like AI, is likely to increase the *speed and tempo* of a crisis contingency operation. The reaction time in a crisis contingency operation is already compressed, but emerging technology is likely to compress reaction times further and aid in quick decisions (a theme that receives further treatment in chapter 4). For example, the Great Scud Hunt may have gone very differently if AI-enabled surveillance aircraft were available to aid in TEL identification and relay targeting data to orbiting aircraft, or even engage targets themselves as Azeri loitering munitions did in the conflict over Nargorno-Karabakh in 2020. It is likely that the targeting time sequence would have been well within the Iraqi crews roughly 36-minute launch and teardown procedure. Again, to properly integrate such technology into SOF formations, SOF will need to experiment with the technology to ensure its use is effective during a crisis contingency operation.

Crisis contingency operations are likely to be a requirement of SOF in future major combat operations despite no clear existing doctrinal definition. Such operations are likely to mimic what has been demanded of SOF in the past, and SOF are likely to operate by, with, and through partners in future operations. Characteristics of future warfare will likely have both adverse and constructive impacts on how SOF carry out crisis contingency operations. Success will hinge on preparation and integration of emerging technology and the viability and extensiveness of SOF's partner network.

CHAPTER 3

EMERGING HORIZONS FOR SPECIAL OPERATIONS

LIEUTENANT COLONEL KEITH L. CARTER, PhD

After two decades of nearly constant deployments supporting counter-insurgency and counter-terrorism missions, the U.S. and its allies are reorienting to an international environment defined by hegemonic competition. In this environment, the risk of a large-scale war between near peers is a salient threat that requires consideration. Although it is likely that conventional forces would bear a preponderance of the responsibility for fighting a large-scale high-intensity war, SOF would undoubtedly play an important, though likely supporting, role. Aspects of special operations in these conditions will be categorically different than the operational experience of the last twenty years and will pose some unique challenges. Emerging technological horizons will further complicate special operations on a hypothetical future high-intensity battlefield, though some more than others.

This chapter considers some hypothesized, yet probable, features of the future operating environment to establish a common contextual basis for understanding what a conventional war would look like. After establishing an operational framework, some of the emerging technological horizons that are likely to impact SOF will be considered. While selecting which horizons to discuss is a difficult task, this chapter focuses on trends that will presumably have a large impact on warfare and specifically may have an *outsized impact for SOF*. Accordingly, this chapter looks at social media, logistics, and human performance augmentation.

FUTURE OPERATIONAL ENVIRONMENTS

Before proceeding to the emerging technological horizons of interest, it is useful to develop a hypothetical Future Operating Environment (FOE), augmenting certain aspects of the broad characteristics described in this

volume's introduction. Inevitably this hypothetical FOE will be incomplete; nevertheless, it is necessary to have a "use case" for evaluating the operational conditions that are driving the trends in warfare towards the emerging horizons that follow. This hypothetical FOE will factor in the "big picture" trends to provide a set of useful test cases for the possible employment of SOF in a large-scale conventional war.

COMMON FEATURES: LETHALITY, SPEED, AND SENSORS

In a high-intensity conventional conflict between rival great powers, the most salient feature of the operational environment will be the degree of lethality, as described in this volume's introduction. Battlefield lethality between peer combatants armed with modern industrial and information age weapons technology and capable of manoeuvre warfare has been increasing since the First World War.¹ Integrated weapons systems linking sensors to weapons delivery platforms that are increasingly capable of precision, regardless of range, will feature prominently in future conventional wars. These trends imply that if you can be found you can be killed, and thus traditional conventional thinking about massing forces for prolonged periods of time against enemy centres of gravity is an increasingly detrimental construct for military force employment. More likely are military operations where – for a limited temporal and spatial duration – a force can achieve overmatch against an adversary's sensor array to achieve limited objectives, while political end states are negotiated.

The 2020 Second Nagorno-Karabakh war between Armenia and Azerbaijan provides a limited case study of this dynamic, even if neither country possesses capabilities as advanced as those found in China, Russia, the U.S., and some of its NATO allies. In this conflict, *which lasted six weeks*, Azerbaijan massed a precision strike campaign aided by drones, rockets, and artillery that destroyed over a thousand Armenian military vehicles and pieces of equipment.² In addition to showcasing the battlefield effects of a highly lethal precision strike complex, this conflict highlighted the ways that social media, private military corporations (PMCs), alliances, and cyberwarfare are features of modern conventional war.

The conventional lethality of the modern battlefield, as demonstrated in this singular case, implies that there is a premium on containing conflict.

If that is not possible and an open conflict ensues, the lethality of massed precision strike capabilities will advantage states that are able to rapidly locate enemy forces while obfuscating and protecting their own positions. The timeframe and signature associated with the large build-up of forces and the positioning of logistics to “set a theatre” that has underpinned U.S. military hegemony in the post-Cold War era is anachronistic at best and foolish at worst. States will face pressure to rapidly achieve military effects in pursuit of a political settlement or suffer staggering combat losses.

In a peer-to-peer war between great powers, the threat of escalating to a nuclear exchange will constrain senior policy-makers and limit military objectives. The credible nuclear threat inherent in a peer-to-peer war may limit the degree of escalation within a theatre and create pressure to find alternative ways to increase political leverage in post conflict negotiations by expanding the conflict horizontally into other domains or geographic locations.³ Horizontal escalation of a great power conflict could engender opening new theatres of operations to place different pressures on an adversary, creating strategic dilemmas and increasing the leverage that can be brought to negotiations.⁴ Against this specification of a future operating environment, SOF could prove well-suited for potential missions. The following section considers a most likely and most dangerous concept of special operations support to conventional forces in high-intensity conventional war.

MOST LIKELY: ECONOMY OF FORCE IN SUPPORT OF CONVENTIONAL CONFLICT

In many ways, SOF are an ideal choice for governments looking to increase political pressure by expanding a conflict to put more of their adversaries’ forces, assets, economies, and territories at risk. The key distinction in this concept of operation is the application of state power to broaden a conflict in ways that do not necessarily increase the level of violence. Rather, this concept envisions conducting cognitive, economic, diplomatic, and military actions at lower levels and possibly using covert forces. Buying infrastructure debts in Africa, sabotaging oil and gas infrastructure, sending forces into contested regions like the Crimea, cyber-attacks, blockades, and social media misinformation campaigns are some of the proven ways to broaden a conflict and increase political leverage. These missions will likely be

economies of force – they will not be extensively supported. Some will require forces that can have an outsized impact because of their extensive training, indigenous force relationships, and orientation to their areas of operation. In short, some of these missions, designed to broaden a conflict, are tailored for SOF.

MOST DANGEROUS: DIRECT ACTION IN SUPPORT OF LARGE-SCALE CONVENTIONAL WAR

SOF will also likely be used within the theatre of active war. As explored in this volume’s previous chapters, high value targeting, direct action raids, unconventional warfare, and special reconnaissance are all likely tasks. Necessarily these operations will put SOF at increased risk of detection and destruction. Success in this environment is likely a matter of gaining relative superiority by achieving surprise, minimizing detection, and executing rapidly.⁵

These hypothesized “most likely” and “most dangerous” scenarios are a backdrop to think through emergent technological and operational problems and determine where to invest organizational focus on developing solutions. In the following section, social media, logistics, and individual technological augmentations are discussed as three emerging horizons that stand out as requiring some attention. The purpose here is not to fully determine how each trend will affect the operational environment, but rather to direct attention toward three areas that merit further consideration today.

EMERGING HORIZONS: SOCIAL MEDIA IS THE BATTLEFIELD IN THE CONTEST FOR COGNITIVE DOMINANCE

Social media already affects the character of war. Manipulation of the social media environment takes place in the cyber domain but differs from what has been traditionally conceived of as cyber war. Whereas cyber focuses on exploiting software vulnerabilities to penetrate networks, conduct denial of service attacks, or damage computer-driven infrastructure, social media attacks use existing social media platforms to target human cognition by manipulating or fabricating information.⁶

The role of SOF in this horizon is less on the technical cyber component and more on the themes and messaging. Psychological operations forces are positioned to capitalize on using the social media platform to elicit operational effects through emotional appeals, disinformation, and manipulation. Additionally, because SOF often have cultural training, possess language skills, operate closely with indigenous forces, and work in otherwise denied areas, they are positioned to assess the effectiveness of social media psychological operations. In many ways, social media is a natural evolutionary development of classic psychological operations. What is different is the speed of transmission, the ability to penetrate denied environments, and the rapid iterative tit-for-tat that characterizes social media competition for the narrative.

Generationally, today's younger soldiers grew up in an environment where maintaining their social media presence was a ubiquitous feature of their lifestyle. Their senior commanders, on the other hand, grew up in an analog age. While this phenomenon is inherently one that will diminish as mid-grade and junior service members advance through the promotion system, it currently presents tensions within the force and vulnerabilities for adversary exploitation. This tension is similar to that of earlier eras of warfare where soldiers' letters home were censored, lest they be intercepted and exploited by the adversary. Today, where forces operate, tension exists between the need to maintain operational security and to simultaneously allow service members to maintain some contact with friends and family.⁷

The digital signature of unregulated social media use is clearly a security vulnerability that can reveal the locations and activities of forces.⁸ Alternatively, however, blanket bans on social media use risk alienation and possibly reduced support for war at home. Regulations, training, and discipline can reduce the amount of overt information leaked through social media, but even then, the metadata that provides spatial and temporal information is harder to control. In 2018, for example, maps generated by fitness applications showed the geographical locations and boundaries of several U.S. outposts in Afghanistan and other forward deployed locations. While these maps integrated data collected over a period of two years, it is entirely plausible that metadata could be extracted from social media posting and exploited in real time for targeting. Using social media to locate targets is similar to the current operational practices that use electromagnetic

signatures to geolocate targets. As such, integrating this use of social media into the existing practices of targeting and operational security is relatively easy – at least conceptually. The second major way that social media is affecting war is more difficult to understand, although it too has its origins in earlier concepts of war.

Social media is also a new and powerful front in the battle for the control of information. In this front, truth is created, manipulated, and disseminated to maximum strategic effect. Clausewitz's classic aphorism states that war is politics by other means, and social media manipulation is already being used to affect electoral outcomes and further state military objectives. In other words, states already leverage social media to affect political outcomes, either as a component of conflict below the level of open hostilities (as in the case of Russian electoral manipulation in the U.S. in 2016), or as a complementary element in a broader active war (as in the case of the Russian invasion of Crimea).⁹ Other adversaries, notably the Islamic State of Iraq and Syria (ISIS), have used social media as a powerful recruiting tool.¹⁰ Straightforwardly, social media will be a salient feature in future conflicts. The manipulation of truth to create uncertainty, sow division, or fracture public support along existing fault lines is not new *per se* but social media greatly expands the reach and believability of classic Psychological Operations (PSYOPS). As a traditional element of special operations, PSYOPS forces need to be ready to compete in the terrain of social media at all levels of competition and conflict in both offensive and defensive capacities.

Social media attacks and the manipulation of the truth through deep fakes (fabricated or manipulated images and audio of real people) will not be isolated to combatants and will extend beyond the theatres of active combat to the home front. During the 2014 incursion in Ukraine, Russia targeted government forces with descriptive text messages threatening families.¹¹ As the technology of deep fakes advances – potentially enhanced by artificial intelligence processes – these attacks will become much more sophisticated. It is prudent to expect that both soldiers and their families will be targeted with specific and graphic depictions about things like sexual infidelity, injuries, deaths, and other powerful emotional images. Meanwhile, the greater population will be flooded with images and “news” regarding atrocities, civilian casualties, inflated death counts, and other misinformation suggesting that the war effort is failing. Using advanced algorithms to

target specific audiences with tailored media, state sponsored social media attacks will attempt to divide and conquer their adversaries' populations, impugn the legitimacy of the conflict, and cast military operations as partisan, eroding domestic support for continued conflict.

As shown in the recent examples mentioned above, social media operations will inherently target civilians. Social media will be used to influence the morale of the population and its willingness to support the continuation of conflict. Skeptics of social media's utility to affect civilian support for war may invoke the flawed concept of strategic bombing argued by early air-power theorists, such as Hugh Trenchard, Giulio Douhet, William Mitchell, and others. Air power enthusiasts argued that strategic bombing against the enemy's economic centres (a thin euphemism for population centres) would defeat a nation's will to continue fighting.¹² Air power was believed to offer a quick and cheap theory of victory; however, it has repeatedly been shown that air power in isolation through a campaign of strategic bombing is not a sufficient strategy for victory.¹³ Likewise, it is unlikely that social media alone can deliver a decisive victory in an open conventional conflict. More probable is that social media operations will be a significant supporting line of effort.

Given the historical relationships between special and psychological operations, working within the social media landscape is an area that SOF should consider investing, or investing more, in. Importantly however, operating effectively in social media is not exclusively a special operations enterprise. Relationships with technology companies, cyber forces, and other governmental organizations will be essential to developing the tools, messages, and legal authorities to operate in this sector of the information domain. Social media operations during periods of competition provide an ideal environment to develop the professional networks and identify the potential legal problem areas inherent in these activities. Finally, replicating the social media environment should be integrated into training exercises.

EMERGING HORIZONS: TRADITIONAL LOGISTICS ARE FOLLY

In the highly lethal operational environment of peer-to-peer war, the traditional concepts of logistics equate to death. The precision and range of modern munitions, combined with the proliferation of sensors, implies

that logistical supply depots, support areas, and extended ground and sea lines of communication will face survivability challenges. (This is another concrete example of the implications of this volume's theme of *informatized* environments, in which friendly forces are likely to face significant challenges in keeping themselves concealed from the adversary's surveillance and targeting systems.) Even in the limited campaigns against insurgent and terrorist forces in Iraq and Afghanistan, U.S. and allied lines of communication were beset by improvised explosive devices.

Attempting to replicate traditional supply lines against a near-peer with a mature precision-strike complex would be devastating. Nevertheless, despite the dangers, the requirements to sustain combat operations have not diminished. Waging war – especially a high-intensity conventional campaign – will require and consume vast amounts of materiel across all classes of supply. Conventional solutions to protect forward positioned supplies could include extending supply lines, hardening supply depots, or conducting resupply operations where massed combat power creates a limited period of overmatch to penetrate a theatre and deliver supplies. For SOF, often working in smaller numbers in more remote areas, and potentially operating as an economy of force effort, resupply techniques relying on protection and mass will rarely be available. Operating away from conventional supply lines, and maintaining operational momentum while staying supplied, will require creativity, flexibility, and training. Adapting to an operational environment marked by supply scarcity after a twenty-year period of supply excess will require organizational leaders to affect a mentality shift and look for creative solutions. There will not be a single solution to operating in an environment of logistic austerity. Rather, units may have to flexibly adopt different combinations of techniques to meet their operational needs.

Scavenging supplies, living off the land, or supplying through local markets, for example, is in a very real way a return to much earlier logistical concepts of foraging. Foraging, however, requires that a unit keep moving as the landscape is depleted of resources, and potentially alienates the local population.¹⁴ Special operations teams will need to remain in good standing with their host-nation partners, and may benefit from mirroring their partner forces' dietary habits. Training could emphasize sanitation, butchery, and, in the event of protracted war, supporting or utilizing host-nation agricultural practices.

While the effects of limited logistics could be felt daily in the stomach, its impact on mobility and offensive capability may be more profound. The sustained offensive operations characteristic of recent Operation Desert Storm and the initial phases of Operation Iraqi Freedom consumed fuel, ammunition, and repair parts at rates that cannot be supplied or stockpiled in theatre without creating a signature that an adversary could locate and destroy. This implies that the technological advantages enjoyed in recent operations, in terms of vehicular mobility and firepower, may not be as readily available unless SOF develop mitigation practices.

Some mobility issues may be staunched with local economic markets, which are likely able to supply certain of the spare parts and Petroleum Oil and Lubricants (POL) needed if units equip themselves with common local vehicles. Outfitting units with limited numbers of popular vehicles (for example the Toyota Hilux) from likely areas of operations so that operators can learn how to repair and modify them in the field for military operations is a prudent, relatively low-cost strategy. Alternative forms of energy and transportation should also be explored. Motorcycles, for example, consume less fuel and are easier to maintain than cars or trucks. Hybrid vehicles powered by an admixture of combustion, electric, and solar are worth further exploration. Long range foot marches (potentially augmented by pack animals) are also a possibility for SOF operating in a logistically denied area of operations.

While the reduction of vehicular mobility is likely one element of reduced offensive capability, the other is ammunition consumption. Traditional offensive operations are ammunition intensive. Echeloning indirect fire with artillery pieces and mortars rapidly consumes on hand stockages, and moving bulky, heavy rounds while maintaining a low signature is impractical. The same is true even for small arms. To take but one example, medium machine guns firing between a sustained rate of fire and a rapid rate of fire will consume between 100-200 rounds per gun per minute.¹⁵ Even if used conservatively, machine guns in support of an assault force's manoeuvre or providing final protective fires in the defence will easily consume thousands of rounds. At a weight of seven pounds per hundred rounds, moving 10,000 rounds requires 700 pounds of carrying capacity – and this only represents enough ammunition for two machine guns to provide thirty to sixty minutes of support, depending on the rate of fire,

and is exclusive of all other equipment. Given the degree to which current tactics are underpinned by massing firepower, a possible lack of secure and readily accessible logistics represents a significant impediment to existing concepts of operation.

While ammunition is a great illustrative example of the larger overarching problem of logistic scarcity, all classes of supply will be adversely affected. Inevitably there will be technological solutions to some of these problems, for example logistic resupply drones, load carrying robotics, or exoskeletons. However, pursuing technological solutions without thinking about addressing the underlying structural operational conditions of logistic scarcity will not satisfactorily address the problem and provide the solutions that future warfare scenarios will require.

Other militaries have faced such logistic challenges and managed to sustain operations – at times against a logistically superior opponent. For example, the Ho Chi Minh trail network was effectively used for well over a decade to supply Viet Cong operations in South Vietnam.¹⁶ This vital logistic conduit was largely responsible for sustaining Viet Cong operations, despite being predominately a foot path that took up to five months to travel.¹⁷ In this case, the key to North Vietnam's victory was matching the tactics of their guerrilla force to their logistical reality that any large scale supply operation that the U.S. and South Vietnam could find could be destroyed with superior air power. For forces accustomed to regular access to hot meals, soft beds, ice cream, and fully apportioned gyms, the logistical reality of peer-to-peer conflict will be a hard transition. Mental and physical deprivation, a soldier's more historically consistent experience, will be the norm. Operational concepts that consider logistical scarcity almost certainly need to be developed and implemented by SOF.

EMERGING HORIZONS: HUMAN PERFORMANCE AUGMENTATION

Humans use technology to augment their sensory, physical, and cognitive abilities. The modern battlefield is replete with technological enhancement. Night vision goggles, heads up displays, and wearable computers are ubiquitous, but these are all tools *used* by humans. They exist separately from biological organisms and using them reflects a binary choice on the

part of the user between using or not using. Advances in human modification, however, integrate modern technology with the biological organism, erasing the distinction between tool and user.

For an example, consider the difference between Cochlear implants and hearing aids. The latter amplify sound and limit extraneous background noise, enabling the user to better distinguish and understand auditory stimuli.¹⁸ Cochlear implants, on the other hand, involve surgery to implant a component of the system into the body either under the skin or, in some cases, into the bone behind the ear.¹⁹ The implant acts as an intermediary between an external sound processor, which receives auditory information from the environment, and the brain.²⁰ The user can remove the sound processor, but the implanted device remains – it is inseparable from the user. Cochlear implants are one example of a larger set of neuroprosthetics, which fundamentally lessen or erase the distinction between tool and user.

Neuroprosthetics integrate a prosthetic device with the individual through a brain-computer interface.²¹ And, it is not difficult to imagine a technological horizon where neuroprosthetics have advanced to a level where they outperform human physiology. Once that threshold is reached, it is possible that elective procedures for cognitive and physical enhancement will become a feature of the human experience. There are a variety of possible military applications for neuroprosthetics, extending the range of the existing senses, increasing physical strength and endurance, accelerating processing speed and memory storage, or allowing geospatial tracking. Furthermore, there is no reason to limit the conception of neuroprosthetics to internally implanted technology. Exoskeletons are already in development and are delivering performance gains in strength and endurance.²² It is entirely conceivable that external devices will connect to users through brain-computer interfaces creating technologically augmented soldiers.

Integrating technology and human neurophysiology is not the only way to enhance human performance. Some nootropic drugs – designed to enhance a range of cognitive, memory, and attention skills – are already in use. Amphetamines, for example, though not without controversy, were used by military aviation in the recent wars in Iraq and Afghanistan to extend the length of combat sorties and counter fatigue.²³ There are also drugs, such as anabolic steroids, that produce some obvious benefits (though not

without well-known side effects) for individual physical performance. There is evidence that soldiers serving in elite units such as the U.S. Army Rangers have used steroids illegally to maintain a performance edge in combat.²⁴ Given the possible performance gains nootropic pharmaceuticals offer, it is not difficult to imagine an increased interest in their use for SOF.

The performance enhancement of humans whether through technological augmentation or nootropic drug use is beset with serious ethical dilemmas. To what degree can governments require their soldiers to either implant technology or take drugs even when there are definitive combat performance outcomes to be gained? Western militaries underpinned by broad liberal understandings of individual freedoms are likely to take a different position on this question than authoritarian governments. Western governments will likely pursue less invasive technologies such as exoskeletons over surgical implants, and Performance Enhancing Drug (PED) use, and if approved, will be restricted and tightly controlled. Authoritarian governments have more latitude to coerce their armed forces, which increases the probability that, in the event of a conventional war, Western forces will encounter enhanced adversary forces. By far the most likely form of enhanced human performance in the short term will be through pharmaceuticals, but an eye must be kept on the horizon for advances in both technological and genetic human performance augmentation.

CONCLUSION

There are prolific challenges to existing SOF concepts of operations in large-scale conventional war, and in many ways, the operational experiences gained by Western forces in Iraq and Afghanistan work against developing strategies for success in a highly lethal peer-to-peer contest. In this chapter, three horizons are illuminated, admittedly in minimal depth, for further consideration. Social media, logistics, and human performance augmentation are all areas where there is evidence that current approaches will not be entirely sufficient without further work to monitor and react to the changing operational environment. These horizons by no means exhaust the set of emerging security challenges, and further study of the field is required. Furthermore, these areas represent both risk and opportunity for Western SOF. There are many possible ways that the challenges presented above can become strengths and our peer adversaries are facing the same operational

CHAPTER 3

constraints. Experimentation with new concepts of operations within the constraints hypothesized for high-intensity conflict is a sound and necessary strategy for developing viable solutions to emerging problems. While it is almost certain that the hypothesized operational environment will not fully capture all the complexity of an actual peer-to-peer conflict, it is also true that some of the solutions will be rapidly tailorable and provide a starting point to orient the force toward the emerging horizon.

CHAPTER 4

FUTURE TECHNOLOGIES FOR SPECIAL OPERATIONS FORCES

TONY BALASEVICIUS

The development and fielding of new and emerging technologies are a priority for all advanced militaries. This requirement exists because the introduction of new technologies onto the battlefield has the potential to change the environment in which forces operate. And, the right technology can provide significant advantages to the side that can create that change. One of the most dramatic illustrations of this potential can be seen with the Allied development of the atomic bomb during the closing stages of the Second World War. More recently, the introduction of the internet has created a totally new form of fighting. Not only has cyber warfare become an important domain in its own right, but ongoing research is evolving it into a critical enabler for a host of capabilities within other military domains.¹

Despite their sometimes game changing successes, emerging technologies can often be difficult to evaluate for their actual potential. This reality is due to the fact that there is always a great deal of uncertainty as to which technologies will actually produce the desired results. In addition, there is often no fixed date as to when the development will mature sufficiently to be of practical use. Finally, more often than not, promising technologies produce little more than incremental improvements to current capabilities.²

Although new and emerging technologies have the potential to redefine warfare, new types of fighting can also arise by fusing different combinations of emerging and established technologies with organisational change to create new operating concepts. The development of German *blitzkrieg* and American Air-Land Battle doctrine are clear examples of this process bringing about fundamental change on the battlefield.³ Thus, when evaluating the possible benefits of technology, it is always important to consider the different opportunities for possible change.

This consideration is even more important for Special Operations Forces (SOF) since their real strength lies in the quality of their operators and what they can achieve rather than in the technology that they are using. As such, the integration of the latest technologies into their force structure may serve to enhance their overall performance, but it is rarely a panacea. That said, new threats are rising for the Western world and SOF will be expected to continue playing a critical role in addressing those perils.

Unfortunately, securing that future will need to occur within the context of a wider and far more demanding environment, one that is witnessing the emergence of a new world order where peer competitors have access to the same, and in some cases better, technology than their Western counterparts. In this situation, SOF will need both the cognitive flexibility and the right tools to properly adapt to conflict in a new, expanded, and far more complex battlespace.⁴ In this situation, selected technologies could play a critical role in aiding future SOF success.

To understand how emerging technologies may be able to aid future SOF operations, it is important to appreciate certain characteristics of the likely environment SOF will be expected to operate in.

KEY ASPECTS OF THE FUTURE SECURITY ENVIRONMENT

The international order is moving from a unipolar world dominated by the United States and its Western allies to a multipolar one where both China and Russia are playing increasing roles on the world stage. Major security trends since the Russian invasion of Crimea in 2014 suggest that dealing with these incipient states will not be easy.

In fact, international relations between China, Russia, and the Western World are currently characterized by very intense competition that has been focused on gaining economic, political, and military advantage using both direct and indirect (asymmetric) methods to achieve desired outcomes. As a result, Western nations have begun facing a variety of threats covering the full spectrum of conflict, with multiple threats occurring simultaneously – not the least of which includes Moscow’s February 2022 invasion of Ukraine and associated threats to regional security.⁵

The Russians, who have driven much of this change in the character of contemporary conflict, have clearly articulated their public belief that the world is now in a continual state of conflict. They also believe that wars are no longer declared and, having begun, will move in different and unfamiliar directions.⁶ According to General Valery Gerasimov, the Chief of the Russian General Staff, this new “template refers to asymmetrical operations using a host of [strategic] capabilities that can be used to nullify an enemy’s advantages in conventional armed conflict.”⁷

Some relatively recent operations carried out by the Russians suggest that the core capabilities needed to affect change will rely heavily on the employment of Special and Specialized Forces linking up to coordinate the activities of internal opposition groups throughout a targeted country.⁸ Once this is achieved, the idea is to expand influence so that an operating front can be established throughout as much of the enemy’s territory as possible. These actions are combined with information operations, cyber warfare, legal warfare, economic war, and other state level activities that are all linked to a strategic outcome and are constantly modified to meet the specific needs of a particular operation.⁹ Such methods, employed and sequenced properly, can, in a very short period of time, throw a stable and thriving state into a web of chaos, humanitarian upheaval, and outright civil war, making it susceptible to foreign intervention or takeover.¹⁰ The Russians believe that the idea of collapsing a state onto itself through social upheaval is becoming an important part of future conflict’s underlying methodology. As such, conventional warfare may in some conflicts be downplayed to focus efforts on the broader use of political, economic, informational, humanitarian, and other non-military measures. These tools are coordinated with the protest or resistance potential of a target population.¹¹ Examples of this trend can be found in the Russian takeover of Crimea and the Donbas region of Ukraine in 2014. NATO has also used elements of this strategy in Libya, where a no-fly zone and naval blockade were combined with the use of private military contractors working closely with the armed formations of the opposition.¹²

Critical to this change has been the introduction of new information technologies, which have opened the information space to the widespread use of asymmetrical applications. For the most part, this has been used to reduce the fighting potential of an enemy through influence operations.¹³ Should

conflict need to escalate into all out warfare, these asymmetric activities will be followed up by an extensive use of high-precision weapons with simultaneous and heavy strikes on the enemy's units and important military, political, and economic facilities. If this is not effective, peer adversaries will begin employing a greater range of conventional military capabilities.¹⁴

This eventuality would entail operations that attempt to roll over areas of resistance in an effort to destroy enemy units. Where possible SOF may be used to coordinate operations between conventional and irregular forces. This function would also include attacks on specific targets and reconnaissance missions to identify enemy units and call in missile, artillery, or air strikes. It is expected that these types of actions will destroy a defender's remaining military capability while manoeuvre operations by ground forces continue to surround points of resistance, take additional territory, and carry out mopping-up operations.¹⁵

Notably, Western military assessments of future conflict acknowledge the rise in interstate competition, suggesting that sub-threshold asymmetric activities will complicate decision-making and responses.¹⁶ In the short term, it is expected that strategic and tactical level actions will be increasingly compressed.¹⁷ The continued emphasis on asymmetric approaches will also likely see a greater integration of non-state actors and various forms of irregular warfare into conventional operations.¹⁸

A major concern for national security forces is the possibility that violent extremism and international criminal organizations will be employed by competitors to threaten target populations. Their aim would be to slowly erode social stability over the long-term. The fear is that these threats will come together with state and other "non-state actors to augment and diversify power projection. In the process, these internal threats will have the ability to access greater and more sophisticated resources."¹⁹

For military forces, the biggest change on the battlefield is the move towards a greater expansion of operations across all military domains, including land, sea, air, space, and cyberspace. More importantly, these domains are becoming more integrated with operations on the cognitive, moral, and physical planes. This trend is moving the focus of conflict towards multi-domain operations as competitors seek to simultaneously dominate the

physical, virtual and cognitive planes in order to gain tactical and strategic advantages.²⁰

The move to multi-domain operations is forcing decision-cycles and reaction times to become more compressed. Furthermore, Western militaries are increasingly required to conduct operations under persistent surveillance, as they seek to overcome advanced capabilities from global competitors. Additionally, major players are becoming more proficient in the novel areas of cyber warfare, counter-space, electronic warfare, and robotics.²¹

As a result, both peer state competitors and sophisticated non-state actors are starting to challenge Western dominance in almost every domain. This development is a significant change for Western military forces, who have long maintained both a technological advantage and overall dominance in all domains over their adversaries.²²

To ensure future success in this environment the West will need to adapt to this new reality. That will mean that as the West's technological advantage is being reduced in one area, advantages must be either re-established or recouped in other capacities.²³ The key to dominating the domains will be to control the cognitive, moral and physical planes.

KEY FINDINGS FOR THE FUTURE OF SOF

As SOF has extensive experience with asymmetric warfare and dealing with non-state actors, they are currently best positioned to take the lead in these areas. This approach means that their services will likely increase significantly over the coming years. They will need to work closely with state and non-state actors and other partners/stakeholders to maintain and possibly regain security dominance in a country or region that has been targeted by a competitor state.

However, as we have seen, the character of the environment in which they will need to operate in will be evolving. There will be a greater and more integrated use of information operations, cyber warfare, legal warfare, economic war, and other activities. Moreover, operations will be carried out across all domains and planes. This reality means that decision-cycles and reaction times will become more compressed at a time when SOF will

need to deal with an expanding battlespace and an ever-widening umbrella of persistent surveillance (that is, the *informatized* operating environment discussed in this volume's introduction). They will also face increasing threats from a plethora of high technology weapon systems that are currently available to all major competitors.

Future SOF missions will continue to place heavy emphasis on an ability to develop relationships with like-minded partners, while putting more importance on unconventional warfare operations. However, such operations will become far more complex as they will need to incorporate a diverse array of mission sets and tasks. Moreover, SOF will have to accomplish these missions and tasks on a battlefield where all sides have a more balanced set of capabilities.

Dealing with the reality of an increasingly high-stress cognitive and physical environment means that gaining and maintaining cognitive overmatch will be critical to future success. To achieve this outcome, research will need to focus on areas where SOF can gain and maintain a cognitive advantage over their opponents. Doing so will eventually lead to control and dominance over contested domains. However, to do this, operators will need to be empowered with technologies that can enhance their cognition. Specifically, they will need increased situational awareness, the ability to reduce their cognitive load, and a means to accelerate their decision-making process.²⁴

As operators become more focused on battle in the cognitive plane, future research priorities may need to emphasize reducing the SOF personnel burden. This requirement can be done by replacing soldiers with machines where it is feasible to do so.²⁵ Importantly, in order to achieve these outcomes, it is critical to understand where the current research priorities are focused and how SOF might benefit from those efforts.

EMERGING TECHNOLOGIES THAT COULD IMPACT MILITARY FORCES

Since the 1970s, advanced militaries have sought to focus their research efforts on specific areas of emerging technology. These areas generally emphasize extending the range, volume, and accuracy of weapon systems, improving system integration, increasing transparency on the battlefield,

and concentrating more firepower, speed, and protection within smaller tactical teams and units.²⁶ These efforts paid off for Western coalition forces during the 1991 Gulf War, where the effectiveness of new high-tech weaponry, along with advanced surveillance and target acquisition, as well as command and control systems, produced devastating results very quickly.²⁷ Based on that success, these research priorities have remained the focus but have evolved as military organizations seek to realize different types of advantage from developing technology. Currently, some of the major areas of interest include:

- artificial intelligence;
- lethal autonomous weapons;
- hypersonic weapons;
- directed energy weapons;
- biotechnology;
- quantum technology; and
- hybrid-electric technology.²⁸

It is important to realize that not all of these areas will apply to SOF priorities, at least not in the short-term. However, over the coming years, they are likely to drive change within larger conventional military organizations so it is important to have a general overview of what they are and what the hoped-for results might produce. Even if SOF are unable to make use of them, they are technologies that are likely to be employed against them.

ARTIFICIAL INTELLIGENCE (AI)

The term AI refers to computer systems that are capable of human-level cognition. Research in this area is broken down into two distinct categories, referred to as narrow AI and general AI:

Narrow AI systems are able to perform specific tasks which they have been programmed to carry out. These systems are currently being incorporated into a number of military applications such as intelligence, surveillance, and reconnaissance; logistics; cyber operations; command and control; and semiautonomous and autonomous vehicles; and²⁹

General AI systems are far more complex and will be capable of performing a broad range of tasks including those for which they have not been specifically programmed. However, it is important to note that General AI systems do not yet, and may never, actually exist.³⁰

The main advantage of AI-enabled systems is that they have the potential to “react significantly faster than systems that rely on operator input. Moreover, they can cope with exponential increases in the amount of data that is available for analysis.”³¹ The long-term hope is that AI-based technologies will augment and eventually replace human operators who will then be available to perform more complex and cognitively demanding work. This outcome would have the potential to reduce both cost and personnel requirements by allowing militaries to field more systems with fewer operators.³²

AI could also impact areas such as remote sensing and electronic warfare, where ground forces could reduce an adversary’s ability to effectively communicate and navigate on the battlefield.³³ Researchers hope that in time AI could enable the development of “new concepts of operations, such as swarming (i.e. cooperative behaviour in which unmanned vehicles autonomously coordinate to achieve a task) that could confer a warfighting advantage by overwhelming adversary defensive systems.”³⁴

LETHAL AUTONOMOUS WEAPON SYSTEMS (LAWS)

LAWS are a category of autonomous military systems that can independently search for and engage targets based on a set of programmed constraints and descriptions.³⁵ They are also known as “human out of the loop” or “full autonomy.” The primary issue with LAWS technology is that the idea of a machine making the decision to use lethal force rather than a human is currently not an acceptable option. As a result, it is unlikely that full autonomy will be given to Western machine systems anytime soon.³⁶

A more likely event is the increased employment of “human on the loop” autonomous weapon systems. These give operators the ability to monitor and halt a weapon’s target engagement should the need arise. Another category on this platform is semi-autonomous, or “human in the loop,”

weapon systems. These systems “only engage individual targets or specific target groups that have been selected by a human operator.”³⁷

Although such systems are unlikely to be employed on the battlefield anytime soon, a key benefit of continued research into LAWS is that weapon systems will continue to increase the “accuracy of weapon guidance on military targets, while contributing to lower rate of unintentional strikes against civilians and civilian targets.”³⁸ Also benefiting from this research is the overall advancement of autonomous vehicles, which can significantly reduce the number of human operators in areas such as logistics and transportation.

HYPERSONIC WEAPONS

Hypersonic weapons are normally defined as fast, low-flying, and highly manoeuvrable weapons designed to be too quick and agile for traditional missile defence systems to detect in sufficient time to provide a counter action.³⁹ These weapons can fly at speeds of at least Mach 5, or five times the speed of sound.⁴⁰ Currently, there are two categories of hypersonic weapons:

- Hypersonic glide vehicles that are launched from a rocket and then glide to a target; and
- Hypersonic cruise missiles that are powered by high-speed engines for the complete duration of their flight.⁴¹

Unlike ballistic missiles that can also travel at hypersonic speeds, hypersonic weapons do not have to follow a parabolic ballistic trajectory. This means that they have the ability to manoeuvre en route to their destination, making defence against them extremely difficult.⁴²

Some analysts believe the technology could hold significant implications for strategic stability. First, “the weapon’s short time-of-flight, which, in turn, compresses the timeline for response, and secondly, its unpredictable flight path, could generate uncertainty about the weapon’s intended target and therefore heighten the risk of miscalculation or unintended escalation in the event of a conflict.”⁴³ However, at the tactical level, the main issue revolves around the difficulty to defend against them since a swarm of these systems, once unleashed onto a single target, can easily overwhelm a defensive systems with speed and mass numbers.⁴⁴

DIRECTED ENERGY (DE) WEAPONS

Directed energy weapons use concentrated electromagnetic, rather than kinetic, energy to achieve results. As such they can “incapacitate, damage, disable, or destroy enemy equipment, facilities, and/or personnel.”⁴⁵ The current research focus in this area centres around their possible employment as short-range air defence (SHORAD), counter-unmanned aircraft systems (C-UAS), or counter-rocket, artillery, and mortar (C-RAM) missions.

The main hurdle facing the quick introduction of this technology has been the inability to find a sufficient power supply to recharge (reload) the weapons. However, if that issue can be overcome, DE weapon systems could become a viable static defence against missile salvos or swarms of unmanned systems as they will have a nearly limitless supply of ammunition.⁴⁶

BIOTECHNOLOGY

Biotechnology leverages life sciences for technological applications. This research area holds a number of potential implications for future military operations including the modification of plants, animals, and humans to either enhance or degrade operational performance. From a tactical perspective, this technology could be used to create such things as adaptive camouflage, cloaking devices, or lighter, stronger, and – potentially – self-healing body and vehicle armour.⁴⁷

QUANTUM TECHNOLOGY

Although quantum technology has not yet reached maturity, in the longer term, it is hoped that it will have significant implications in the areas of military sensing, encryption, and communications. For example, quantum communications could enable secure communications that prevents interception or decryption.

Other military applications might include “quantum sensing, which could theoretically enable significant improvements in underwater detection, rendering bodies of water transparent.” Advances in this area may also “provide alternative positioning, navigation, and timing options that could in theory allow militaries to continue to operate at full performance in

Global Positioning System (GPS) degraded or denied environments.” That said, widespread adoption will likely require significant advances in materials science and fabrication techniques and as such this a technology that provides few if any short-term benefits.⁴⁸

HYBRID-ELECTRIC TECHNOLOGY

Recent studies have concluded that all-electric ground vehicles are not a practical option for most battlefield vehicles into the foreseeable future. As a result, hybrid electric technology is becoming an increasingly important area of research into alternative power solutions for both future manned and unmanned military vehicle systems.

Hybrid-Electric Drive (HED) vehicles are powered by an internal combustion engine, an electric motor(s), and an energy storage system, usually consisting of batteries. These vehicles are recharged through regenerative braking and the internal combustion engine that is coupled to a generator.⁴⁹ Because HED vehicles charge themselves, they do not require charging stations so they can still tap into the existing infrastructure that is available for supplying fuel. This ability means that militaries do not have to replace their existing battlefield infrastructure.⁵⁰

Other advantages of HED could include improved fuel economy and range, packaging flexibility, lower life cycle cost, and improved mobility. More importantly, the onboard batteries can also be used to power additional auxiliary loads that can reduce overall engine idling when stopped. Researchers hope that together, these features can result in better overall fuel economy without sacrificing performance on the battlefield.⁵¹

TECHNOLOGIES THAT COULD BENEFIT SOF

To increase performance for operating effectively in the future operating environment, SOF priorities should be placed on enhancing the operator and team’s ability to carry out their missions in the most efficient way possible. Key to doing this will be to focus on better overall cognition that entails increasing situational awareness, reducing cognitive load, and accelerating the decision-making process.⁵² Research will also need to focus on areas where tasks can be eliminated or handed over to machines. Thus, areas

of interest should include technology that enhances cognitive overmatch, autonomous military vehicles, and hybrid-electric technology.

Cognitive Overmatch

Developments in AI appear to provide the best option for SOF to deal with issues of cognitive overmatch, at least in the short-term. In addition, AI could have a significant impact in areas such as autonomous vehicles, lethal autonomous weapons, human machine interface, and big data analytics. All of these areas have a direct bearing on a variety of different future SOF capabilities and mission requirements.

In fact, research is already moving in this direction. The U.S. military is currently developing future SOF operators and teams that will become more empowered by technologies that enhance situational awareness, reduce cognitive load, and accelerate the decision-making process.⁵³ This concept is referred to as the Hyper-Enabled Operator (HEO).⁵⁴

When fully operational, the HEO will have technological aids to significantly shorten the time needed to complete the observe, orient, decide, and act (OODA) loop, thereby providing the hoped-for cognitive overmatch. The HEO concept is envisioned “as a system of cutting-edge electronics – including sensors, processors, and augmented reality, to provide operators with a tactical edge.” Its main objective “is to provide the right information to the right person at the right time without overloading them.”⁵⁵

Alex MacCalman, who served as director of the hyper-enabled operator joint acquisition task force, believes that increased digitization will reduce an operator’s workload thus allowing them to focus their attention on more high value activities. He believes that artificial intelligence will be key for achieving these goals.⁵⁶

The project has “identified 31 different technologies that will allow for hyper-enabling an operator. These 31 technologies are grouped into five larger categories that include sensing, algorithms and processing, communication, human-machine interface, and system level technologies.”⁵⁷ The research is currently focused on increasing AI performance in four technology areas including communications, computing, data/sensors, and

human-machine interfaces. Eventually, it is hoped that tailored information can be pushed to a dismounted operator or unit in the field regardless of where they are or what they are doing.⁵⁸

However, achieving this will require heavy investment in areas such as data, presentation, and computation.⁵⁹ Moreover, developers will have to overcome issues with long-range communications and optimizing data throughput in contested environments. MacCalman assesses that “the management and distribution of computer processing from the cloud down to edge (battlefield) devices is another area for development.”⁶⁰

In the end, researchers hope that “these efforts will foster a more data-centric culture so that increased digitization will reduce operators’ workloads for a variety of tasks, allowing them to focus their attention on more high value activity.”⁶¹ As operators become more focused on the cognitive plain, SOF research will need to help reduce personnel requirements. The ideal solution would be to replace as many human soldiers as possible. To do this, investments in Autonomous Military Vehicles may need to be considered. In fact, a number of major powers have already established different applications for both semi and fully autonomous military vehicles.

Autonomous Military Vehicles

Militaries are already starting to move in this direction. American SOF are investing in autonomous light tactical all-terrain vehicles (LTATV). Analysts expect that these systems will initially be employed in a variety of missions including infiltration, reconnaissance, and medical evacuation.⁶² According to U.S. Colonel Joel Babbitt, program executive officer for the SOF Warrior program, in the short-term, “Autonomy could also reduce manpower requirements for logistics and resupply missions, especially when special operations forces are spread out over large areas.”⁶³

The natural progression for this research is to see unmanned ground vehicles eventually become capable of autonomous target identification – and, ultimately have the potential for target engagement. Over time, Autonomous Military Vehicles will cross over into different types of fighting vehicles that can carry out a variety of missions for SOF. Missions could include such things as perimeter security, overwatch, and fire support.⁶⁴

Hybrid-Electric Technology

With future SOF operations requiring an increasingly extensive array of communications and information processing capabilities, more energy will be needed. The most practical way to obtain this is by using a vehicle as a platform that can be configured with the necessary power requirements.⁶⁵

In the short-term, hybrid-electric technology is a well-established and proven option. In addition to providing a larger power source for various suites when the electric system is in use, it can provide teams with additional stealth, especially as they carry out their final approach to their objectives. According to Babbitt, “When it comes to the hybrid technologies, it’s really about the last 15 minutes as you’re approaching the objective.” He explains, “If a Prius can sneak up on you, then certainly something that SOCOM has should be able to sneak up on you.”⁶⁶

Another benefit of hybrid-electric technology is the ability to increase the length of time electrical equipment such as sensor suites can run when the vehicle is shut down.⁶⁷ Although the technology is currently available in the civilian market, a great deal of research and testing is still required to make sure it can stand up to the extreme conditions and requirements of the battlefield.

CONCLUSION

SOF have unique operational challenges, but in the end, rely on individual operators and small teams to get the job done. As such, research into future technologies must focus on enhancing individual and team performance. Moving forward, the major areas of interest for SOF should include exploiting technologies that can increase an operator’s overall cognition so that they can deal with the complexities of the evolving security environment.

Current developments in AI appear to offer this opportunity. As time goes on, operators will be increasingly expected to do more with fewer resources. As such, autonomous vehicles and systems with the help of AI may aid in covering off shortfalls in personnel. Finally, hybrid-electric technology has the potential to reduce the logistic burden while providing SOF teams with a platform to carry and power more systems.

CHAPTER 5

SOF ORGANIZATIONAL CONSIDERATIONS

LIEUTENANT COLONEL C.G. LANDRY

For those with insight into military institutional design, a DOTMLPF analysis would be a sound way to examine what a SOF element must do to become more prepared for those high-intensity conflict roles discussed thus far.¹ And, while that would be appropriate should our efforts be to assess a specific military element – the United Kingdom’s Special Air Service (SAS) or the United States’ Navy SEALs, for example – our intent remains to consider SOF within the context of Clausewitzian warfare more generally, and so SOF organizations must remain generalized through our analysis as well. As such, in this chapter we will consider those high-end warfare tasks relative to SOF in a generic sense by asking the question, what must a SOF organization consider to achieve readiness for high-intensity warfare environments?

Two terms within that question require further attention. First, when we discuss *readiness*, we are referring to a state of preparedness to conduct assigned missions. In other words, if a war broke out tomorrow, how “ready” would a given military unit be to fight in its designated role effectively and win?² Some might take this concept for granted, but since there can be long periods of time between wars, generating and sustaining readiness is often the central business for a military on most days. In isolation, tactical military leaders tend to measure readiness by echeloned units at each level, but that assumes too much for our query.

Second, and progressively, the term *organization* is meant here to encompass a broader perspective with regards to readiness and thus what establishing real readiness means. For this chapter, it may not be enough to acknowledge organizations simply as assemblages of people, each of whom has a different purpose or collective purpose towards some greater utility. Organizations are also a result of organizing, implying an active aspect to what otherwise might be thought of as a static entity. Thus, for a SOF organization, their

collective purpose and national utility is the ability to perform assigned tasks during anticipated periods of conflict. Rather quickly, the connection between readiness and how we organize becomes apparent, as organizational functionality is a by-product of readiness. But more so, the SOF organization's contribution to readiness is equally important as it relates to resourcing and decision-making processes, coalescence between structure and organizational behaviours, internal management policies, and of course, military training.

That said, this chapter is not meant to be a dive into organizational theory, just as it is not meant to be a detailed DOTMLPF analysis. Rather it is simply meant to provide considerations along many of those same lines. This chapter will break down those organizational considerations in five parts. First, we will take a brief look at how two decades of the Global War on Terrorism (GWOT) (2001-2021) has had a negative effect on SOF's readiness to conduct high-intensity conflict. Second, we will examine the effects that policy and plans have on SOF readiness. Third, we will look at how structural considerations and resourcing can impact functional readiness from a practical perspective. Fourth, we will highlight how readiness management can allow for SOF to be well rooted in capability or set functionally adrift. Finally, we will look at the role organizational culture plays within SOF readiness.

As this chapter continues, historical or hypothetical observations will be made, but they are meant to be illustrative rather than empirical. Also, as with the previous chapters, observations will remain generalist in nature to increase their applicability, as SOF units vary in complex and substantial ways from country to country and even within countries. With those two thoughts in mind, we begin by offering a problematic point of departure for SOF high-intensity readiness: the GWOT overspecialized SOF organizations to a significant degree. While counter-terrorism is applicably not a wartime activity for SOF, a brief examination of the past two decades is worthwhile before progressing.

Organizationally, the GWOT has had three significant effects on SOF. First, with a transnational enemy threatening all states, SOF partnerships entered period of unprecedented cooperation and geographic collaboration. Enabled by governments that required transregional strategies to combat

a transregional threat, organizationally diverse SOF entities migrated towards tactical homogeneity for the purpose of interoperability and mission success. As uniformity between national SOF units persisted in the sustained coalition campaigns of Iraq and Afghanistan, it also instilled a muddled concept of Western SOF employment that permeated many of the allies and partners. In other words, SOF units that were initially organized for high-intensity tasks and operations became increasingly counterterrorism-oriented because the low probability of interstate wars failed to generate interest by political leadership.³ This muddling of SOF's value proposition to both governments as well as national armed forces constitutes the first effect the GWOT had on SOF; it was more useful outside of high-intensity war than within it.⁴

Such universalism nevertheless proved successful at demonstrating SOF's utility, and Western SOF units – as well as other partnered SOF units alongside them – began to institutionalize this functionality in order to secure funding from their own departments and ministries. Effective justification for resourcing becomes a powerful incentive for organizational inertia, and while sustained military campaigns by occupying powers are nothing new, the primacy of SOF within the coalition military footprints of Iraq and Afghanistan was as unprecedented as were associated price tags.⁵ As a result, arguments for SOF resourcing became consistent and effective.⁶ Thus, the second and more nuanced organizational effect the GWOT had on SOF was a deeply increased acceptance of sustained military operations other than war. Seen this way, most SOF units had little incentive to prioritize wartime readiness when lavish funding and the promise of near-continuous force employment were secure.

The third effect of the GWOT on SOF was that through the institutionalization of a niche counter-terrorism role, SOF's relationship to the rest of the military also eroded. In a threatened national security environment, SOF serves as an interagency leader, but during periods of acute threats to national defence, SOF is best conceived as having a supporting role to the joint force.⁷ In this way, quibbling between terms like counter-terrorism or counter-insurgency actually had significant implications as the latter allowed a more concerted military response and greater subjugation of SOF to its conventional brethren. Not surprisingly, SOF's divestiture of its more traditional military role estranged many individual SOF units from

their parent joint forces, and unlike SOF's pivot to counter-terrorism, most conventional military leaders associated with the GWOT staunchly retained that their primary purpose was to fight and win their country's wars, not serve as a stability force. Preferring to see themselves as the force called upon when a mission was inappropriate or unsuitable for the conventional military, SOF adhered to counter-terrorism as an obvious choice, but it left conventional leaders unsure of whether or not SOF still had a role in large scale modern combat operations.⁸

Cumulatively, these three effects – fraternity between increasingly interoperable foreign SOF, an embrace of a non-war counter-terrorism role that secured funding, and isolation from conventional forces – restrained individual SOF organizations from sustaining high-intensity conflict readiness. Notably, it was political awareness of increasing threats from adversarial states that drove many countries to make military organizational changes *writ large*. Indeed, how a country frames policy objectives that could lead it to war has an immense impact on how militaries organize. How each country perceives the causes and cost of war also influences how they spend finite national resources. SOF's role in that perception of potential war drives their own organizational change in order to enable readiness in anticipation of potential employment. Reciprocally, the military's organizational actions will reinforce governmental leaders' perception of SOF's role in a major war.

For example, smaller nations living in the shadow of a larger, more powerful potential adversary conceptualize their SOF employment as defensive and reactionary, likely fighting on their own soil. Baltic nations clearly acknowledge the security threat that the Russian Federation poses to them, and, as a result, the contemporary Resistance Operating Concept provides a strategic basis for employment and organization.⁹ Alternatively, larger countries with a capability to project their militaries over greater distances not only maintain the strategic capacity to initiate warfare but also envision responding to allies when they come under attack. Here, SOF are organized to be expeditionary in nature, fighting on foreign soil for a variety of policy or national interest rationales, which can also, in turn, effect a SOF organization conceptually.¹⁰ The United Kingdom and the Commonwealth nations of Canada and Australia have no modern history of major land wars occurring inside their borders, and not surprisingly, their SOF evoke a commando-mystique

of operating in the far-away hinterlands of Afghanistan or the jungles of West Africa. Perhaps most interesting, certain smaller, less stable countries of the Global South – within which expeditionary SOF are often perceived as operating – wrestle with threats of violent warfare that originate internally, not from neighbouring or regional aggressors.¹¹ As a result, those countries' SOF are most commonly organized to be counterinsurgency-oriented, aligned with law enforcement, and often serve as republican guards, levied against coup attempts and protecting the regime in power. While not explicitly, these SOF elements are conceptually organized to be employed against their own people. Examples of these sorts of SOF are plentiful in both the Americas and Africa, in countries such as Colombia, Niger, Nigeria, and even Mexico.

Additionally, other strategic defence capabilities impact countries' probable operating scenarios and thus also shape conceptual SOF employment. The possession of nuclear weapons can limit an adversary's strategic options; however, the promise of future nuclear capabilities can also generate a strategic framework for national defence that makes some SOF concepts viable and other infeasible. For example, Iranian and North Korean nuclear programs are provocative towards the international rules-based order. In order to buy those programs time to mature, their SOF organizations contribute to deterrence by supporting military plans to attrite an invasion force and thus must be organized towards asymmetric defensive applications.¹² Alternatively, the mature nuclear capabilities of Britain and the United States generate their own deterrence against attack, making the concept of war at home unfathomable and predisposing their SOF organizations towards expeditionary employment options.

Offensive or defensive, direct or asymmetric, the expectation of SOF employment during periods of war significantly affects how military leaders organize their elements to do the tasks they anticipate, and the way they expect to execute them. These examples are not meant to be taxonomy, and certainly there are many Venn-hybrids to what is offered above. But the point is just that: tactical variance within conceptual wartime SOF employment is as diverse and nuanced as the politics that guide SOF staffing, training, and equipping. This is an extremely novel starting point despite contrary intuitions that look at tactical or adversarial capabilities.

As the role for SOF in war starts to become clearer, the real task of organizing SOF begins to take shape. Although the military is responsible for determining the training and readiness requirements of war capabilities, to include SOF, the burden of resource investment ultimately belongs to national leadership. What is more, SOF must objectively understand its assigned role inside of war plans to assess accurately how much of the military's finite resources they can expect during battle. Robust allocations of Intelligence, Surveillance, and Reconnaissance (ISR), medical coverage, and close air support cannot be assumed as means of removing risk to SOF units as those capabilities may otherwise be supporting echeloned manoeuvre or protecting rear areas and critical infrastructure. The military may expect SOF to either produce effects or generate lethality on its own that rival what otherwise could be accomplished with those same assets supporting larger units of action.

Indeed, those two expectations play nicely with this volume's notions of traditional, enduring roles and Contingency Response, respectively. As previous chapters demonstrate the potential variance in mission sets, it is unlikely that a single SOF unit can be organized to maintain readiness in all types for high-intensity conflicts. Two functional readiness factors serve as points of divergence to this end: force structure and infrastructure. Let's examine both in turn.

Force structure here refers to the authorized staffing of a single SOF unit of action. Like all military units, SOF units of action are typically standardized with codified force structure to justify personnel requirements to decision-makers, and, as those standardized units collect and multiply, they require overarching command and control structures, i.e. headquarters. However, the desired structure of the smallest SOF unit of action has massive tactical implications, including, but not limited to, lethality, survivability, and detectability, all of which relates back to anticipating the role that SOF will play in war. Illustratively, for a hyper-aggressive commando-esque force, a traditional infantry company-platoon structure may be perfectly sufficient. The former Selous Scouts of Rhodesia serve as a ready example, as does the more contemporary U.S. Ranger Regiment, with both organized as battalions.¹³ However, while larger units provide significant tactical mass, they require substantial assets for movement and manoeuvre, insertion and extraction, as well as greater support requirements. Alternatively, smaller

assault units allow for greater insertion speeds and tactical flexibility while only sacrificing degrees of lethality. U.S. Navy SEALs are organized in platoons, but internally break down into sections of eight soldiers for modular assaults on specific target sets. Indeed, most modern SOF assault elements are organized in this way: a modular troop/platoon or squadron/company structure that can be easily combined and made interoperable for larger, more complex objectives. These structures can be thought of as being more appropriate to Contingency Response applications.

Though units of thirty soldiers are still relatively discrete, even smaller teams are practical when direct engagement with the enemy is not the primary objective, and survivability over longer periods is expected. In situations where more clandestine or covert mission sets are expected, twelve-soldier or even small four-soldier SOF teams are more typical. The Canadian Special Operations Regiment, U.S. Special Forces, and even the Iranian Quds Force are all organized down to these smaller units of action.

Decisions about force structure are some of the most fundamental because in addition to affecting mission performance, the size of a SOF unit of action can multiply requirements or provide efficiencies. On the more obvious side of things, a smaller unit structure equates to less required materiel; a thirty-soldier platoon requires more stuff than an eight-soldier detachment. However, mission requirements may require force structure offsets that appear inefficient or redundant, especially with units intended for decentralized operations. For example, a U.S. Ranger company comprised of more than 120 soldiers is led by a single captain. Meanwhile, a U.S. Special Forces Company of fewer than eighty soldiers contains seven captains and a major. The latter comprises six smaller sub-units, additionally illustrating how different structures drive different training, development, and career advancement of those leaders as well as placing different strains on the military from which these leaders are recruited.

Force structure can also affect procurement, potentially establishing SOF-specific requirements. Consider a SOF maritime unit organized into ten-soldier teams. Now, let's say their navy updates their small craft fleet with boats that require six-person crews. SOF force structure challenges the organization's acceptance of this new craft, leaving them a choice of modifying the newly-purchased craft so that they can be piloted by five-person crews

(split-teams), adjusting their task organization during missions utilizing the newly-purchased craft, or procuring a SOF-specific craft. Each of these options will have effects of the SOF organization in terms of training, funding, and mission performance, and they may further lead to secondary material considerations like fuel compatibility, spare part stocks and supply chains, and interoperability with SOF weapon systems, to name a few.

This provides a nice segue into infrastructure considerations. Infrastructure is here meant to consider substructures that support the force structure. For the purposes of our examination, there are three aspects of infrastructure relative to our pursuit: exercise infrastructure, sustainment infrastructure, and human infrastructure. Each have subtle relationships to high-intensity conflict readiness. Take something as relatively simple as live ammunition ranges. These must ensure local populations are safe and that the range itself is maintained for prolonged usage, but they must also be relevant to SOF's envisioned employment. For example, modular shoot houses are very helpful to train SOF units for complex close-quarter combat environments, but they are not useful at all for long range marksmanship or larger unit live-fire manoeuvres. Further still, high-intensity conflict readiness requires ranges that integrate mobility platforms as well as training areas with significant distance to exercise communications equipment or indirect fire systems. SOF organizations may also need to consider cross-domain fires, which is to say air-to-ground or sea-to-shore fires, something that SOF has traditionally been called upon to control during periods of warfare. Range variance is only an example of exercise infrastructure considerations that also include dynamic insertion, environmental variances, cultural role players, and even survival training areas as distinct requirements for SOF high-intensity conflict readiness.

Second, SOF organizations require sustainment infrastructure to store, repair, and keep their weapons, vehicles, communications, and other critical materiel for high-intensity operations in good working order. More than just hard structures, sustainment infrastructure should include the specialized individuals that maintain SOF equipment as well as maintain the facilities themselves, as this is unlikely something that the SOF unit can do all on its own.¹⁴ Additionally, access to supply chains that can refresh stockpiled ammunition, spare parts, fuel, and all other manner of consumable goods is a major aspect of sustainment infrastructure, without which readiness levels

dwindle substantially. Transportation networks also play a key component as they serve a dual readiness purpose in both training but also in wartime logistical enablers for the SOF organization.

Finally, human infrastructure takes into account life support mechanisms for the SOF organization. There are many aspects to analyzing human infrastructural components, and their effects on the SOF organization can be direct as well as ancillary. For example, consider living space for the men and women who will make up the SOF organization. This might be barracks or other communal buildings, but private or commercial living quarters are more often common. In the case of the former, more close-knit relationships within younger ranks can be expected, but the latter is usually desired by older SOF personnel for the purposes of individual freedom and privacy. Unlike exercise and sustainment infrastructure that have direct relationships with the force structure, human infrastructure tends to impact organizational aspects of recruiting, *esprit de corps*, and culture, which will be discussed later in this chapter.

Other aspects of human infrastructure include, but are not limited to, access to and quality of health care, quality and access to commercial goods, ease of access to and price of food stuffs, proximity to off-duty entertainment and social aspects, and finally support to the family. Perhaps most important – most human infrastructure considerations are oriented towards the family, as their stability during periods of high-intensity conflict, when SOF units are forward employed, can have meaningful impacts on readiness and morale. Units may therefore have sharply increased obligations to support families when high-intensity operations occur.

Taken together, force structure and infrastructure provide the blueprint for the SOF organization, which frequently serves as a basis for resourcing and funding. If a SOF element is templated as a twelve-person detachment, then the organization requests the resources associated with what that detachment requires when at full strength. Logistical stores are further justified based upon consumption rates that intrinsically take complete force structure into account, such as exercise infrastructure and available sustainment infrastructure, as much as operational employment projections. Resourcing also drives human infrastructure insofar as it can. In some cases, quality of life support mechanisms under military control can be enhanced through

increased resourcing, while other times increased funding to the SOF service members allows for greater services to be purchased on the economy.

Structural considerations play an important part creating the functional readiness of SOF organizations in high-intensity conflict, but they are only part of the justification for resourcing. Remaining justifications rest on how SOF organizations utilize the structure that is put into place, or in other words, how SOF train and prepare themselves for combat. It is acknowledged that *how* SOF carries out its objectives is arguably as important as achieving the mission's objective itself, a notion that highlights the significance training plays to both mission achievement and SOF organization. But like all military training, SOF training is less about realizing the tasks at hand and more about managing the challenges associated with achieving them. Overcoming those challenges allows the SOF organization to achieve readiness and thus real capability in war.

For our macro-focus, we will now discuss three key general and managerial readiness challenges that configure and effectively prepare the SOF organization. While there certainly may be more, these three offer a foundation for what SOF organizations should consider when defining and preparing their force structure for a high-intensity wartime focus.

The first is appreciating that time is a resource, or in other words, time management matters. What this somewhat obvious reality means can be lost on even experienced military leaders, which can lead to SOF units being diversely tasked, and well-resourced for it, but ultimately less efficient overall. We call this phenomenon “the Bourne Principle,” coined after the fictional rogue agent Jason Bourne. In Robert Ludlum’s novels, Bourne speaks a dozen languages, expertly drives a vast array of foreign vehicles, and exhibits a diverse knowledge of contemporary tradecraft, medical skills, explosives, and hand-to-hand combat. Most notably, Bourne does most of this with almost zero skills sustainment training as he spends most of his time in hiding. Thus, the Bourne Principle is a nod to fictionalized excellence without time dedicated to maintain readiness. Point of fact, real-world SOF prowess is brought about through focused and professional training that exists within the confines of a calendar year already filled with competing requirements – administration, holidays, family and health obligations, and even necessary social outlets.

Assuming how much time is available for training is dangerous organizationally. Illustratively, the United States military starts with only 201 non-sequential training days per year after removing weekends, mandatory government holidays, and annual authorized leave. Three general considerations for time management show up in this broad illustration; let us take each of these separately to tease this concept out a bit further. First, every country has different holiday periods to take into account, and their sequencing, celebrations, and proximity can have impacts on building a military training calendar. Ramadan and Christmas, for example, occur at different times of the year, and depending on the country, can have different and major seasonal implications. Even subtle differences can affect time management. For example, Canadian Thanksgiving occurs in October and on a Monday, allowing for nearly two uninterrupted months of training before Christmas. Contrast that with the United States, which effectively loses a work week to the same holiday, disrupting that same two-month period.

Second, days lost to weekends may not seem worth analysis, but they are. Some SOF organizations may feel that training over weekends is acceptable or even admirable. Others, however, may dismiss the concept of weekend training except under specific and uncommon instances, which in turn limits the length of sustained training periods. In this same vein of analysis, informal organizational norms may also impact time allotments, like limiting training on Fridays or not remaining in the garrison area after a certain point in the afternoon. The point is that when reviewing the time available, the periods in the margins cannot be taken for granted either.

Third, individual leave often creates a two-fold challenge from a time management perspective. Within the general theme, leave periods naturally mean that personnel are not available for training; but, because individuals may choose when to take leave and because SOF units are often small, the loss of only a few key individuals can negatively impact the sort of training the team can accomplish. As a common alternative, SOF units may look at all personnel taking leave together, which results in large blocked-out periods, unsuitable for training.

Additionally, time management must consider the SOF organization's operational requirements. Regardless of this monograph's look at employment

during periods of high-intensity, SOF units are routinely employed along the spectrum of conflict, and while such deployments can provide a modicum of training value towards wartime readiness, it is ultimately unpredictable and thus should not be counted upon.¹⁵ Further, one must also consider the amount of time that the unit has to invest in preparations for force employment activities as well as the amount of time required for reconstitution after mission completion. Taken collectively, SOF organizations that function with high-operational tempos may find only a fraction of their time is available for training. Seen this way, time can often become the most finite resource of all with regards to fielding a capable and lethal SOF organization for high-intensity conflict.

Once the assessment of how much time is available has been finalized, the task of determining what do to with it can begin. Training management then becomes the second central challenge to SOF organizational readiness. After all, preparing for high-intensity conflict may require training in new skill sets, within the finite available training time. There are four conceptual training tiers that SOF organizations generally consider, each building upon the next in a fundamental way. The first tier is individual training. Unlike a conventional approach to military training, SOF typically invests in individual training to a greater degree because relatively smaller SOF units often require more diverse skillsets than conventional units, relating directly to the difficulty of their assigned missions. Individual training can be accomplished in one of two ways, the second of which comprises the second training tier. First, truly individual training involves sending an individual to “school,” or a training venue exterior from their organic SOF unit for prolonged periods. Losing members of a small team for extended periods of individual training is not unlike losing them for leave as it impacts their availability to the rest of the SOF unit. The purpose of this first tier is to provide individual SOF personnel an enhanced skillset or qualification that may not be required of every member of the SOF organization. For example, not everyone on the team needs to be a demolitions expert for a team to be considered capable of executing a sabotage mission; one or two demolitions experts are probably sufficient.

Individual-collective training is a similar but distinct second tier that allows for individual skill training – marksmanship for example – to be trained collectively in order to offer economies of scale through the maximization of

time allowances and resources. In fact, most conventional military skills can be trained in this manner, but individual-collective training should not be confused for collective training, which represents the third tier. Collective training includes practicing those tasks that require the entire SOF unit to accomplish. The distinction between individual-collective and collective is subtle but important. Take for example the requirement for a SOF unit to conduct a squad-sized ambush in a triple-canopy jungle. In an individual-collective training event, SOF personnel could go to the range and practice setting up anti-personnel mines or marksmanship from concealed positions, each engaging and refining individual skills. In this instance, if only half the team is available, then half team is still able to train on those tasks. However, a collective training event for that same requirement would focus on manoeuvring as a team in lush undergrowth, establishing the ambush line, and executing actions on the objective. Here, the entire team needs to be present to achieve maximum training value.

Finally, joint training becomes the critical fourth tier of training for a SOF organization preparing for high-intensity conflict. Unlike counter-terrorism or other national security environments where the SOF organization may be the lead or even sole military entity participating on behalf of their government, the conduct of high-intensity conflict is the responsibility of the military as a whole, meaning that – as the previous chapters emphasize – the SOF organization will be supporting the conventional force. Because of this, the SOF organization must consider training events where they can train alongside conventional units and under joint headquarters in the conduct of wartime tasks, both for the purposes of readiness and inter-operability, but also so that the conventional force commander will understand the capabilities of the supporting SOF organization.¹⁶ Scheduling this type of training will place further demands on an already-stressed training calendar.

What this ultimately means for training management is balancing individual, individual-collective, collective, and joint-collective training within the allocated time in order to achieve adequate readiness for assigned tasks. While this seems straightforward, the greater SOF organization may need to objectively check all of its desired capabilities against the Bourne Principle to determine prioritization. Indeed, training management must also consider

the complete litany of tasks assigned to the SOF organization, including those applicable in periods of low-intensity as well as high-intensity conflicts.

In addition to time management and training management, the SOF organization must lastly consider talent management as the third managerial challenge associated with gaining readiness for high-intensity conflict. Talent management can be looked at through a human resourcing lens as well as a materiel and technology lens. Beginning with the former, the SOF organization's readiness can be positively or negatively affected by either the acknowledgement or ignorance of the full life cycle of its personnel. Enhancements relative to readiness can be most critically impacted at three points – recruitment, entry-level training, and unit composition. First, the SOF organization's messaging towards potential recruits is important as it relates to its role within high-intensity conflict. But beyond the recruiting campaign, the SOF organization's designated recruitment pool could be just as impactful to readiness. Personnel can be recruited either from within the military or from off-the-street. The benefits of recruiting personnel who are already in the military are plentiful – they already have military experience, possess basic soldiering skills, and understand how to interact with conventional forces. Each of these contributes to readiness for the SOF organization without significant investment. However, recruiting from the civilian population allows the SOF organization to recruit for specific skills that may be finite within the ranks of conventional forces. Language capabilities, cyber training, and even elite physical fitness levels are more plentiful in the civilian sector. Moreover, developing these skills involves sizable investments by the SOF organization to achieve functionality, both within the rank-and-file as well as the creation of an instructor cadre. The question the SOF organization must ask itself is what skills does it want to be responsible for in training its recruits and what skills does it want to recruit for? The answers may have implications for operator selection processes.

This comes to the second point of entry-level training. Whether recruiting from in-service or out-of-service, virtually all SOF organizations place their personnel through an assessment, selection, and training period, and the variance between these can differ significantly in length and scope. Most commonly, these are used to train new personnel on the SOF organization's core mission set as it is prescribed in policy or doctrine, but it is critical that the SOF organization balances the readiness achieved by entry-level

training with current force employment requirements. For example, if entry-level training for a given SOF organization focuses on establishing baseline readiness for high-intensity conflict, but personnel are routinely deployed to low-intensity environments upon graduation, then not only will the achieved readiness be poorly utilized, but it may also cause some to question whether the entry-level curriculum was correct at all. SOF organizations faced with this difficult question could see real reductions in high-intensity conflict readiness if new personnel do not perceive those tasks associated with high-intensity conflict to be worthy of entry-level training. Of course, the alternative – limiting training for major operations in operator-qualification courses – would also adversely affect readiness.

When assessing entry-level training, SOF units may also need to consider how they would generate personnel reserves, given the lethality of high-intensity warfare. Inevitably-high casualty rates may produce elevated reinforcement requirements to keep deployed teams up to strength. At the same time, other critical low-intensity missions or a mandate to provide rapid-response forces may remain during a high-intensity war. Generating the necessary reserves of personnel after they are needed to achieve the mission violates one of the SOF truths, yet wartime requirements are still wartime requirements.¹⁷ For the SOF organization, this will mean re-examining decisions and standards associated with recruitment and entry-level training, which could prove a thorny challenge. Where the SOF organization encounters difficulties in recruiting, selecting, and training enough people, associated decisions and standards may want to be examined proactively, before a high-intensity conflict breaks out.

As a third and final personnel life cycle point, the composition of SOF units can also generate increased readiness for the organization. Composition is distinct from force structure considerations in that the SOF organization must determine what skills need to reside in the SOF unit, not simply its size. Usually this has a greater impact on smaller SOF units that need to maintain a minimum force structure in accordance with their mission set. For example, a deep reconnaissance team cannot afford to bring extra personnel, such as medical and communication support, so they must train themselves to conduct those tasks in addition to things like sniper training, calling for indirect fire support, and infiltration techniques. The SOF organization may determine that each member of the unit must be both

medic and communications trained, or they may decide that only some members of each team need those skills. Not only do these decisions impact both training and time management as previously noted, but they also might impact recruiting. Requiring each SOF team to have two proficient linguists would take years of individual training to achieve; would it not make more sense to recruit specifically for that skill and train that individual to shoot, move, and communicate?

Complex composition decisions can have impacts on force structure and training management. Alternatively, maintaining a simpler composition can reduce those same challenges, simplifying readiness management and opening the door for increased opportunities with the second aspect of talent management: technology. Here technology refers to materiel advancements that the SOF organization requires to be operationally capable in a high-intensity war characterized, as emphasized in the introduction, by speed and tempo, interconnected information systems, an informatized environment that makes it difficult for friendly forces to evade enemy surveillance, and pronounced lethality. Technology may affect training similarly to assessments of available time since even baseline equipment like radios and rifles require allowances for proper training in order to achieve appropriate readiness levels. Seen this way, technology management is something of a dual-edged challenge for the SOF organization; as procurements are made to enhance survivability, lethality, and speed during times of high-intensity war, they come with training requirements in order to be realized. In other words, buying a new attack helicopter does not mean that anyone knows how to fly it, fire it, fuel it, or fix it.

Despite best efforts to procure versatile technologies, all materiel universally has limitations. This creates a second-order training management challenge. On the one hand, the SOF organization can look for ways to offset these limitations with the technologies they have. Bridging solutions or enhancements can be found through scheduled training, which is ultimately an indicator of readiness. Alternatively, additional technologies can be procured by the SOF organization to more optimally decrease limitations and enhance readiness through a materiel solution. However, new technologies can have an inverse drag on both time and training as new equipment generates new management burdens. Beyond baseline technologies, emerging technologies, such as those described in the previous chapter, may in

some cases add to training burdens. In other cases, emerging technologies may be focused not only on reducing certain training requirements but, in some cases, removing them altogether.

It is important to note that SOF organizations invest in technological solutions in order to enhance readiness in low-intensity conflicts too, and sometimes those investments are not evenly applicable in high-intensity environments. For example, many of the up-armoured vehicles developed for increasing survivability of SOF coalition units in Iraq and Afghanistan against roadside bombs have very limited capability during high-intensity war due to their large signature on the battlefield and low levels of off-road mobility. As time has gone on, those vehicles have had continued utility for some SOF organizations, while for others they merely take up space in the motor pool.¹⁸ This difference highlights a final point on talent management: divestiture. Referencing back to the Bourne Principle, SOF organizations need to be assessing continuously the totality of their required mission sets as well as the technology that supports them, to determine inefficiencies and redundancies.

For instance, let's say a SOF organization has three primary mission sets, and because it wants to provide enhanced equipment for its teams, it decides to procure three different vehicles, each providing the best tactical advantage for a particular mission set. However, the SOF organization must ask if the materiel's advantage, as well as its fiscal cost, out-weighs the readiness that the tactical SOF teams could maintain if they had only one of those vehicles but were able to spend three times the amount of time training on it. Of course, this is just one hypothetical situation, but it illustrates that technology does not guarantee increased readiness. Moreover, divestiture analysis as a principle is not limited to technologies. SOF organizations should periodically check their functional readiness structure and readiness management decisions in order to determine optimization levels. Over-arching to all this, and of particular relevance to preparing for high-intensity conflict, the SOF organization may also want to assess if its mission sets are still envisioned correctly, both internally as well as within the parent military or political body.

Such organizational introspection can often reveal mismatches in functional readiness and readiness management. Periodic reviews are not a bad thing,

per se, as there is always a natural friction in military organizations between what is planned and what is occurring. In fact, without episodic internal assessments too much divergence can lead to real consequences for readiness. Perhaps counterintuitively, this divergence does not usually occur simply between high-intensity and low-intensity conflict readiness but when too great of a divergence exists between the related functional readiness and readiness management of each. SOF organizations will want to manage low-intensity force employment in a focused manner to ensure that high-intensity readiness is being reinforced (at best) and not detracted (at worst) when SOF units are deployed.¹⁹ To put it another way, if your go-to-war role is covert sabotage behind enemy lines then you cannot continuously deploy as a quick reaction force to peacekeeping missions and expect to stay at high readiness levels for either.

In addition to the SOF organizational considerations that we have already discussed, imbalances between readiness and force employment can impact organizational culture, specifically identity, which will serve as the final readiness consideration in this chapter. Identity is often very important to a SOF organization, and reciprocally the SOF organization tends to see the maintenance of an organizational culture as the best method to inculcate identity. However, identity is an individual aspect of the organization, wherein divergence in readiness and force employment considerations can lead to confusion for SOF personnel. Referencing the GWOT's effects on high-intensity conflict readiness from earlier in this chapter, many Western SOF organizations noted an "identity crisis" within their ranks, resulting in ethical lapses, failures of leadership, and operational catastrophes.²⁰ While different commanders assessed different reasons for this, the common theme was rifts, inconsistencies, and a lack of adherence to the outlined organizational culture. Regardless, imbalances between readiness and force employment can significantly undermine organizational culture when individual members perceive the SOF organization to be acting inconsistently with its prescribed values and with what it selects and trains people to do. More specifically, individuals equate their membership in the SOF organization with their ability to execute its core mission set – assumptively a role in high-intensity conflict – making their readiness a critical factor in their personal identity. When the organization is not perceived to respect or honour individual members' commitment to high-intensity conflict readiness, then those same members may develop grievances of mistrust,

distaste towards careerism, and betrayal. The derivatives of these grievances manifest in an SOF organization sub-culture of isolation, frustrations, and defensiveness, respectively. Increased negativity towards the status quo and desperation to effect organizational change emerge, which sets a socio-psychological glass ceiling on readiness potential.

In response, the SOF organization may stress its profession of arms, core ethos, or organizational standards as methods of sustaining its culture to new members as well as external audiences. While this can bulwark the SOF organization to a degree, it can also backfire. Most SOF organizations call upon their members to be “adaptive,” and interpretively, this attribute may be seen to justify imbalances between readiness and force employment.²¹ Also, other common watchwords usually include “trustworthiness,” “integrity,” and a heightened sense of “duty.” These terms reinforce some members’ expectations of the SOF organization, and its leaders, to hold themselves to the same values in determining force employment priorities. Displaying personal courage and upholding high standards are other desired SOF organizational attributes, which have the dual distinction of bolstering readiness potential while simultaneously charging members to challenge internal inconsistencies through counter-action.

Made worse, some members may actually find greater identity through divergent force employment in low-intensity conflict, believing that their experiences, personal readiness investments towards that alternative mission set, and the current actions of the SOF organization justify and dictate a realignment of primary mission sets. This can lead to multiple identity groups within a single SOF organization: those who want to return to a previous set of organizational readiness considerations; those who adhere to current considerations; and those who desire some new configuration. Each of these groups will have their own informal advocates who debate and passively challenge the current leadership’s decisions that are perceived to be unaligned with their own group’s feelings of identity, culture, and organizational direction. As it is unlikely that all sub-groups will favour a high-intensity conflict readiness model, the intra-organizational friction becomes an outlet for determination and energy that would otherwise be spent on developing readiness.

To avoid unhealthy levels of organizational friction, SOF organizations must remain beholden to their own stated cultures, which may include prioritizing readiness over short-term utility. Recalling from earlier that organizational action will reinforce governmental leaders' perception of what SOF's role is, the goal of maintaining and communicating aligned, non-divergent force employment options within low-intensity conflict will help increase levels of readiness potential. This means articulating which of those low-intensity missions are also well-suited to the SOF organization's high-intensity missions as well as those that are inappropriate. The worst thing the SOF organization can do in this regard is perceive that anything the conventional force cannot do, or cannot do well, is a SOF mission.

In conclusion, it is worth acknowledging that healthy and consistent concerns over SOF organizational direction are not only normal but required in order to maintain a keen and contemporary level of high-intensity conflict readiness. Modifications to force structure and composition impact training management, which then can impact talent management considerations and potential capabilities divestment. These interactions are dynamic and continuous, and neither functional readiness, readiness management, nor organizational culture considerations dictate a position of primacy; all are equally important to the development and sustainment of real readiness for the SOF organization. Rather, it is readiness itself – readiness towards high-intensity conflict – that serves most perfectly as the foundational element for decisions, direction, and excellence within the SOF organization.

CONCLUSION

NEVER SAY NEVER: FINAL THOUGHTS ON THE IMPLICATIONS FOR SOF IN HIGH-INTENSITY WARFARE

COLONEL (RETIRED) BERND HORN, PhD

The idea of the onset of a high-intensity war is unfathomable to most. Reasons to discount the incomprehensible march to war are normally anchored on a number of factors. First, a “hot” war would severely impact the stability and prosperity of the interconnected world that globalization has enhanced.¹ For that reason, the most current iteration of strategic competition, namely the struggle for access and influence to further national political objectives and disrupt, deny and defeat those of adversaries, focuses mainly on activities below the threshold of armed conflict (e.g. cyber and informational attacks, leveraging economic power, sabotage, subversion, agitation, use of proxy forces).² In essence, the argument posits that no-one benefits from a conventional war, particularly against a major power such as the U.S.

Another argument under-cutting the credence of the possibility of a high-intensity war is based on the belief that the accessibility and proliferation of technology make the prospect of conflict so devastating that no state would risk engaging in all-out war. Quite simply, an increasing number of nations with substantial nuclear arsenals, as well as the global propagation of stand-off precision missile systems and platforms, including highly manoeuvrable cruise missiles, as well as hypersonic weaponry (weapons that travel at five times the speed of sound) and glide vehicles, matched with networked sensors that are capable of delivering large payloads of munitions at increased ranges so that targets can be engaged and destroyed almost anywhere with accuracy within a short period of discovery and decision-making, make a high-intensity conflict a losing proposition for all belligerents.

In short, the future battlefield will be characterized by increased lethality, enhanced speed and tempo of operations, amplified informatization empowered through AI, increased complexity, and the loss of traditional Western

CONCLUSION

supremacy in all domains. Quite simply, conflict between belligerents using modern weaponry will be disturbingly swift and horrifically destructive.

In essence, the formidable capabilities of current and emerging technology and munitions makes the fielding of large conventional armies and their platforms laden with risk. Added to this daunting array of threats is a myriad of additional perils. Jamming of communications, the targeting of satellites, electronic warfare and cyber-attacks that target networks and the vulnerable software programs that seemingly run the entirety of today's society and militaries will only increase risk and consequence of a high-intensity war. The increasing development and deployment of autonomous systems only adds to this complexity.³ As such, for most, the prospect of a high-intensity war is highly unlikely, if not negligible.

However, never say never. Through design or miscalculation, the occurrence of a major conflict between peer, near-peer and/or regional powers can never be discounted. History is replete with instances of unexpected attack. Examples include: the German invasion of the Soviet Union on 22 June 1941; the North Korean assault on its southern neighbour on 25 June 1950 and the Chinese engagement later in October; the Egyptian crossing of the Suez Canal and assault on Israeli forces in the Occupied Sinai Peninsula on 6 October 1973; the seizure of the British Falkland Islands by Argentina on 2 April 1982; and the invasion of Kuwait by Iraq on 2 August 1990 leading to the First Gulf War. The 24 February 2022 Russian invasion of Ukraine, as well as Chinese provocations across the Taiwan Strait, provide recent disturbing examples of how through design or miscalculation a high-intensity conflict could erupt.⁴

The point is, discounting a possible eventuality leads to punishing consequences. It is always important to anticipate possible events, which allows for quicker adaptation and change should the inconceivable occur. Having considered, brain-stormed, war-gamed possible scenarios, organizations and institutions have, at a minimum, a conceptual idea of what the challenges, as well as possible roles, tasks and requirements will be.

With regards to SOF and high-intensity war, this contemplation and planning is extremely important. After all, for the SOF community the previous two decades have been focused primarily on counter-terrorism (CT) and

CONCLUSION

counter-insurgency (COIN). Importantly, these activities were conducted with virtual overmatch in every domain. SOF forces had freedom of manoeuvre on the ground, sea and air. They had technological and informational overmatch, as well as supremacy in intelligence gathering and firepower. In short, they held advantage in virtually every aspect of the conflicts in which they were engaged. This prolonged advantage and sense of superiority tends to build strong habits and can blind organizations to systemic weaknesses and/or shortfalls. It builds a false sense of security, if not capability, particularly for engagement in operations that have not been conducted for decades against peer or technologically advanced and equipped adversaries.

It is for this reason, that as unlikely as many feel the prospect of a “hot” war between major international actors may be, SOF must expend some intellectual effort in understanding high-intensity conflict and the implications for SOF, particularly the challenges and potential requirements, as well as determining possible roles and tasks, so that it can best provide employment options to senior political and military decision-makers.

The role of SOF in a high-intensity war is not without precedent. Although every conflict has its own unique characteristics, or in Clausewitzian terms “grammar,” three examples from contemporary military history provide some insight into SOF roles and tasks during high-intensity war (albeit not between two great powers). The first example is the 1982 Falklands War between Great Britain and Argentina over the Falkland Islands in the South Atlantic. Throughout this relatively short conflict Argentinian special forces, as well as both the British Special Air Service and the Special Boat Service conducted operations.

The Argentinians utilized their special forces (SF) to initiate the assault and capture of the islands with attacks on Moody Brook Barracks and Government House. They also used their SF for aggressive patrolling, as well as attacks on designated highly-important objectives throughout the conflict.

Similarly, the British Task Force Commander utilized the 22 Special Air Service (SAS) Regiment, as well as the Special Boat Service (SBS) for a myriad of tasks during the conflict.

CONCLUSION

During the Falklands campaign British SOF conducted:

- Strategic and tactical intelligence gathering (by conducting active fighting patrols and covert observation posts);
- Close target reconnaissance of identified facilities and targets;
- Direct Action assaults against static targets and targets of opportunity;
- Diversionary raids to confuse, delay or inhibit enemy movement;
- Domination of no-man's-land between enemy positions;
- Sabotage or destruction of critical facilities (active airfields, communication lines, fuel storage areas, command and control locations); and
- Direct forward air control of fighter aircraft and naval gunfire support against identified targets.⁵

The first mission the SAS undertook was Operation Paraquat, the recapture of South Georgia Island. In atrocious weather conditions "D" Squadron (Sqn), as part of a small subordinate Task Force that included a company of Royal Marines and SBS personnel, sailed south to retake the British possession. South Georgia itself was of little military consequence, however; the task itself was of great strategic importance. After a number of British ships were sunk by Argentinian aircraft, the British Government needed a quick victory. Therefore, South Georgia became an important political requirement. After a number of set-backs, elements of "D" Sqn conducted a hasty attack and captured the Argentinian garrison and reclaimed the island providing the British Prime Minister with the immediate "win" she required.

British SOF were also instrumental in establishing observation posts (OPs) to monitor and conduct surveillance on Argentinian movements of troops, aircraft and equipment in the Falkland Islands. The information they provided was quickly transformed into critical intelligence that assisted the Task Force Commander's battle plans. In the same vein, aggressive patrolling by both the SAS and SBS fulfilled a similar function.⁶

In fact, SOF reconnaissance and observation brought to light the potential danger of an Argentinian airfield on Pebble Island. This air base essentially provided the Argentinian forces the ability to strike naval, land and air

CONCLUSION

targets (such as Sea Kings) in the San Carlos operational area within minutes from taking off from their airfield. This advanced base ensured British forces operating in the area would have very little warning. As a result, the SAS launched a raid, which harkened back to SAS airfield raids in North Africa during the Second World War. The daring raid destroyed all eleven enemy aircraft, as well as destroying the runway and a fuel depot.⁷

Additionally, British SAS and SBS elements conducted beach reconnaissance, supported the main Task Force landings at San Carlos, conducted diversionary attacks at Goose Green and Wireless Ridge to support 2 Parachute Regiment, and led the initial assault on the strategic heights of Mount Kent.

Another task that was initially intended for British SOF was Operation Mikado, the plan for SAS operators to destroy Argentinian Étendard strike fighters and their Exocet missiles on their mainland airbase at Rio Grande, Tierra del Fuego. The British Director Special Forces, General Sir Peter De La Billiere, was a staunch protagonist for the mission. He envisioned landing two British C-130 Hercules transport aircraft loaded with approximately 60 SAS operators and their vehicles directly onto the tarmac at Rio Grande airbase. The SAS would then disgorge from the aircraft, similar to the Israeli mission at Entebbe years earlier, and destroy the Étendard fighters, the remaining Exocet missiles, as well as the pilots in their quarters.⁸ The aircraft and SAS "B" Squadron deployed to the staging base at Ascension Island, but the British Prime Minister did not authorize the raid in the end.⁹ In all, British SOF played an instrumental role in the Falklands campaign.

SOF was once again employed in a high-intensity conflict between 2 August 1990 and 28 February 1991, during the First Gulf War. Coalition SOF conducted:

- Special reconnaissance;
- Foreign Internal Defence (i.e. training allies and partner forces);
- Liaison/Joint Terminal Attack Controller (JTAC) activities;
- Direct Action;
- Diversionary activities;
- Visit, Board, Search and Seizure (VBSS) in the Persian Gulf; and
- Unconventional Warfare.

CONCLUSION

Special reconnaissance, particularly OPs along Saudi-Kuwaiti border to monitor Iraqi movements, was the first SOF task that was undertaken. SOF also penetrated into Iraq and they ensured the route for the “left flanking” of the Iraqi positions was suitable to support the movement of Abrams heavy tanks.

Equally important, SOF trained Coalition partners, particularly non-NATO members, to ensure they could operate in a coalition setting. This task was especially important to hold together the multi-national partnership. As such, SOF was also embedded in coalition units to serve as liaisons, primarily to coordinate close-air-support.

In addition, SOF conducted Direct Action. As such, they seized oil platforms, destroyed Iraqi fibre-optic communication cables, blew up microwave relay towers and communication bunkers and attacked enemy vehicles, “painted” enemy targets for close-air-support, recaptured the British embassy in Kuwait City and in what is probably their most well-known public mission, hunted SCUD missile Transporter-Erector-Launchers (TEL), a strategically essential task that was critical to maintaining the Coalition by keeping Israel from retaliating against Saddam Hussein’s continued SCUD missile attacks on Israeli soil.¹⁰ SOF were given the difficult task of locating and destroying the mobile launchers.¹¹

SOF also conducted diversionary raids on the coast to deceive the Iraqis into thinking that a large-scale amphibious operation was looming. Additionally, U.S. SEALs conducted VBSS operations in the Persian Gulf, often raiding suspicious ships. Finally, SOF teams were also assigned to work with Kuwaiti resistance, rescue key civilians trapped behind enemy lines and capture Iraqi military personnel.¹²

The final example of SOF employment in high-intensity conflict is the Second Gulf War, namely the invasion of Iraq on 19 March 2003. During this conflict Coalition SOF conducted:

- Special Reconnaissance;
- Direct Action;
- JTAC activities;
- Support to Conventional Forces;

CONCLUSION

- Sensitive Site Exploitation (SSE);
- Hostage Rescue Operations; and
- Unconventional Warfare.

Similar to the previous two examples, SOF were instrumental in conducting special reconnaissance to identify Iraqi positions and movements, particularly to monitor the Karbala Gap. Additionally, Direct Action was a key activity for SOF. At the onset of hostilities they eliminated Iraqi border observation posts and once again, hunted down SCUD TEL launchers in the Western desert. Furthermore, SOF seized the Haditha Dam complex, conducted ambushes on the highway to Tikrit to tie up Iraqi forces, “painted” enemy targets and vehicles for close-air-support and they captured high value targets (HVTs) attempting to flee to Syria. SOF also eliminated Uday and Qusay Hussein, captured their father Saddam Hussein and killed the al-Qaeda in Iraq (AQI) leader, Abu Musab al Zarqawi. They also captured or killed over 100 AQI members including at least eight high value targets. In addition, Coalition SOF seized national oil production facilities, as well as capturing key infrastructure and transport nodes. A Naval Task Group also seized Umm Qasr, Iraq’s only deep-water port, the oil production facilities of the Al Faw Peninsula and two off shore platforms that the pipelines fed.¹³

Support to conventional forces was also a significant undertaking. SOF conducted screening tasks in support of conventional forces, captured strategic sites to allow follow-on conventional forces to deploy, supported the seizure of Rumaylah oilfields and worked with local Sheikhs and their militiamen to capture a key town infrastructure, as well as to establish a police service and restore 80 percent of the town’s electricity within a fortnight. They also reopened schools and hospitals all in support of conventional force thrusts in the area.

SOF were also instrumental in conducting a number of high priority SSEs, particularly in suspected Weapons of Mass Destruction (WMD) sites. Furthermore, Coalition SOF also successfully conducted hostage rescue operations, saving Private Jessica Lynch, three Italian contractors, as well as three non-governmental organization (NGO) workers. Finally, SOF worked with local Kurdish Peshmerga forces to draw Iraqi forces away from reinforcing Baghdad, as well as capturing strategic sites to allow follow-on conventional forces to deploy.¹⁴

CONCLUSION

In all, the missions conducted by SOF in these three conflicts were in essence largely the same tasks as SOF performed in the Second World War (e.g. raids, reconnaissance, deception, unconventional warfare). Granted the examples reflect a great power (i.e. U.S. and Britain) against regional powers and not peer or near-peer adversaries. Nonetheless, the belligerents in all three examples had access to state-of-the-art weaponry and technology. As such, the conflicts in question provide insight into potential SOF employment and tasks.

POTENTIAL TASKS

Despite the dated examples, and although circumstances have changed (i.e. the availability and proliferation of advanced munitions, sensors, weapon systems, as well as Intelligence, Surveillance, Reconnaissance (ISR) capabilities), most, if not all, the enduring SOF tasks remain relevant. If SOF were to become involved in a contemporary or future high-intensity war between peer, near-peer or regional power adversaries they could expect to undertake the following potential tasks:

1. Special Reconnaissance;
2. Advanced Force Operations (AFO);
3. Preparation and Shaping of the Operational Environment;
4. Theatre Break-in;
5. Direct Action;
6. Target Designation;
7. Battle Damage Assessment;
8. Hard Target Defeat;
9. Contingency Operations
10. Deception/Diversion/Disruption;
11. Sabotage;
12. Irregular Warfare (i.e. Unconventional Warfare, support to insurgency, CT, COIN);¹⁵
13. Second Front/Horizontal Escalation;

CONCLUSION

14. Counter-SOF;
15. Counter-Shipping;
16. Chemical, Biological, Radiological, Nuclear (CBRN) SSE;
17. Role in Phase IV (stabilization);
18. Psychological Operations (Psyops); and
19. Economy of Effort operations.

SOF through its high readiness, rapid-deployability, superlatively trained and educated personnel and integral proficiencies, techniques and methods of employment make it an ideal partner to assist the Joint Force fight. Its ability to conduct special reconnaissance, as well as AFO, in hostile, denied, or highly sensitive environments allow it to “sense” (i.e. determine changes within a theatre, confirm events, specifically threats) and “signal” (i.e. provide ground truth and warning) to governments and military commanders.¹⁶ In addition, they are adept at shaping and preparing, as well as breaking-in to theatres in support of the Joint Force. Although ISR assets are irreplaceable, clever camouflage and deception of armaments and weapon systems by adversaries, as well as physical destruction of, or electronic interference with, friendly ISR assets can create a veil of darkness. SOF can “illuminate” these gaps and provide decision-makers and the Joint Force with the necessary information for planning, deployment and actual operations.

Additionally, SOF is also highly-capable of conducting Direct Action against critical infrastructure, command and control nodes, weapon systems (e.g. A2AD, nuclear weapon launchers) and lines-of-communication. Specifically, SOF becomes an essential enabler for the Joint Force by eliminating hard targets (e.g. fixed defences, missile batteries, nuclear launchers, headquarters), as well as disrupting enemy lines of communication through either Direct Action or through target designation by JTACs.¹⁷ Equally important, SOF can conduct battle damage assessment (BDA) to determine effectiveness of friendly strikes to ensure the necessary results have been achieved.

Importantly, SOF can also conduct contingency operations that require a rapid response, precision and high reliability of success. SOF’s characteristics position it to be highly responsive to situations that occur that were unforeseen (and no contingency plans in place to address) or that create

CONCLUSION

such a threat or crisis that immediate action is required for either existential, operational or political/morale reasons.

SOF operations can also assist the Joint Force through deception, diversion and/or disruption operations. By staging feints, holding attacks, diversionary strikes or harassment in adversary rear areas or lines-of-communication, SOF can tie down enemy forces, divert their attention away from critical areas and disrupt their intended operations. Moreover, sabotage of key infrastructure, as well as disruption of their lines-of-communication can curtail enemy capability and tie down enemy forces for vital point/rear area security.

Yet another important task SOF can conduct in a high-intensity conflict is irregular warfare, defined as a “violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s).”¹⁸ Irregular warfare is an important tool for friendly forces. After all, irregular warfare concentrates on indirect and asymmetric approaches to avoid the military strengths of an adversary. From a U.S. doctrinal perspective irregular warfare includes the specific missions of unconventional warfare (UW), stabilization, foreign internal defense (FID), CT and COIN.¹⁹

SOF conducting irregular warfare acts as both a force enabler, as well as an economy of effort capability. Leading UW operations (i.e. working with host-nation forces behind enemy lines) SOF can tie down adversary troops needed for rear-area security, disrupt enemy operations and activities, destroy adversary infrastructure, equipment and their war effort in general.²⁰ UW operations can also be used to create “second fronts” or horizontal escalation by inserting small teams, who, working with resistance cells/guerrilla groups, can foment new theatres of operations to which adversaries must devote resources.

Irregular warfare operations also represent a critical ongoing, enduring task for SOF. A high-intensity war will not create a pause in undertakings for the myriad of global terrorist organizations that exist. In fact, many would probably increase their attacks believing major powers will be consumed by the larger conflict. As such, FID, CT and COIN all become critical activities to assist allies, friendly or at-risk nations deal with internal security issues that could evolve into larger security issues for not only single states, but

CONCLUSION

allies and partners as well. For instance, as the current tranche of strategic competition smolders, insurgency and terrorism remain rampant in Africa and the Middle East. SOF conducting irregular warfare operations can have both an offensive and defensive function, as well as an economy-of-effort effect by keeping these threats in check.

Undeniably, irregular warfare is a formidable means of striking at an adversary. It is one methodology that both the Chinese and Russians wield authoritatively. As such, “counter-SOF” becomes another important task. Ensuring enemy SOF are unable to conduct UW behind friendly lines, interfere with lines-of-communication, and/or interfere with command and control are extremely essential. Additionally, denying enemy SOF the freedom of movement to conduct special reconnaissance, AFO, break-in operations, direct action and/or targeting becomes imperative. Although conventional forces can certainly undertake rear area security tasks and vital point security, SOF is best suited to understand tactics, techniques and procedures (TTPs) that their counter-parts will employ. As such, counter-SOF employment, particularly for high-value infrastructure, events/operations and/or geographically vital areas, etc., will be necessary.²¹

Additionally, SOF can undertake a host of other tasks. Counter-shipping to interfere with adversary maritime operations or supply can have a seriously detrimental impact on the enemy’s war effort. For nations that embed PSYOPs with their SOF forces, this task can have serious consequences on targeted adversary forces and/or populations, as well as on affected populations in theatres of operations and international targeted audiences that may be neutral or wavering on support.

SOF can also play a valuable role in conducting SSE on high value objectives, particularly headquarters, CBRN facilities (e.g. storage sites, laboratories, launch vehicles) and communication hubs. Finally, SOF can also contribute to post-hostility Phase IV Stabilization operations. Working with friendly or at-risk states, SOF can employ FID to assist with the reconstruction and/or establishment of the necessary security infrastructure to ensure a stable and secure environment for reconstruction and development.

Although the enduring nature of these SOF tasks is not surprising, the difference lays in the daunting challenges that the proliferation and access to

CONCLUSION

modern precision munitions and technology available to adversaries pose to SOF operations.

CHALLENGES

Undoubtedly, there would be innumerable challenges to SOF operations in a high-intensity conflict. As mentioned earlier, the proliferation of accessible, relatively cheap, advanced satellite, informational, sensor and weapon technology has levelled the playing field between belligerents in many aspects. Remaining hidden and simply moving has become extremely difficult. Precision, range and lethality of munitions, as well as the efficacy of sensors and radars, has become frighteningly effective. The decades-long advantage of technological, informational and firepower overmatch is no longer a given. Neither is freedom of manoeuvre on land, sea or air. As such, SOF must examine carefully the impediments it will face and the means to overcome those obstacles.

In short, some of the challenges that SOF will encounter include:

1. Command, Control, Communications and Computers (C4);
2. AI/machine learning;
3. Speed/tempo;
4. Capacity;
5. Cooperation with the Joint Force;
6. Self-image/failure to evolve;
7. Lethality/Advanced technology;
8. Direct Energy Weapons;
9. A2AD (theatre entry/manoeuvre);
10. Freedom of manoeuvre/mobility;
11. Aerospace Control;
12. Concealment (i.e. sensors, CCTV, cell phones);
13. Risk Acceptance;
14. CBRN battlespace;

CONCLUSION

15. Supporting fires;
16. Adversary SOF;
17. Influence Activities/Influence local populations;
18. Domestic support/trust; and
19. Mental health.

A major concern will be the nexus of C4, AI machine learning and speed/tempo of operations. The use of AI will press tempo to limits not yet experienced in conflict. Decision-cycles will be collapsed and decision-making pressed to extremes as belligerents try to make sense of what is occurring and what capabilities still exist. Jamming, cyber-attacks as well as the destruction of satellites and relay stations will stress communications, endanger the ability to utilize supporting fires, as well as the capacity to control operations at all once they have crossed the “start line.” The recent successful test of a Russian ground launched missile that destroyed a defunct space satellite should raise alarm since this advancement jeopardizes the ability to potentially use satellites that enable much of society and the military.²²

Capacity will also pose issues for SOF in high-intensity warfare. With the myriad of potential tasks how will SOF missions be prioritized? There just simply isn't enough SOF capacity to deal with all the required missions.²³ Once casualties are factored in the issue becomes even more difficult. As such, a clear prioritization of tasks, as well as a concerted effort to educate commanders to fully understand the best utilization of SOF to avoid needless casualties must be in place. In fact, this requirement raises the issue of cooperation with the Joint Force. A robust framework and deep understanding how the conventional force and SOF can complement one another, as well as a concerted effort at ensuring inter-operability, are required prior to any conflict erupting. Working together, the Joint Force and SOF can provide effective capability, however, to achieve this outcome a clear and cogent understanding of requirements, strengths and limitations of all actors must be in place prior to conflict.

Without diminishing the aforementioned challenges, arguably, the greatest test facing SOF in a high-intensity conflict will be the issue of lethality due to advanced technologies. Hypersonic missiles, such as the one tested

CONCLUSION

by China, which flew around the world at more than five times the speed of sound, then dropped off a hypersonic glide vehicle that struck a target in China, pose huge threats. Importantly, unlike intercontinental ballistic missiles that travel in a predictable arc and are trackable by long range radars, a hypersonic missile moves much closer to the earth, making it difficult for radars to detect.²⁴

Furthermore, the exponential proliferation of precision missiles with ever-increasing destructive power, directed energy weapons²⁵ and autonomous systems capable of loitering and swarming targets bodes ill for forces that are discovered in the battlespace.²⁶ The increased precision, payload and density of munitions make concealment, manoeuvre and access into theatres or specific objective areas increasingly difficult and deadly. Moreover, mobility itself becomes a critical concern as outright superiority in any one domain is questionable. Bereft of outright superiority, adversaries will struggle for control over specific corridors for restricted periods of time and even that will be difficult to achieve.

In essence, the overarching threat becomes the marriage of sensor/detection to shooter/munition precision and lethality. For example, the danger of sensor to shooter timeliness and accuracy was demonstrated by the Russians in the Ukraine since 2014. They had “shortened to mere minutes the time between when their spotter drones first detected Ukrainian forces and when their precision rocket artillery wiped those forces off the map.”²⁷ The use of AI, space-based weapons, lasers, directed-energy technology and high-powered microwaves, as well as CBRN munitions, will only increase lethality and reach. Importantly, well-timed and accurate delivery of ordnance has become increasingly possible since the world has become one big sensor making masking military deployments or actions virtually impossible. As one researcher concluded:

The amount of data generated by networked devices, is on pace to triple between 2016 and 2021. More significant, the proliferation of low-cost, commercial sensors that can detect more things more clearly over greater distances is already providing more real-time global surveillance than has existed at any time in history. This is especially true in space. In the past, the high costs of launching satellites required them to be large, expensive, and designed to orbit

CONCLUSION

for decades. But as access to space gets cheaper, satellites are becoming more like mobile phones—mass-produced devices that are used for a few years and then replaced. Commercial space companies are already fielding hundreds of small, cheap satellites. Soon, there will be thousands of such satellites, providing an unblinking eye over the entire world. Stealth technology is living on borrowed time.²⁸

Making the battlespace even more challenging is the advancements in the miniaturization of cameras and satellites. New microsattellites are relatively cheap, small, and effective. Moreover, a single rocket launch can deliver 80 small photo reconnaissance satellites into orbit. For example, this capability has permitted the American company “Planet” to photograph any corner of the globe with one of its 200 satellites. Furthermore, it can update images daily with two-metre resolution. Importantly, actors need only project coverage over their objective areas. They can achieve this by deploying 300 to 500 microsattellites over their areas of interest or concern. Remarkably, these satellites can generate imagery of one-metre resolution and transmit data every five to ten minutes. The point is, this satellite array will have complete photo coverage of a conflict zone or area of interest and be able to spot any aircraft or ship entering into the battlespace and provide exact targeting data.²⁹

In addition, next-generation high-power radio frequency-directed energy weapons that can disrupt electronic controls and shut off vessel engines without harming occupants, as well as millimetre wave active denial-directed energy technology further complicate the battlespace. Additionally, developing motor-powered exoskeleton suits that increase human capacity to carry weight or cover distances already exist. The use of armour plate, weapon suites and jet-packs for flight are just a matter of time.³⁰

In short, the future battlefield will be characterized by increased lethality, enhanced speed and tempo of operations, amplified informatization empowered through AI, increased complexity, and the loss of traditional Western supremacy in all domains. Conflict between belligerents using modern weaponry will be disturbingly swift and horrifically destructive. In more than eight wargames set in the Indo-Pacific theatre, covering campaigns lasting from several days to several weeks, typical attrition exceeded the estimated combined U.S. and Japanese ship and aircraft losses from the

CONCLUSION

Battle of the Coral Sea and the Battle of Midway, which were two of the costliest air and naval battles in the Second World War. The wargames also determined that “combat is also disorientingly chaotic, regardless of whether information and command systems worked (in which case, long-range precision fires resulted in catastrophic attrition and destruction) or not (in which case, both sides scrambled to understand what was happening, make decisions, and communicate these decisions across their forces).³¹ In another wargame that simulated an AI-enhanced ground fight where troops were outnumbered three to one by enemy forces, the addition “of autonomous air and ground sensors allowed troops to smartly detect, target, and engage adversaries (find, fix, finish), realizing an approximate 10-fold increase in combat power.”³²

Adding to the enormity of the challenges are a myriad of other difficulties. Risk acceptance will have to be reviewed. In the context of the past two decades a premium has been placed on low casualties to friendly forces as well as limiting, if not negating, collateral damage. In the context of a high-intensity war, the reservation of “causing harm” will need to be reviewed. Restraint in undertaking operations because of probable cause in death and destruction can put success against adversaries, as well as lives of friendly forces, at great peril. Related to potential casualty rates and collateral damage is the issue of influence activities. Whether involved in irregular warfare or in operations in direct support of the Joint Force, SOF will require to place emphasis on gaining/maintaining the support of domestic and local populations, as well as influencing host-nation/local populations and international opinion/support. Support and trust of societies and their governments equals freedom of manoeuvre. It also translates into direct support in the way of passage of information, denial of the same to the enemy, as well as acceptance of set-backs and errors. The challenge lies in the difficulty of earning trust, particularly of alien cultures. The proliferation and sophistication of disinformation and “deep fakes,” that is “highly realistic and difficult to detect digital manipulations of audio or video” (or advanced Photo Shop for laymen) is making it easier than ever to disseminate false information purporting to portray someone doing something or saying something that is detrimental to their credibility or reputation. As technology develops and spreads, deep fakes will push disinformation to an entirely new level.³³ Within this environment

CONCLUSION

SOF will be required to win “hearts and minds” while combating aggressive disinformation campaigns.

Additionally, adversary SOF will also pose a significant challenge. As mentioned earlier, enemy SOF will be employed comparably to friendly SOF both in an offensive and defensive context. As such, forces that have been similarly selected, trained and equipped, with analogous TTPs and operating methodologies, will pose a substantial test. Operations will require significant planning, coordination and mitigation strategies for the plethora of challenges that will pose hurdles to success. Anticipation of these potential quandaries and contingency plans that allow for adaptation and rapid response is the first step.

The final challenge to be discussed is that of SOF self-image and a failure to evolve. For the past two decades SOF have been regularly touted as the “Force of Choice.” Media in its fullest form (e.g. television, movies, social media, books, internet, video games, etc..) have all created a larger than life image of SOF warriors. Much of this has been deserved as SOF have been a significant, if not overpowering, contributor to the “war on terror” and the spate of COIN and CT operations in the new millennium. However, an acknowledgement of the theoretical construct of SOF involvement in a high-intensity war is not enough. Habits die hard, particularly when they have been rooted in success. As such, the past twenty years of dominance in all aspects and domains of conflict can have a numbing effect on what changes are required to succeed in a new paradigm. As one analyst observed:

The high tempo of Western special operations forces’ activity over the past two decades has led to repetitive behaviors and the formation of a set of persistent patterns. Before operators arrived in Sana’a, for example, specialist kit would often be flown in by C-130 and picked up by the embassy, giving Yemeni customs workers a fairly reliable indicator that something was going to happen...the widespread collection of biometrics and the pervasive surveillance and archiving of data from public spaces, combined with the existing target decks established through the observation of counterterrorism operations, mean that theater entry in a covert posture against a great power competitor requires careful planning, novel techniques, and a credible digital past to support any false identities...Against a peer

CONCLUSION

adversary long-range standoff will force back insertion capabilities so that special operations forces will need to conduct an extended approach to the objective. They will need to look after themselves for a prolonged period in the field. They will need to minimize their emissions, which will require them to be unplugged from support by the joint force and necessitate that commanders are comfortable with only intermittent updates on their progress. The detailed planning necessary to operate undetected in an electronically contested environment will require a slow and deliberate tempo of operations. As with the challenges in covert operations there are cultural implications to how units prepare for fighting unplugged. Special operations forces have become accustomed to multiple successive short operations, rather than prolonged periods in the field. This is reflected in equipment: significant advances in the ergonomics of tactical gear, for example, have not been matched by advances in systems for carrying heavy loads long distances. It is even evident in the physiology of personnel. Within many units it is noticeable that operators who became lean to pass the endurance tests they faced in selection rapidly bulk up their upper bodies upon joining their units. While this allows for speed and power—ideal for raids—it comes at the expense of endurance. And there is a reflexive tendency to reach for technology to observe adversaries, such as the use of unmanned aerial systems that necessarily have a significant electronic signature. If units must increasingly operate at reach then dependence upon technological tools also risks exposure. Finally, as with the problems with pattern forming in a discreet posture leading to the exposure of covert forces, communications patterns used during exercises will form a set of expectations among adversaries. As a result, operators cannot simply rely on communications procedures that emphasize the usual equipment, but should design them with a conscious assessment of the mission, the threat, and the enemy's expectations.³⁴

The observations are a stark reminder of the challenges that exist. Importantly, since you cannot build SOF capability overnight, SOF cannot afford to “learn through experience,” which normally entails casualties in a high-intensity conflict. Therefore, careful consideration and thought must be applied to this issue, including the aspect of mental health, which

CONCLUSION

will undoubtedly be a major factor in the high stress, high tempo, lethal, battlespace of high-intensity conflict.

SUMMARY

It is impossible to predict the future. Although history provides cautionary tales, trends and possible outcomes, there is no crystal ball that can foretell events. As such, the observations of renowned historian Michael Howard are apropos. He asserted, “No matter how clearly one thinks, it is impossible to anticipate precisely the character of future conflict. The key is to not be so far off the mark that it becomes impossible to adjust once that character is revealed.”³⁵ As such, although the notion held by many that a high-intensity war is unfathomable, this belief must not allow SOF to become blinded to possible future outcomes. As Howard emphasizes, organizations must be able to adjust to realities on the ground. This ability requires forethought and an open-mindedness.

History has shown that through design or miscalculation, the occurrence of a major conflict between peer, near-peer and/or regional powers can never be discounted. A failure to anticipate the possibility of a high-intensity war could lead to punishing consequences. It is fundamentally important to anticipate possible events, which then enables quicker adaptation and change should the inconceivable occur. Having pondered, brain-stormed, war-gamed potential developments, SOF, at a minimum, can develop a conceptual picture of what the possible roles, tasks and challenges, as well as requirements will be.

After two decades of COIN and CT operations, in which SOF has held advantages in virtually every domain, the potential change in mindset, behaviour and TTPs to operate in a high-intensity warfare environment is daunting. This challenge can only be met by a proactive approach that puts the necessary effort and horse power behind anticipating future scenarios in the fullest sense and determining SOF contributions in those circumstances. In the end, as unlikely as many believe that the possibility of a conventional war between major international actors may be, SOF must expend some intellectual effort in understanding high-intensity conflict and the implications for SOF, particularly the challenges and potential requirements, as well as determining possible roles and tasks, so that it can best provide employment options to senior political and military decision-makers.

CONTRIBUTORS

BALASEVICIUS – Tony Balasevicius is a retired infantry officer. During his career he has served with the Canadian Airborne Regiment and with Joint Task Force Two (JTF2). He has worked in the Department of Applied Military Science at the Royal Military College of Canada (RMC) and as an Analyst with the Directorate Future Security Analysis (Chief Force Development). He was Team Leader at the Canadian Forces Warfare Centre (CFWC) Concepts Group, and worked at Chief of Defence Intelligence and the Canadian Forces Land Warfare Centre. Tony has a Master’s degree in War Studies from RMC. He has completed the Land Force Technical Staff Programme and Canadian Forces Staff College. He is currently doing contract work. His current field of research is focused on Russian military modernization and their development of Hybrid Warfare, the future of SOF, and non-state actors.

BROWN – Lieutenant-Colonel Andrew L. Brown, PhD is an assistant professor at the Royal Military College of Canada, where he teaches military history and serves as Associate Chair of War Studies. A Canadian Intelligence Corps officer, and former non-commissioned infantryman, he has served in the Royal Canadian Regiment, 3 Commando (The Canadian Airborne Regiment), and Canadian Special Operations Forces Command (CANSOFCOM). Lieutenant-Colonel Brown is a graduate of the Canadian Army Command and Staff College and the Joint Command and Staff Programme.

HORN – Colonel (Retired) Bernd Horn, OMM, MSM, CD, PhD is a former infantry officer who has held key command and staff appointments in the Canadian Armed Forces, including Deputy Commander of Canadian Special Operations Forces Command (CANSOFCOM), Commanding Officer of the 1st Battalion, The Royal Canadian Regiment and Officer Commanding 3 Commando, the Canadian Airborne Regiment. He is currently the CANSOFCOM Command Historian, an appointment he fills as a civilian. Dr. Horn is also an adjunct professor of history at the Royal Military College of Canada and a non-resident senior fellow at the Joint Special Operations University in Tampa.

CONTRIBUTORS

KIRAS – James D. Kiras is Professor of Strategy at the School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, where he has directed the School’s course of instruction on irregular warfare for almost twenty years. He is a non-resident senior fellow of the Joint Special Operations University, Tampa, Florida; a Fellow of Irregular Warfare Studies at the U.S. Air Force Special Operations School, Hurlburt Field, FL; and a founding member of the Special Operations Research Association and its peer-reviewed publication, the *Special Operations Journal*. He worked for several years in defense policy and consulting, counter-terrorism, and special operations, and publishes and lectures regularly on these subjects. His most recent books, for which he was a contributing editor, are *The (In)Visible Hand: Strategic Sabotage, Case Studies* (CANSOFCOM, 2021) and *Special Operations: Out of the Shadows* (Lynne Reinner, 2020). Dr. Kiras’s first book was entitled *Special Operations and Strategy: From World War II to the War on Terrorism* (Routledge 2006).

KRAMER – Lieutenant Colonel Nicholas J. Kramer is a U.S. Army officer and Middle East specialist with assignments at U.S. Special Operations Command and U.S. Central Command as a strategic planner. Lieutenant Colonel Kramer has deployed as an infantry officer to Iraq and as a Special Forces Detachment Commander to Afghanistan. He holds a Master’s degree in Non-proliferation and Terrorism Studies from the Middlebury Institute of International Studies at Monterey, California.

LANDRY – Lieutenant Colonel C.G. Landry is a career U.S. Army Special Forces Officer currently serving as USSOCOM’s Special Operations Liaison to Canada. He has served in a gamut of military advisor roles over the past two decades, from tactical training and exercise development to personally advising foreign General Officers and their staffs. In addition to his military training, Lieutenant Colonel Landry holds a BA from Xavier University in Cincinnati and an MA from the National Defense University in Washington DC. A native Acadian from Western Maine, Lieutenant Colonel Landry enjoys exploring new cities, finishing home projects, and modern philosophy.

MCCABE – Dr. Peter McCabe is an independent contractor who previously served as a Resident Senior Fellow with the Joint Special Operations University (JSOU) Institute of SOF Strategic Studies. Dr. McCabe came to JSOU from the U.S. Central Command, where he was a Strategic Policy

CONTRIBUTORS

Planner. Prior to that, Dr. McCabe served in the U.S. Air Force, retiring in 2011 as a Colonel. He has a Doctorate in Political Science, three Master's Degrees in Political Science, National Security Strategy, and Aeronautical Science, and a Bachelor of Science in Physics. His military education includes the National War College.

PROVENCHER – Captain Nicolas Provencher is a former Army Reserve Infanteer. He spent six years at the Voltigeurs de Québec where he completed a bachelor's degree in history and a graduate diploma in Cegep Education from Université Laval in Quebec City. In 2016, he changed careers and joined the regular force as a Training Development Officer (TDO). He was then posted to 2 Wing Bagotville in 2017 and has held a TDO position at CANSOFCOM since 2019. In 2020, he completed a Master of Arts in War Studies at the Royal Military College of Canada in Kingston.

GLOSSARY OF ABBREVIATIONS

A2AD	Anti-Access/Area Denial
AFO	Advanced Force Operations
AI	Artificial Intelligence
AQI	Al-Qaeda in Iraq
BDA	Battle Damage Assessment
C4	Command, Control, Communications, Computers
CANSOFCOM	Canadian Special Operations Forces Command
CBRN	Chemical, Biological, Radiological, Nuclear
CCTV	Close Circuit Television
C-RAM	Counter-Rocket, Artillery, and Mortar
COIN	Counter-Insurgency
CT	Counter-Terrorism
DE	Directed Energy
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
EW	Electronic Warfare
FID	Foreign Internal Defence
FRY	Federal Republic of Yugoslavia
FUSAG	First United States Army Group
FOE	Future Operating Environment
FSSF	First Special Service Force
GWOT	Global War on Terrorism
HED	Hybrid-Electric Drive
HEO	Hyper-Enabled Operator
HVT	High Value Targets
ISR	Intelligence, Surveillance, Reconnaissance

GLOSSARY OF ABBREVIATIONS

JADO	Joint All Domain Operations
JSOU	Joint Special Operations University
JTAC	Joint Terminal Attack Controller
LAWS	Lethal Autonomous Weapon System
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NSS	National Security Strategy (U.S.)
OODA	Observe, Orient, Decide, and Act
OP	Observation Post or Operation (dependent on context)
PLA	People's Liberation Army, Chinese
PMC	private military corporation
PSYOPS	Psychological Operations
SAS	Special Air Service
SASR	Special Air Service Regiment (Australian)
SBS	Special Boat Service
SF	Special Forces
SHORAD	Short-Range Air Defence
SOF	Special Operations Forces
Sqn	Squadron
SSE	Sensitive Site Exploitation
TEL	Transporter-Erector-Launchers
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle
UW	Unconventional Warfare
VBSS	Visit, Board, Search and Seizure
WMD	Weapons of Mass Destruction
POW	Prisoners of War
SOE	Special Operations Executive

NOTES

INTRODUCTION

1 The Office of the President of the United States, *National Security Strategy of the United States of America* (Washington, DC: Office of the President of the United States, December 2017), 2.

2 “Afghanistan: What has the conflict cost the US and its allies?” *BBC News* (3 September 2021). <https://www.bbc.com/news/world-47391821>, accessed 15 March 2022.

3 For details of the rationale, genesis, development, and maturation of this targeting process, see Stanley McChrystal, “It Takes a Network: The New Front Line of Modern Warfare,” *Foreign Policy* (21 February 2011). <https://foreignpolicy.com/2011/02/21/it-takes-a-network/>, accessed 15 March 2022; and Richard H. Shultz, Jr., *Transforming US Intelligence for Irregular War: Task Force 714 in Iraq* (Washington, DC: Georgetown University Press, 2020).

4 In keeping with the tradition of creating new terms to drive change in the national security community, authors have employed several metaphors drawn from other fields to capture the characteristics of global violent Islamic extremist terrorism, including evolutionary biology (contagion and cellular mutation and adaptation) and geography (insurgent “archipelagos”). One metaphor that captured national security imagination to describe terrorist networks for a considerable period was the starfish, which can regenerate lost appendages. See Ori Brafman and Rod Backstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York, NY: Portfolio, 2006).

5 A long-standing observation regarding American SOF, captured officially in General Accounting Office, *Special Operations Forces: Opportunities to Preclude Overuse and Misuse*, GAO Report NSIAD-97-85 (Washington, DC: Government Printing Office, May 1997).

6 Bernd Horn, J. Paul de B. Taillon, and David Last, eds., *Force of Choice: Perspectives on Special Operations* (Kingston, ON: McGill-Queen’s University Press, 2004).

7 White House, *National Security Strategy of the United States of America*, 27.

8 For examples see Charles Q. Brown, Jr., *Accelerate Change or Lose* (Washington, DC: Department of the Air Force, 2020), https://www.af.mil/Portals/1/documents/csaf/CSAF_22/CSAF_22_Strategic_Approach_Accelerate_Change_or_Lose_31_Aug_2020.pdf; Headquarters Canadian Army, *Advancing with Purpose: The Canadian Army Modernization Strategy* (Ottawa, ON: HQ Canadian Army, December 2020), http://www.army-armee.forces.gc.ca/assets/ARMY_Internet/docs/en/national/2021-01-canadian-army-modernization-en.pdf; and, Public Diplomacy Division, *NATO 2030*, NATO Factsheet (Mons: NATO, June 2021), https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf.

NOTES

- 9 United States Department of Defense, *Defense Space Strategy Summary* (Washington, DC: Department of Defense, June 2020), https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF.
- 10 See for example Bernd Horn, James Kiras, and Emily Spencer, eds., *The (In)Visible Hand: Strategic Sabotage, Case Studies* (Ottawa, ON: Canadian Special Operations Forces Command, 2021) and Otto Fiala, *Resistance Operating Concept (ROC)* (Tampa, FL: Joint Special Operations University Press, 2020), <https://www.hsdl.org/?view&did=838149>.
- 11 Aaron Bazin, ed., *On Competition: Adapting to the Contemporary Strategic Environment* (MacDill Air Force Base, FL: JSOU Press, 2021), especially the “elegant alternative” proposed in Chapter 4.
- 12 Commander, Air Force Special Operations Command, *AFSOC Strategic Guidance* (Hurlburt Field, FL: Air Force Special Operations Command, 2020).
- 13 “CANSOF/JSOU/SOCNORTH Research Working Group Charter and Agenda,” 20 July 2021.
- 14 Edward Mazuchowski et al, “Mortality review of US Special Operations Command battle-injured fatalities,” *Journal of Trauma Acute Care Surgery* 88, no. 5 (May 2020): 686-695. DOI 10.1097/TA.0000000000002610.
- 15 A metaphor developed and popularized by Nassim Nicholas Talib, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed. (New York, NY: Random House, 2010).
- 16 Robert Spulak, *A Theory of Special Operations: The Origins, Qualities, and Use of SOF*, JSOU Report 07-7 (Hurlburt Field, FL: JSOU Press, 2007) and Richard Rubright, *A Unified Theory for Special Operations*, JSOU Report 17-1 (MacDill AFB, FL: JSOU Press, 2017).
- 17 The Joint Staff, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 2021), 49. Available online at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.
- 18 Canada, Department of National Defence, *B-GL-30-001/FP-001 Land Operations* (Kingston, ON: Army Publishing Office, 2008), 2-9.
- 19 Office of Strategic Research, “Soviet Nuclear Doctrine: Concepts of Intercontinental and Theater War.” Top Secret, redacted and released 12 December 1993. Central Intelligence Agency, June 1973. https://www.cia.gov/readingroom/docs/DOC_0000268107.pdf.
- 20 Michael Carver, “Conventional Warfare in the Nuclear Age,” in Peter Paret, ed., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, NJ: Princeton University Press, 1986), 811.
- 21 Sean McFate, “The F-35 tells everything that’s broken in the Pentagon,” The Hill (11 March 2021), <https://thehill.com/opinion/national-security/542412-the-f-35-tells-everything-thats-broken-in-the-pentagon>; and Robert Charette, “F-35 Program Continues to Struggle with Software,” *IEEE Spectrum* (19 September 2012), <https://spectrum.ieee.org/f35-program-continues-to-struggle-with-software>.

NOTES

- 22 Valeri Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* (January-February 2016): 23-29.
- 23 Blake Stillwell, "Why Russia's Hypersonic Missiles Can't Be Seen on Radar," *Military.com* (2021), available online at <https://www.military.com/equipment/weapons/why-russias-hypersonic-missiles-cant-be-seen-radar.html> accessed 12 April 2022.
- 24 Xiao Tianliang, ed., *战略学* (*The Science of Strategy*), (Beijing: National Defense University, 2015), U//FOUO translation 2016, 188.
- 25 United States, Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2020* (Washington, DC: Department of Defense, 2020), 161. <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>.
- 26 Tianliang, ed., *战略学* (*The Science of Strategy*), 127.
- 27 Timothy Thomas, *Russian Military Thought: Concepts and Elements*, MITRE Report MP190451V1 (McLean, VA: MITRE, August 2019), 10-1.
- 28 Gerasimov, "The Value of Science," 25.
- 29 A concise, entry-level guide to JADO is available in John Hoehn, *Joint All-Domain Command and Control: Background and Issues for Congress*, CRS Report R46725 (Washington, DC: Congressional Research Service, 18 March 2021), <https://crsreports.congress.gov/product/pdf/R/R46725/2>.
- 30 Gerasimov, "The Value of Science," 24.
- 31 Ibid.
- 32 A metaphor developed in pursuit of a general theory of strategy in Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2011).
- 33 Maksymilian Cziperski et al, *Hiding in Plain Sight: Putin's War in Ukraine* (Washington, DC: The Atlantic Council of the United States, 2015), available online at https://www.atlanticcouncil.org/wp-content/uploads/2019/08/HPS_English.pdf, accessed 12 April 2022.
- 34 Jethro Mullen and Sophia Saifi, "Whatever happened to guy who tweeted about raid that killed Osama bin Laden?" *CNN World* (20 January 2016), available online at <https://www.cnn.com/2016/01/20/asia/osama-bin-laden-raid-tweeter-sohaib-athar-rewind/index.html>.
- 35 Warren Strobel, "Biometrics, Smartphones, Surveillance Cameras Pose New Obstacles for U.S. Spies." *The Wall Street Journal* (27 November 2021), available (behind paywall), <https://www.wsj.com/amp/articles/biometrics-smartphones-surveillance-cameras-pose-new-obstacles-for-u-s-spies-11638009002>.
- 36 The prevailing narrative about the Social Credit System (SCS) derived from its promises and implications, in articles such as Alexandra Ma and Katie Canales, "China's

NOTES

‘social credit’ system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy,” *Business Insider* (9 May 2021), available online at <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4>. Others claim SCS is nowhere nearly as pervasive as some suggest. See Vincent Brussee, “China’s Social Credit System Is Actually Quite Boring,” *Foreign Policy* (15 September 2021), <https://foreignpolicy.com/2021/09/15/china-social-credit-system-authoritarian/>.

37 Thomas, *Russian Military*, 9-1.

38 Dale Hersping, “Nikolay Ogarkov and the Scientific-Technical Revolution in Soviet Military Affairs,” *Comparative Strategy* 6:1 (1987): 29-59, DOI: 10.1080/01495938708402702.

39 Gerasimov, “The Value of Science,” 24.

40 Thomas, *Russian Military Thought*, 9-18.

41 Bernd Horn, “Introduction,” in Bernd Horn, ed., *Risk & Decision-Making* (Ottawa, ON: Canadian Special Operations Forces Command, 2019), iii.

42 For an excellent primer on the “ground rules” of combined arms warfare on land, devoid of fashionable jargon and written in an accessible (i.e., non-specialist or doctrinal) manner, see Christopher Bellamy, *The Evolution of Modern Land Warfare: Theory and Practice* (London: Routledge, 1990), 15-29.

43 The Joint Staff, *Joint Publication 3-18: Joint Forcible Entry Operations* (Washington, DC: The Joint Staff, July 2021). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_18ch1.pdf?ver=A9WjEODmKtKqabuKPDGu_g%252525253d%252525253d.

44 United Kingdom, Ministry of Defence, *Joint Doctrine Note 1/17: Joint Theatre Entry*, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668722/doctrine_uk_joint_theatre_entry_jdn_1_17.pdf.

45 United States Army War College, *Campaign Planning Handbook – Academic Year 2017*, Carlisle Barracks, Pennsylvania: 2017, 105.

46 Gerasimov, “The Value of Science,” 24; and Andrew Duncan, “New ‘Hybrid War’ or Old ‘Dirty Tricks’? The Gerasimov Debate and Russia’s Response to the Contemporary Operating Environment,” *Canadian Military Journal* 17, no. 3 (Summer 2017): 7.

47 For an extended treatment of this subject, see Sam Tangredi, *Anti-Access Warfare: Countering A2/AD Strategies* (Annapolis, MD: Naval Institute Press, 2013).

CHAPTER 1

1 Various national doctrines emphasize SOF’s role in supporting joint operations. For instance, American SOF doctrine states that most SOF operations “are planned and conducted in support of theatre campaigns. Special operations typically complement—not compete with nor substitute for—conventional operations.” This includes SOF support to “large-scale combat.” See Joint Publication 3-05, *Special Operations*, 16 July

NOTES

2014 (hereafter JP3-05), pages I-2 and I-9. Similarly, Canadian joint operations doctrine states that while SOF may plan and execute independent operations for the Government of Canada, SOF normally operate in support of a joint force. See B-GJ-005-300/FP-001 Canadian Forces Joint Publication (CFJP) 3.0 (2011-09), *Operations*, paras 0327 and 0330, pages 3-6 and 3-7.

2 American doctrine uses the term *Joint Forcible Entry Operations*. British doctrine uses the term *Joint Theatre Entry*.

3 Niccolò Petrelli, "The Missing Dimension: IDF Special Operations Forces and Strategy in the Second Lebanon War," *Small Wars and Insurgencies* 23, no. 1 (2012): 64 and 68. See also Avi Kober, "The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance?," *Journal of Strategic Studies* 31, no. 1 (2008): 5 and 27.

4 American SOF doctrine formally recognizes this as a SOF limitation. JP 3-05, I-6.

5 JP3-05, II-4 and II-5.

6 *Ibid.*, II-6.

7 Mark Galeotti, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?" *Small Wars and Insurgencies* 27, no. 2: 282-286.

8 Michael S. Repass, *Combatting Terrorism with Preparation of the Battlespace* (Carlisle, Pennsylvania: U.S. Army War College Strategy Research Project, 2003), 18-21.

9 Ohad Leslau, "Worth the Bother? Israeli Experience and the Utility of Special Operations Forces," *Security Policy* 31, no. 3 (2010): 516.

10 Repass, *Combatting Terrorism*, 19.

11 Bob Woodward, *Plan of Attack: The Definitive Account of the Decision to Invade Iraq* (New York: Simon & Schuster Paperbacks, 2004): 55 and 99.

12 Leigh Neville, *Special Operations Forces in Iraq* (Oxford: Osprey Publishing, 2008), 10.

13 Woodward, *Plan of Attack*, 381.

14 Alastair Finlan, *Special Forces, Strategy and the War on Terror: Warfare by Other Means* (London: Routledge, 2008): 143-44. Finlan concedes that no evidence exists proving that Saddam Hussein wanted to engage Israel with missiles.

15 A2AD is a new name for an old problem. While the term "A2AD" does not enjoy universal recognition as a well-defined concept, it is sufficient for this chapter's purposes of introducing major challenges and proposing potential SOF roles.

16 Keir Giles and Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined," *Parameters* 49, no. 1 (2019): 24.

17 *Ibid.*, 30.

NOTES

18 Government of Sweden, Swedish Defence Research Agency (FOI). *Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*. Robert Dalsjö, Christofer Berglund, and Michael Jonsson. FOI-R-4651-SE. Stockholm: FOI, 2019: 11.

19 Giles and Mathieu Boulegue, "Russia's A2/AD Capabilities," 25.

20 Dalsjö, Berglund, and Jonsson, *Bursting the Bubble*, 46.

21 Warships can degrade A2AD systems by striking seaborne and shore-based targets. *Ibid.*, 50.

22 *Ibid.*, 51.

23 Major Christopher J. Mihal, "Understanding the People's Liberation Army Rocket Force: Strategy, Armament, and Disposition," *Military Review* (July-August 2021): 232.

24 Dalsjö, Berglund, and Jonsson, *Bursting the Bubble*, 54-55.

25 Giles and Boulegue, "Russia's A2/AD Capabilities," 34-35. The authors propose that with the right investments, the U.S. Army can field capabilities to degrade Russian A2AD operations.

26 U.S. doctrine recognizes SR as a special operations core activity. JP 3-05, II-3. Canadian joint doctrine assigns CANSOFCOM with responsibility for conducting SR. CFJP 3.0 (2011-09), *Operations*, para 0326, pages 3-7.

27 For a definition of special reconnaissance, see JP 3-05, x.

28 Benjamin S. Lambeth, "Lessons from the War in Kosovo," *Joint Force Quarterly* (Spring 2002), 14.

29 Finlan, *Special Forces, Strategy and the War on Terror*, 10.

30 Sebastien Ritchie, "Air Power Victorious? Britain and NATO Strategy during the Kosovo Conflict," in *Air Power History: Turning Points from Kitty Hawk to Kosovo*, ed. Sebastian Cox and Peter Gray (New York: Frank Cass Publishers, 2002), 322.

31 Sean M. Maloney, *Operation Kinetic: Stabilizing Kosovo* (Lincoln, Nebraska: Potomac Books, 2018), 169-170.

32 Lambeth, "Lessons from the War in Kosovo," 17.

33 *Ibid.*, 19.

34 Finlan, *Special Forces, Strategy and the War on Terror*, 10.

35 Lieutenant-General Sir Cedric Delves, *Across an Angry Sea: The SAS in the Falklands War* (London: Hurst & Company, 2018), 113 and 127. Also, see Alastair Finlan, "British Special Forces in the Falklands Conflict: Twenty Years On," *Defense and Security Analysis* 18, no. 4 (2002): 322.

36 Finlan, "British Special Forces in the Falklands Conflict," 323.

NOTES

- 37 Delves, *Across an Angry Sea*, 113-114.
- 38 For precise definitions of these terms, see North Atlantic Treaty Organization (NATO), *AAP-06 – NATO Glossary of Terms and Definitions* (NATO Standardization Office, 2020): 41 and 52.
- 39 Delves, *Across an Angry Sea*, 188-189.
- 40 *Ibid.*, 191-192.
- 41 *Ibid.*, 215 and 223.
- 42 The information in this paragraph comes from two sources: Richard Overy, *Why the Allies Won* (New York: W.W. Norton & Company, 1995), 151-152; and John Keegan, *The Second World War* (New York: Penguin Books, 1989), 373-374.
- 43 Neville, *Special Operations Forces in Iraq*, 26.
- 44 *Ibid.*, 22.
- 45 *Ibid.*, 32.
- 46 Bernd Horn, "The End of 'The Golden Age of SOF'? Is There a Role for Special Operations Forces in the Renewed Great Power Competition," *The Journal of Future Conflict* 2 (Fall 2020), 4-5.
- 47 Colonel David Bickers, "Understanding China's New Joint Force," *Joint Force Quarterly* 103, (4th Quarter 2021): 85.
- 48 Stefan Heglund, "The Future of Russia's Special Operations Forces," Geopolitical Intelligence Services, 27 February 2019, <https://www.gisreportsonline.com/the-future-of-russias-special-operations-forces,defense,2813.html>.
- 49 Delves, *Across an Angry Sea*, 295.
- 50 Neville, *Special Operations Forces in Iraq*, 15-16.
- 51 Anthony H. Cordesman, *Lessons and Non-Lessons of the Air & Missile Campaign in Kosovo* (Westport, Connecticut: Praeger Publishers, 2001), 233.
- 52 Ritchie, "Air Power Victorious," 322; Lambeth, "Lessons from the War in Kosovo," 16.
- 53 Cordesman, *Lessons and Non-Lessons*, 233.
- 54 U.S. Library of Congress, Congressional Research Service, *Iran's Foreign and Defense Policies*, by Kenneth Katzman, R44017, 11 January 2021, 1.
- 55 U.S. Library of Congress, Congressional Research Service, *Iran: Internal Politics and U.S. Policy and Options*, by Kenneth Katzman, RL32048, 20 November 2019, 6-7 and 14.
- 56 *Ibid.*, 17.

NOTES

- 57 Colonel Liam Collins and Captain Harrison Morgan, “King of Battle: Russia Breaks out the Big Guns,” *Army Magazine* 69, no. 2 (2019): 44-45.
- 58 Janes Sentinel Security Assessment – Russia and the CIS, Russian Federation Armed Forces, Joint Forces Interoperability, 21 May 2021.
- 59 Janes Sentinel Security Assessment – China and Northeast Asia, Armed Forces, Unmanned Aerial Vehicles, 2 March 2021.
- 60 Collins and Morgan, “King of Battle,” 45.
- 61 Lieutenant-Colonel Dan Sukman and Lieutenant-Colonel (retired) Charles Davis, “Divided We Fall: How the U.S. Force Is Losing Its Joint Advantage over China and Russia,” *Military Review* (March-April 2020): 49-56.
- 62 The five SOF Truths are:
- Humans are more important than hardware.
 - Quality is better than quantity.
 - Special Operations Forces cannot be mass produced.
 - Competent Special Operations Forces cannot be created after emergencies occur.
 - Most special operations require non-SOF assistance.
- U.S. Special Operations Command website, <https://www.socom.mil/about/sof-truths>, accessed 15 April 2022.

CHAPTER 2

- 1 IMDb website, <https://www.imdb.com/title/tt0062886/>, accessed 13 December 2021.
- 2 See U.S. Army Center of Military History, 1st SPECIAL FORCES GROUP, 1st SPECIAL FORCES REGIMENT, accessed 13 December 2021, <https://history.army.mil/html/forcestruc/lineages/branches/sf/001sfgrp1sf.htm>, National Museum of the U.S. Army, accessed 13 December 2021, <https://armyhistory.org/first-special-service-force/> and History of the First Special Service Force, accessed 13 December 2021, <http://www.firstspecialserviceforce.net/history.html>.
- 3 See Bernd Horn and Wycyznski, *Of Courage and Determination: The First Special Service Force, 1942-44* (Toronto: Dundurn, 2013); and “History of the First Special Service Force,” <http://www.firstspecialserviceforce.net/history.html>, accessed 13 December 2021.
- 4 *DOD Dictionary of Military and Associated Terms*, August 2021, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.
- 5 Joint Publication 3-0, *Joint Operations*, 17 January 2017, V-5, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.
- 6 JP 3-0, V-7.
- 7 *DOD Dictionary of Military and Associated Terms*, August 2021, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.

NOTES

8 Joint Publication 3-05, *Special Operations*, 18 April 2011, I-4. From a CANSOF perspective, “CANSOFCOM capabilities deliver to the CAF [Canadian Armed Forces] early, essential awareness of rapidly developing crises. In addition, the modularity and scalability of the SOTFs [Special Operation Task Forces] allow for a tailored, enabled SOF capability to be rapidly projected into a crisis situation, providing valuable support to the larger CAF mission.” Canada, *CANSOFCOM’s Strategic Plan* (Ottawa: DND, 2015), 13.

9 Steve Balestrieri, “Two Ranger Bns Wiped Out at Cisterna, Jan 30, 1944,” *SOFREP* (31 Jan 2019), <https://sofrep.com/specialoperations/two-ranger-bns-wiped-out-at-cisterna-jan-30-1944/>.

10 Hal Brands, “Pentagon’s special forces need to go back to the future,” American Enterprise Institute (24 May 2021), <https://www.aei.org/op-eds/pentagons-special-forces-need-to-go-back-to-the-future/>.

11 “Keynote Address – Special Operations Theory” by Charles Cleveland in *Special Operations Theory* edited by Peter McCabe and Paul Lieber (Tampa, FL: JSOU Press, 2017): 20.

12 William H. McRaven, *Spec Ops Case Studies in Special Operations Warfare: Theory and Practice*, (Novato: Presidio Press, 1995), 278.

13 Ibid., 246.

14 Ibid., 246-250, 279.

15 Ibid., 246.

16 Ibid., 273

17 Ibid., 246.

18 Ibid., 247.

19 Ibid., 279.

20 Ibid., 280.

21 Ibid., 260.

22 Ibid., 278.

23 Ibid., 257-262.

24 Ibid.

25 Ibid.

26 Ibid., 260.

27 Ibid., 257-262.

28 Ibid., 270.

NOTES

- 29 Ibid.
- 30 Ibid., 271-272.
- 31 Ibid.
- 32 Ibid.
- 33 Ibid.
- 34 Ibid., 273.
- 35 Ibid., 277.
- 36 Neal Bascomb, *The Winter Fortress: The Epic Mission to Sabotage Hitler's Atomic Bomb*, (Boston: First Mariner Books, 2016): 6-7.
- 37 Ibid., 29, 42-43.
- 38 Ibid.
- 39 Ibid., 91-92, 164, 181-182.
- 40 Ibid., 68-69.
- 41 Ibid., 87-88.
- 42 Ibid., 92-96.
- 43 Ibid., 113-116.
- 44 Ibid., 119-123.
- 45 Ibid., 123.
- 46 Ibid., 80-82, 138.
- 47 Ibid., 129.
- 48 Tony Insall, *Secret Alliances: Special Operations and Intelligence in Norway 1940-1945*, (London: Biteback Publishing, 2019): 261.
- 49 Bascomb, *The Winter Fortress*, 130.
- 50 Ibid., 138
- 51 Ibid., 169-170.
- 52 Ibid., 177-178.
- 53 Ibid., 154-155, 167-168.
- 54 Ibid., 184-197.
- 55 Ibid.
- 56 Ibid., 196-199.

NOTES

- 57 Ibid.
- 58 Ibid., 199.
- 59 Ibid., 199-202.
- 60 Ibid., 201-203.
- 61 Ibid., 202.
- 62 Ibid., 203.
- 63 Ibid., 198-200.
- 64 Ibid., 209-225.
- 65 Ibid.
- 66 Ibid., 213.
- 67 Ibid., 221.
- 68 Ibid.
- 69 Ibid., 222.
- 70 Ibid., 241-242, 248.
- 71 Ibid., 263-269, 273.
- 72 Ibid.
- 73 Ibid., 277.
- 74 Ibid.
- 75 Ibid., 279.
- 76 Ibid.
- 77 Ibid., 221.
- 78 Ibid., 283.
- 79 Ibid., 290.
- 80 Ibid., 294
- 81 Ibid., 303-306.
- 82 William Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets: Lessons from Vietnam and the Persian Gulf War* (Washington, DC; RAND, 2001): 29.
- 83 Ibid.

NOTES

- 84 Ibid.
- 85 Ibid.
- 86 Ibid.
- 87 Ibid., 30.
- 88 Ibid., 31.
- 89 Ibid.
- 90 Ibid.
- 91 Ibid.
- 92 Sebastien Roblin, "What the Great Scud Hunt Tells About a War With North Korea," *National Interest*, 6 October 2017, accessed 24 November 2021, <https://nationalinterest.org/blog/the-buzz/what-the-great-scud-hunt-tells-about-war-north-korea-22637>.
- 93 Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets*, 33.
- 94 Roblin, "What the Great Scud Hunt Tells About a War With North Korea."
- 95 Ibid.
- 96 Ibid.
- 97 Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets*, 32.
- 98 Ibid., 34.
- 99 Roblin, "What the Great Scud Hunt Tells About a War With North Korea."
- 100 Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets*, 35.
- 101 Ibid., 34.
- 102 Ibid., 35-36.
- 103 Ibid., 37.
- 104 Ken Connor, *Ghost Force: The Secret History of the SAS* (London: Lume Books, 2018): 506.
- 105 Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets*, 37.
- 106 Roblin, "What the Great Scud Hunt Tells About a War With North Korea."
- 107 Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets*, 35.
- 108 Ibid.
- 109 Ibid., 33.

NOTES

110 Ibid.

111 Ibid., 32.

112 Ibid.

113 Ibid.

114 Ibid.

115 Roblin, “What the Great Scud Hunt Tells About a War With North Korea.”

116 Ibid.

117 Ibid.

118 Ibid.

119 Ibid.

120 Ibid.

121 Ibid.

122 Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets*, 43.

123 See Thomas F. Lynch III, “The New Era of Great Power Competition and the Biden Administration,” *Joint Forces Quarterly* 103, (4Q 2021); Alexander Boroff, “What is Great-Power Competition, Anyway?” *Modern War Institute*, 17 April 2020, <https://mwi.usma.edu/great-power-competition-anyway/>; and Jack MacLennan, “The Problem with Great-Power Competition,” *Modern War Institute*, 1 May 2020, <https://mwi.usma.edu/problem-great-power-competition/>.

124 National Security Strategy, The White House, December 2017: 2, <https://nssarchive.us/wp-content/uploads/2020/04/2017.pdf>.

125 Ibid.

126 Charles Cleveland, “Keynote Address – Special Operations Theory” in *Special Operations Theory* edited by Peter McCabe and Paul Lieber (Tampa, FL: JSOU Press, 2017), 20.

127 See General Joseph Votel statement before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 18 March 2015; and David Barno and Nora Bensahel, “Fighting and Winning in the ‘Gray Zone,’” *War on the Rocks*, May 2015.

128 See Joseph Votel, Charles Cleveland, Charles Connett, and Will Irwin, “Unconventional Warfare in the Gray Zone,” *Joint Forces Quarterly* 80, (1st Quarter 2016); Michael Eisenstadt, “Operating in the ‘Gray Zone’ to Counter Iran,” *Washington Institute*, 18 Sep 2019, washingtoninstitute.org; and Barnett Koven and Katy Lindquist, *Barriers to Special Operations Forces-Led Counterterrorism Effectiveness* (Tampa, FL: JSOU Press, 2021): 2.

NOTES

129 George F. Kennan, "The Inauguration of Organized Political Warfare," Office of the Historian of the State Department, 4 May 1948.

130 RAND study, "Countering Russia: The Role of Special Operations Forces in Strategic Competition," November 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA400/RRA412-1/RAND_RRA412-1.pdf.

131 Sabine Siebold, "Latvia calls for permanent U.S. troops to guard against Russia threat," *Reuters*, 29 November 2021, <http://www.reuters.com/world/europe/latvia-calls-permanent-us-troops-guard-against-russia-threat-2021-11-29/>.

132 Otto Fiala, ed., *Resistance Operating Concept (ROC)* (Tampa, FL: JSOU Press, 2020): ix.

133 See series of three volumes that study resistance movements: Will Irwin, *Support to Resistance: Strategic Purpose and Effectiveness* (Tampa, FL: JSOU Press, 2019); Will Irwin, *How Civil Resistance Works (Any Why it Matters to SOF)* (Tampa, FL: JSOU Press, 2019); and Will Irwin, *Decision-Making Considerations in Support to Resistance* (Tampa, FL: JSOU Press, 2020).

134 Utilizing conventional forces to counter SOF teams can be very personnel intensive. During the Vietnam War, the Studies and Observation Group (SOG) operations to interdict the Ho Chi Minh trail required the North Vietnamese Army to allocate approximately three full divisions, approximately 30,000 men, to rear area security. This effect was achieved by about 50 American SOG members and their host-nation soldiers working in small teams of four to twelve operators. See John L. Plaster, *SOG* (New York: Onyx, 1997), 251, 267 and 355. Moreover, in March 2003, M Squadron, SAS, operating deep behind enemy lines necessitated the pursuit by large components of the Iraqi Army 5th Corps, as well as thousands of Saddam Hussein's Fedayeen. See Damien Lewis, *Zero Six Bravo* (London: Quercus, 2013).

135 Adam Entous and Evan Osnos, "Qassem Suleimani and How Nations Decide to Kill," *The New Yorker*, 23 February 2020, <https://www.newyorker.com/magazine/2020/02/10/qassem-suleimani-and-how-nations-decide-to-kill>, accessed 30 December 2021.

136 Benjamin Armitter and Kurt Carlson, "The Changing Face of Russian Counter-Irregular Warfare," *War On The Rocks*, 21 December 2021, <https://warontherocks.com/2021/12/The-Changing-Face-Of-Russian-Counter-Irregular-Warfare/>, accessed 21 December 2021.

137 Tyler Rogoway, "Special Ops Train To Defend Strategic Aleutian Islands Radar Outpost During All-Out War," *The War Zone*, 18 October 2021, <https://www.thedrive.com/the-war-zone/42783/special-ops-train-to-defend-strategic-radar-outpost-in-the-aleutian-islands-during-all-out-war>, accessed 26 October 2021.

138 Christopher Marsh, *Developments in Russian Special Operations: Russia's Spetsnaz, SOF and Special Operations Command* (Ottawa: CANSOFCOM, 2017), 12.

139 Alexey Nikolsky, "Little, Green and Polite: The Creation of Russian Special Operations Forces," in *Brothers Armed: Military Aspects of the Crisis in Ukraine*, eds. Colby Howard and Ruslan Pukhov (Minneapolis: East View Press, 2015), 126-127.

NOTES

- 140 Alexey Nikolsky, "Russian Special Operations Forces: Eight Years and Three Wars," in *Elite Warriors: Special Operations Forces From Around the World*, edited by Ruslan Pukhov and Christopher Marsh (Minneapolis: East View Press, 2017), 29.
- 141 Dennis Blasko, "Chinese Special Operations Forces: Not like 'Back at Bragg,'" *War on the Rocks*, 1 January 2015, <https://warontherocks.com/2015/01/chinese-special-operations-forces-not-like-back-at-bragg/>.
- 142 Vasilily Kashin, "Chinese Special Operations Forces," in *Elite Warriors: Special Operations Forces From Around The World*, eds. Ruslan Pukhov and Christopher Marsh (Minneapolis: East View Press, 2017), 211.
- 143 Warren P. Strobel, "Biometrics, Smartphones, Surveillance Cameras Pose New Obstacles for U.S. Spies," *Wall Street Journal*, 27 November 2021, accessed 30 November 2021, <https://www.wsj.com/articles/biometrics-smartphones-surveillance-cameras-pose-new-obstacles-for-u-s-spies-11638009002?page=1>.
- 144 Thomas Hegghammer, "Resistance is Futile: The War on Terror Supercharged State Power," *Foreign Affairs*, September/October 2021, <https://www.foreignaffairs.com/articles/middle-east/2021-08-24/resistance-futile>, accessed 21 December 2021.
- 145 Strobel, "Biometrics, Smartphones, Surveillance...".
- 146 Ronen Bergman and Farnaz Fassihi, "The Scientist and the A.I.-Assisted, Remote-Control Killing Machine," *The New York Times*, 18 September 2021, <https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html>, accessed 30 November 2021.

CHAPTER 3

- 1 Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.: Princeton University Press, 2004), 28-51.
- 2 Robyn Dixon, "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare," *Washington Post*, November 11, 2020. https://www.washingtonpost.com/world/europe/nagorno-karabakh-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html.
- 3 Andrew F. Krepinevich, "Protracted Great-Power War: A Preliminary Assessment," Center for a New American Security, February 5, 2020, 16-19. <https://www.cnas.org/publications/reports/protracted-great-power-war>.
- 4 Ibid., 18-19.
- 5 McRaven, *Spec Ops*, 4-8.
- 6 Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 67-72; and Peter W. Singer, and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018), 118-147.

NOTES

- 7 Christopher Scott, Robin Brachear, Donald Boyer, Larry Forrest, William Travis, Andrew Moore, Sergei Volodin, "Russian New Generation Warfare Version 2.1." Asymmetric Warfare Group, April 2017, 60-61.
- 8 Ibid., 60-61.
- 9 United States Government, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election." 116th Congress 2nd Session. Washington D.C.: Select Committee on Intelligence United States Senate, November 10, 2020: 73-147. Scott, Brachear, Boyer, Forrest, Travis, Moore, and Volodin, "Russian New Generation Warfare Version 2.1," 60-62.
- 10 Singer and Brooking, *Like War*, 148-149.
- 11 Scott, Brachear, Boyer, Forrest, Travis, Moore, and Volodin, "Russian New Generation Warfare Version 2.1," 37-38.
- 12 R. J. Overy, *Why the Allies Won* (New York: W.W. Norton, 1996), 106.
- 13 Robert Anthony Pape, *Bombing to Win Air Power and Coercion in War*. Cornell Studies in Security Affairs (Ithaca, N.Y: Cornell University Press, 1996), 314-331.
- 14 Martin Van Creveld, *Supplying War: Logistics from Wallenstein to Patton*. 2nd ed (Cambridge, UK : Cambridge University Press, 2004), 12.
- 15 Headquarters, Department of the Army (U.S.). *Training Circular 3-22.240: Medium Machine Gun*. Army Publishing Directorate, 2017, 2-3.
- 16 James G. Zumwalt, *Bare Feet, Iron Will* (Jacksonville, FL: Fortis Publishing, 2010), 223.
- 17 Ibid., 232.
- 18 Cochlear, "How Do Cochlear Hearing Implants Work?" Accessed December 10, 2021. <https://www.cochlear.com/us/en/home/diagnosis-and-treatment/how-cochlear-solutions-work/cochlear-implants/how-cochlear-implants-work>.
- 19 Ibid.
- 20 Morgan B. Lee, Daniel R. Kramer, Terrance Peng, Michael F. Barbaro, Charles Y. Liu, Spencer Kellis, and Brian Lee, "Clinical Neuroprosthetics: Today and Tomorrow," *Journal of Clinical Neuroscience* 68 (2019), 13-19. <https://doi.org/10.1016/j.jocn.2019.07.056>.
- 21 M. F. Mridha, Sujoy Chandra Das, Muhammad Mohsin Kabir, Aklima Akter Lima, Md. Rashedul Islam, and Yutaka Watanobe, "Brain-Computer Interface: Advancement and Challenges," *Sensors (Basel, Switzerland)* 21, no. 17 (August 26, 2021), 5746. <https://doi.org/10.3390/s21175746>.
- 22 Lockheed Martin, "Exoskeleton Technologies: Military," May 10, 2021. <https://www.lockheedmartin.com/en-us/products/exoskeleton-technologies/military.html>.
- 23 ABC News, "U.S. Combat Pilots on Speed." Accessed December 18, 2021. <https://abcnews.go.com/2020/story?id=123779&page=1>.

24 Chad Peltier and Kyle Pettijohn, "The Future of Steroids for Performance Enhancement in the U.S. Military," *Military Medicine* 183, no. 7–8 (July 1, 2018), 151-153. <https://doi.org/10.1093/milmed/usy093>.

CHAPTER 4

1 Andrew D. James, *Policy Brief: Emerging Technologies and Military Capability* (Singapore: R. Rajaratnam School of International Studies, 2013), 3. <https://www.files.ethz.ch/isn/174574/Policy%20Brief-Emerging%20Technologies%20and%20Military%20Capability.pdf>, accessed 1 March 2022.

2 Ibid., 3.

3 Ibid., 1.

4 John Taft, Liz Gormisky and Joe Mariani, *Special operations forces and great power competition: Talent, technology, and organizational change in the new threat environment* (Washington D.C.: Deloitte Center for Government Insights, 2019), 14. Future of US Special Forces and the great power competition | Deloitte Insights <https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-special-operations-forces-great-power-competition.html>, accessed 5 March 2022.

5 Captain Paul D. Erickson, *Competition-and-Conflict-Implications-for-Maneuver-Brigades* (West Point, NY: DoD, 2021), 6. <https://mwi.usma.edu/wp-content/uploads/2021/06/Competition-and-Conflict-Implications-for-Maneuver-Brigades.pdf>, accessed 5 March 2022. Also see Richard H. Shultz, *Transforming US Intelligence for Irregular War: Task Force 714 in Iraq* (Washington, DC: Georgetown University Press, 2020), 1-3.

6 Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear," Blog - In Moscow's Shadows. <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>, accessed 10 May 2015. Note: many authorities on Russia believe that the article, which was first posted in 2013, may have been written by someone else. Also, the same briefing was presented by the Chief of the Russian General Staff, Army General Valeriy Gerasimov, in January 2013 at the Russian Academy of Military Sciences' annual meeting. Key elements of the Gerasimov Doctrine have since been integrated into the new edition of the Russian Military Doctrine, as approved in December 2014.

7 Ibid.

8 Ibid.

9 Ibid.

10 Colonel S.G. Chekinov (Reserve), Lieutenant General S.A. Bogdanov (Retired), "The Nature and Content of a New-Generation War," *Military Thought. A Russian Journal of Military Theory and Strategy*, 13. <https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Military%20Thought%202013.pdf>, accessed 7 March 2022.

11 Ibid.

NOTES

- 12 Galeotti, "The 'Gerasimov Doctrine.'"
- 13 Ibid.
- 14 Ibid.
- 15 Tchekinov and Bogdanov as cited in Janis Berzins, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy, Policy Paper, 6* (Riga: Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014), 2.
- 16 Land Forces Command, *Advancing with Purpose: The Canadian Army Modernization Strategy*, (Ottawa: DND, 2021). <http://www.army-armee.forces.gc.ca/en/news-publications/canadian-army-modernization-strategy.page#fn8> accessed 9 March 2022.
- 17 Ibid.
- 18 Ibid.
- 19 Ibid.
- 20 Alex MacCalman, Jeff Grubb, Joe Register and Mike McGuire, "The Hyper-Enabled Operator," *Small Wars Journal Online*, 6 June 2019. <https://smallwarsjournal.com/jrnl/art/hyperenabledoperator#:~:text=USSOCOM%20defines%20HEO%20as%20a,load%2C%20and%20accelerating%20decision%20making>, accessed 9 March 2022. Note: operating in the virtual plane involves seeking advantages within computer generated environments or cyberspace, while operating within the cognitive plane seeks to influence the minds of potential competitors and populations.
- 21 Land Force Command, *The Army Strategy* (Ottawa: DND, 2018). https://www.army.mil/e2/downloads/rv7/the_army_strategy_2018.pdf, accessed 10 March 2022.
- 22 Chris Balcik, "For Hyper-Enabled Operators, Cognitive Dominance is Built on Mobility," *Insights*, 13 May 2020, 2. <https://insights.samsung.com/2020/05/13/for-hyper-enabled-operators-cognitive-dominance-is-built-on-mobility/> accessed, 10 March 2022.
- 23 Ibid.
- 24 MacCalman et al, "The Hyper-Enabled Operator."
- 25 Ibid.
- 26 Vinod Anand, "Impact of Technology on Conduct of Warfare," *Strategic Analysis*, Vol XXIII, No. 1, April 1999. https://ciaotest.cc.columbia.edu/olj/sa/sa_99anv02.html, accessed 10 March 2022.
- 27 Ibid.
- 28 Kelley M. Sayler, *Emerging Military Technologies: Background and Issues for Congress*, (Washington D.C.: Congressional Research Service, 10 November 2021), 1. <https://sgp.fas.org/crs/natsec/R46458.pdf>, accessed 11 March 2022.
- 29 Ibid., 2.

NOTES

- 30 Laurie A. Harris, *Artificial Intelligence: Background, Selected Issues, and Policy Considerations*, (Washington D.C.: Congressional Research Service, 19 May 2021), 2. <https://crsreports.congress.gov/product/pdf/R/R46795>, accessed 20 March 2022.
- 31 Sayler, *Emerging Military Technologies*, 2.
- 32 Pragya Soni, "AI in Military Sector - Advantages and Disadvantages," *Analytic Steps*, 5 November 2021. <https://www.analyticssteps.com/blogs/ai-military-sector-advantages-and-disadvantages>, accessed 21 March 2022.
- 33 Sayler, *Emerging Military Technologies*, 6.
- 34 *Ibid.*, 2.
- 35 Khari Johnson, "Andrew Yang warns against 'Slaughterbots' and urges global ban on autonomous weaponry," *VentureBeat Online*, 31 January 2020. <https://venturebeat.com/2020/01/31/andrew-yang-warns-against-slaughterbots-and-urges-global-ban-on-autonomous-weaponry/>, accessed 9 March 2022.
- 36 Sayler, *Emerging Military Technologies*, 6.
- 37 *Ibid.*, 6. Note: LAWs are also known as lethal autonomous weapon systems (LAWS), autonomous weapon systems (AWS), robotic weapons, killer robots or slaughterbots. LAWs may operate in the air, on land, on water, underwater, or in space. The autonomy of current systems as of 2018 was restricted in the sense that a human gives the final command to attack – though there are exceptions with certain "defensive" systems.
- 38 *Ibid.*, 10.
- 39 Roxana Tiron, "Hypersonic Weapons: Who Has Them and Why It Matters," *Bloomberg Online*, 27 October 2021. <https://www.bloomberg.com/news/articles/2021-10-27/hypersonic-weapons-who-has-them-and-why-it-matters-quicktake>, accessed 28 March 2022.
- 40 *Ibid.*
- 41 *Ibid.*
- 42 Kelley M. Sayler, *Hypersonic Weapons: Background and Issues for Congress* (Washington D.C. CRS Report R45811, 19 October 2021), 13. <https://sgp.fas.org/crs/weapons/R45811.pdf>, accessed 28 March 2022.
- 43 *Ibid.*, 3.
- 44 *Ibid.*, 20.
- 45 Andrew Feickert, John R. Hoehn, Ronald O'Rourke, with Kelley M. Sayler, *Department of Defense Directed Energy Weapons: Background and Issues for Congress* (Washington D.C.: Congressional Research Service, 28 September 2021), 1-2. <https://crsreports.congress.gov/product/pdf/R/R46925>, accessed 27 March 2022.

NOTES

46 Sayler, *Emerging Military Technologies*, 15. A subset of DE weapons are high-powered microwave systems that could be employed as a non-kinetic method of disabling electronics, communications systems, and improvised explosive devices, or as a nonlethal “heat ray” for crowd control.

47 *Ibid.*, 18-19.

48 *Ibid.*, 23.

49 BAE Systems, “Hybrid Electric Drive: For the Military of Tomorrow,” ND. <https://www.baesystems.com/en-us/feature/hybrid-electric-drive-for-the-military-of-tomorrow>, accessed 27 March 2022.

50 *Ibid.*

51 US Department of Energy, Alternative Fuels Data Center, “How Do Hybrid Electric Cars Work?” ND. <https://afdc.energy.gov/vehicles/how-do-hybridelectriccarswork#:~:text=Hybrid%20electric%20vehicles%20are%20powered,by%20the%20internal%20combustion%20engine>, accessed 27 March 2022.

52 MacCalman et al, “The Hyper-Enabled Operator.”

53 *Ibid.*

54 *Ibid.*

55 *Ibid.*

56 *Ibid.*

57 Andrew Davidson, Scott Flanick, Ashley Yoo, John David Mote, and Vikram Mittal, *Expanding the Hyper-Enabled Operator Technology Across the Special Forces* (West Point, NY: DoD, 2019), 75. http://www.ieworldconference.org/content/WP2019/Papers/GDRKMCC-19_25.pdf, accessed 22 March 2022.

58 *Ibid.*, 76.

59 Yasmin Tadjdeh, “SOCOM Warrior: Hyper-Enabled Operator Concept Inches Closer to Reality,” *National Defense - Special Operations Technology Review, Special Report*, ND, 15. https://www.nationaldefensemagazine.org/-/media/sites/magazine/ebook/specialops_ebook.ashx, accessed 22 March 2022.

60 *Ibid.*, 18-19.

61 *Ibid.*

62 *Ibid.*

63 *Ibid.*, 5.

64 *Ibid.*, 6.

NOTES

- 65 National Academies of Sciences, Engineering, and Medicine, *Powering the U.S. Army of the Future* (Washington, D.C.: The National Academies Press, 2021), 9-5. <https://doi.org/10.17226/26052>. <https://www.fie.undef.edu.ar/ceptm/pdf/prospectiva/poweringTheUS-ArmyOfTheFuture-2021.pdf>, accessed 4 April 2022.
- 66 Jon Harper, "SOCOM Vehicles," *National Defense - Special Operations Technology Review, Special Report*, ND, 6.
- 67 US Department of Energy, "How Do Hybrid Electric Cars Work?"

CHAPTER 5

- 1 Pronounced "dot-mil-p-f", this acronym stands for doctrine, organization, training, materiel, leadership and education, personnel, and facilities. It is used by the United States Department of Defense and was defined in the Joint Capabilities Integration Development System, or JCIDS Process, as the framework to design administrative changes and/or acquisition efforts to fill a capability need.
- 2 James G. Herrera, *The Fundamentals of Military Readiness*, Congressional Research Service Paper, R46559 October 2, 2020.
- 3 Orlandrew Danzell and Steve Zidek, "Does Counterterrorism Spending Reduce the Incidence and Lethality of Terrorism: A Quantitative Analysis of 34 Countries," *Defense & Security Analysis* 29, Issue 3: Terrorism (2013), 218-233.
- 4 The author recognizes that there are purpose-built counterterrorism SOF that are definitively *not* organized for warfare but rather for crisis. While they may have secondary applications, warfighting is simply not their *raison d'être* from the perspective of mandates, authorities, and requirements of their parent governments. However, such counterterrorism-specific SOF are fewer in number and not intended to be conflated with those SOF organizations that maintain a traditional wartime role.
- 5 Peter D. Feaver, "Chapter Three: The Informal Agent Theory," in *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, Massachusetts: Harvard University Press, 2003), 54-95.
- 6 Nina M. Serafino, *Security Assistance Reform: "Section 1206" Background and Issues for Congress*, Congressional Research Service Paper, RS22855, 18 February 2010.
- 7 Canada, Department of National Defence, *Beyond the Horizon – A Strategy for Canada's Special Operations Forces in an Evolving Security Environment*. Catalogue No.: D2-426/2020, 2019, 18.
- 8 In late 2018, the US Army published TRADOC Pamphlet 525-3-1 *The US Army in Multi-Domain Operations 2028*. The publication was meant to energize and guide the US Army back into a more traditional role in high-intensity modern conflict, and away from irregular combat roles such as counter-insurgency. USSOF are barely mentioned. In fact, the capabilities of adversarial SOF are more clearly articulated at several points in the 87-page document.
- 9 Ottow C. Fiala, *Resistance Operating Concept* (Tampa, FL: JSOU, 2020).

NOTES

10 Jack C. Zeigler Jr. "The Army Special Operations Forces Role in Force Projection," Strategy Research Project ADA415798, US Army War College, Carlisle Barracks, Pennsylvania. 2003.

11 Philip Roessler, "The Enemy Within: Personal Rule, Coups, and Civil Wars in Africa," *World Politics* 63, No. 2 (April 2011), 300-346s.

12 Michael Connell, "Iran's Military Doctrine," *The Iran Primer*, US Institute of Peace, October 11, 2010. <https://iranprimer.usip.org/resource/iran-military-doctrine>, accessed 4 March 2022.

13 *Special Operations Forces Reference Manual, Fourth Edition* (Tampa, FL: JSOU, 2015), 78-83.

14 In 1988, the Commander of the US Army John F. Kennedy Special Warfare Center & School developed the "SOF Truths" as basic guidance for US Army SOF units. They are 1) Humans are more important than Hardware; 2) Quality is better than Quantity; 3) Special Operations Forces cannot be mass produced; and 4) Competent Special Operations Forces cannot be created after emergencies occur. A fifth SOF Truth – Most Special Operations require non-SOF assistance – was dropped, as US Army SOF was trying to defend its utility to the conventional forces. However, at the height of the GWOT, the Commander of USSOCOM added the fifth SOF Truth in 2009. <https://sof.news/sof/sof-truths/>, accessed 4 March 2022.

15 Programs of record can help align low-intensity employment as training events. Since the late 1960s, the United States Special Forces have used Joint Combined Exchange Training or JCETs (pronounced "Jay-sets") as a method of gaining specific funding for overseas training. Typically, one or several US Special Forces detachments will partner with a host nation's SOF or special missions-aligned unit to provide them SOF-specific training. However, the program is unique in that a JCET is specifically for the US Special Forces to practice their skills at building a partner's military capability in a culturally immersive environment. It is often said that while the host nation may benefit mightily from the instruction, 51 per cent of the training belongs to the US Special Forces detachment. The SOF unit therefore has a distinct say of the courseware and timing of a given JCET insofar as it also benefits their own readiness.

16 Justin Woodward, "How Should US Special Operations Forces Train For Great Power War?" *1945*, published 13 September 2021. <https://19fortyfive.com/2021/09/how-should-us-special-operations-forces-train-for-great-power-war/>, accessed 4 March 2022.

17 Fourth SOF Truth: Competent Special Operations Forces cannot be created after emergencies occur. See endnote 14.

18 Editorial Board. "US Clears Excess MRAP sale to United Arab Emirates, Apache Upgrades for Egypt," *Defense Brief*. Published on May 8, 2020. <https://defbrief.com/2020/05/08/us-clears-excess-mrap-sale-to-uae-apache-upgrades-for-egypt/>, accessed 4 March 2022.

19 During census interviews with US Special Forces enlisted members in 2019, one of the most common grievances was training for and deploying on low-prioritized missions without tactical objectives or operational longevity. Several soldiers noted as

NOTES

many as three such mission cycles back-to-back, each to very different parts of the world, and all complained about feeling less “ready,” unable to find an intersect or base-line for what they were supposed be trained for.

20 Mission Essential (YouTube Channel). “Mission Essential Conversations: The Identity Crisis in Special Forces with COL Edward Croot.” published 2 March 2021. <https://www.youtube.com/watch?v=QPAhSd4wDio>, accessed 4 March 2022.

21 “Adaptability” remains one of the listed core attributes for US Army Special Forces, as per the US Army John F. Kennedy Special Warfare Center & School. The schoolhouse defines this attribute in clear operational context: “Possessing the ability to maintain composure while responding to or adjusting one’s own thinking and actions to fit a changing environment; the ability to think and solve problems in unconventional ways; the ability to recognize, understand and navigate within multiple social networks; the ability to proactively shape the environment or circumstances in anticipation of desired outcomes.” Nevertheless, common definitions of the term are more readily understood and accepted organizationally.

CONCLUSION

1 Globalization is defined as “the process of interaction and integration among people, companies, and governments worldwide. Globalization has accelerated since the 18th century due to advances in transportation and communication technology.” <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095855259>, accessed 28 October 2021.

2 USSOCOM, *On Competition: Adapting to the Contemporary Strategic Environment*. JSOU Report 21-5 (Tampa: JSOU Press, 2021), xi.

3 The Turkish use of drone swarms to engage Syrian bases and chemical weapon depots in March 2020, as well as the South Korean demonstration of 1,218 autonomous drones equipped with lights collaborating to form intricate images in the night sky over Pyeongchang during the opening ceremonies of the 2018 Olympics provide a preview of what drone swarms are capable of achieving. See Seclan Hacaoglu, “Turkey’s Killer Drone Swarm Poses Syria Air Challenge to Putin,” *Bloomberg*, 1 March 2020. <https://www.bloomberg.com/news/articles/2020-03-01/turkey-s-killer-drone-swarm-poses-syria-air-challenge-to-putin>, accessed 2 March 2020; and Christian Brose, “The New Revolution in Military Affairs,” *Foreign Affairs*, 16 April 2019. <https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs>, accessed 25 April 2019.

4 See Nick Allen, Nataliya Vasilyeva and Joe Barnes, “Russia may invade Ukraine, U.S. warns as Russian forces gather near border,” *The Telegraph*, 11 November 2021. <https://nationalpost.com/news/world/russia-may-invade-ukraine-u-s-warns-as-russian-forces-gather-near-border>, accessed 13 November 2021; Sam Fleming and Valentina Pop, “NATO calls on Moscow to ease tension over military build-up near Ukraine,” *Financial Times*, 16 November 2021. <https://archive.md/HODrs#selection-1503.0-1503.72>, accessed 16 November 2021; and Eric Cheung and Brad Lendon, “China air force sends 77 warplanes into Taiwan defense zone over two days, Taipei says,” *CNN*, 3 October 2021. <https://www.msn.com/en-ca/news/world/china-air-force-sends-warplanes-into-taiwan-defense-zone-over-two-days-taipei-says/ar-AAP57ZO?ocid=sapphireappshare>, accessed 4 October 2021.

NOTES

5 Alan Bell, "On A Wing and A Prayer: Task Force 317 And The Recapture Of South Georgia Island," In Colonel (retired) Bernd Horn, ed., *Risk: SOF Case Studies* (Kingston: ERC Press, 2020), 125. See Bell's chapter, as well as Lieutenant General Sir Cedric Delves, *Across an Angry Sea. The SAS in the Falklands War* (London: Hurst & Company, 2018), 41-107, for an "operator's account" of the entire mission.

6 Ken Connor, *Ghost Force. The Secret History of the SAS* (London: Orion, 368-371; and John Strawson, *A History of the SAS Regiment* (London: Secker & Warburg, 1985), 236-238.

7 Delves, *Across an Angry Sea*, xvii, 131-174.

8 De La Billiere's plan was not met with enthusiasm. One former SAS operator recalled, "the Director [De La Billiere] wished us all good luck, said he would have our backs and that we would have his full support throughout the [Falklands] campaign. Unfortunately, at that time, little did we realize what he meant, but we were to learn later in the conflict that we were being signed on to execute "mission impossible" tasks, without the benefit of discussion or first refusal." Alan Bell, "On a Wing and a Prayer – Task Force 317 and the Recapture of South Georgia Island," unpublished paper, 2014. The Officer Commanding SAS "B" Squadron also disagreed. He was not convinced of the plan's viability. While staging on Ascension Island he voiced his concern. Director Special Forces was not impressed. De La Billiere lamented, "I was dismayed to find that the attitude of this unit [B Squadron] remained lukewarm. The trouble, I found, lay in the squadron commander, who himself did not believe in the proposed operation." The squadron commander was duly sacked. General Sir Peter De La Billiere, *Looking for Trouble. SAS to Gulf War* (London: Harper Collins Publishers, 1995), 346-347. Cedric Delves, then a squadron commander in the SAS later explained, "The EXOCET menace eventually grew acute. But an operation employing us to reduce the threat would have been pregnant with disproportionate risk, probably requiring a sizeable carrier task group to take forward the Squadron and its supporting helicopters, closing the Argentine mainland, bringing us all well within range of hundreds of enemy aircraft. And there could be no guarantee of nailing the objective, aircraft having a habit of moving. Nobody in his right mind would contemplate such a gamble. It was the sort of thing that could end in catastrophe and lose us the war." Delves, *Across an Angry Sea*, 115.

9 In advance of the raid, a Sea King helicopter was to drop off eight SAS operators (Operation Plum Duff) to observe the Argentinian Base and report. Due to weather conditions the helicopter was forced to abort. The helicopter pilot flew to Chile, ditched and destroyed the aircraft and all eight SAS operators and three aircrew were eventually picked up by Chilean forces and later returned to Britain. The aborted mission now compromised the element of surprise. Moreover, British intelligence discovered that Argentina's radar system was better than had originally been thought. As a result, Operation Mikado was cancelled. Peter Jackson, "Falklands War: SAS role in the conflict," *BBC*, 4 May 2021. <https://www.bbc.com/news/uk-17203398>, accessed 4 November 2021; and Connor, *Ghost Force*, 373-378.

10 The first US SOF teams began searching for mobile Transporter-Erector- Launchers on 7 February 2001. U.S. SOF and the SAS divided the responsibility for searching for the SCUD TEL launchers. The Americans operated in a several thousand square mile area northwest of the main Baghdad to Amman route up to the Syrian border (known

as “Scud Boulevard”) and the SAS was given the same size area known as “SCUD Alley.” William Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets. Lesson from Vietnam and the Persian Gulf War* (Santa Monica, CA: RAND, 2001), 30-39. See also DoD, *USSOCOM History*, 34-42; Douglas C. Waller, *Commando. The Inside Story of America’s Secret Soldiers* (New York: Simon & Shuster, 1994), 225-352; Susan Maquis, *Unconventional Warfare* (Washington D.C.: Brookings Institute Press, 1997), 227-249; Thomas K. Adams, *US Special Operations Forces in Action. The Challenge of Unconventional Warfare* (London: Frank Cass, 1998), 231-244; T. Carney and Benjamin F. Schemmer, *No Room for Error* (New York: Ballantine Books, 2003), 224-236; Connor, *Ghost Force*, 456-501; and Robin Neillands, *In the Combat Zone. Special Forces Since 1945* (London: Weidenfeld and Nicolson, 1997), 287-297.

11 There is no firm number of how many TELs were destroyed, however, the Iraqi launch rate dramatically decreased. Overall, the Iraqis fired 88 missiles against Israel and Saudi Arabia and Bahrain. They fired 33 in the opening week of Desert Storm at a daily rate of 4.7 launches. During remaining 36 days, they fired 55 missiles at a daily rate of 1.5. Rosenau, *Special Operations Forces*, 42. See also DoD, *USSOCOM History*, 42-44; B.J. Schemmer, “Special Ops Teams Found 29 Scuds Ready to Barrage Israel 24 Hours Before Ceasefire,” *Armed Forces Journal International*, July 1991, 36; Mark Thompson, Azadeh Moaveni, Matt Rees, and Aharon Klein, “The Great Scud Hunt,” *Time*, 23 December 2002, Vol 160, no. 26, 34; and Cameron Spence, *Sabre Squadron* (London: Michael Joseph, 1997).

12 R. Jeffrey Smith, “U.S. Special Forces Carried Out Sabotage, Rescues Deep in Iraq,” *The Washington Post*, 4 March 1991. <https://www.washingtonpost.com/archive/politics/1991/03/04/us-special-forces-carried-out-sabotage-rescues-deep-in-iraq/5b3738be-100c-40b2-b550-27be373cb88d/>, accessed 5 November 2021.

13 Leigh Neville, *Special Operations Forces in Iraq* (Oxford: Osprey Publishing, 2008), 26-27.

14 In late 2002, CIA and 10 SFG infiltrated into Kurdistan, into the Harir Valley to develop intelligence and organize and train Peshmerga guerrillas. These teams paved the way for SOF teams when the war started.

15 See Eric V. Larson, Derek Eaton, Brian Nichiporuk and Thomas S. Szayna, *Assessing Irregular Warfare* (Santa Monica, CA: RAND, 2008).

16 For example, British SOF are currently conducting OPs to monitor Russian activity in the Ukraine. Marco Giannangeli, “British SAS soldiers in Ukraine report spike in ceasefire violations,” *Express*, 11 April 2021. <https://www.express.co.uk/news/uk/1421624/russia-ceasefire-ukraine-british-soldiers-violations>, accessed 12 April 2021.

17 If reporting is accurate, Ukrainian Special Forces were utilized to attack Russian lines of communication, which aggravated the Russian logistical problem. In addition, Russia deployed SOF elements to infiltrate Kiev to shape operations for follow-on conventional forces, as well as tasking them with assassinating top Ukrainian political leaders. See Federico Bosari, “Hunting the Invader: Ukraine’s Special Operations Troops,” CEPA, 15 March 2022. <https://cepa.org/hunting-the-invader-ukraines-special-operations-troops/>, accessed 17 April 2022; and Cahal Milmo, “Russian special

NOTES

forces have entered Kyiv to hunt down Ukraine's leaders, says Volodymyr Zelensky," *inews.com.uk*, 25 February 2022. <https://inews.co.uk/news/russia-special-forces-kyiv-ukraine-leaders-mercenaries-behind-lines-1483303>, accessed 17 April 2022.

18 Department of Defense (DoD), *SOF Interagency Reference Guide, Fourth Edition* (Tampa: JSOU, April 2020), c6.

19 DoD, *Irregular Warfare Annex to the National Defense Strategy* (Washington D.C.: DoD, 2020), 5.

Definitions are as follows:

UW is defined as "a broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery."

FID is defined as "Participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security."

CT is defined as "Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals."

COIN is defined "Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes."

Source: DoD, *Department of Defense Dictionary of Military and Associated Terms Joint Publication 1-02* (Washington D.C.; DoD, 2010 as amended through 31 January 2011), 383, 145, 54 & 53.

20 See Insider, "US Green Berets Who've Trained Taiwanese Troops Explain How They Could Fight China and Why the US Keeps Their Mission Secret," *SOFREP*, 26 October 2021. <https://sofrep.com/news/us-green-berets-whove-trained-taiwanese-troops-explain-how-they-could-fight-china-and-why-the-us-keeps-their-mission-secret/>, accessed 28 October 2021; and Dr. Sandor Fabian, "Building and Enabling Urban Resistance Networks in Small Countries - A Crucial Role For U.S. Special Forces In Great Power Competition," *Small Wars Journal*, 11 April 2021. <https://smallwarsjournal.com/jrnl/art/building-and-enabling-urban-resistance-networks-small-countries-crucial-role-us-special>, accessed 12 April 2021.

21 For example, see Tyler Rogoway, "Special Ops Train To Defend Strategic Aleutian Islands Radar Outpost During All-Out War." *The War Zone*, 18 October 2021. <https://www.thedrive.com/the-war-zone/42783/special-ops-train-to-defend-strategic-radar-outpost-in-the-aleutian-islands-during-all-out-war>, accessed 26 October 2021.

22 Ellen Mitchell, "Outcry grows over Russian missile test that hit satellite," *The Hill*, 17 November 2021. <https://www.msn.com/en-ca/news/politics/outcry-grows-over-russian-missile-test-that-hit-satellite/ar-AAQO4K0?ocid=sapphireappshare>, accessed 18 November 2021. This test was in addition to Russian tests of a "non-destructive space-based anti-satellite weapon" in July 2020. At the time, General John Raymond, the head of U.S. Space Command, asserted that the test was "further evidence of Russia's continuing efforts to develop and test space-based systems" and an "example that the threats to U.S. and Allied space systems are real, serious and increasing." *Ibid.*

23 The British have already addressed this issue to some degree by creating a new "Ranger" Regiment and tasking the Royal Marine Commandos to undertake tasks normally given to the SAS and SBS (e.g. COIN, FID) so that the SOF entities can focus on countering "big state adversaries." Larisa Brown, "Military chief reveals secret new role for special forces against China and Russia," *The Times*, 17 July 2021. <https://www.thetimes.co.uk/article/military-chief-reveals-secret-new-role-for-special-forces-against-china-and-russia-hgbdwscg7>, accessed 25 July 2021; and Oliver Trapnell, "UK special forces to take on Russia and China in new covert role - 'Ready to react'," *Express*, 19 July 2021. <https://www.express.co.uk/news/world/1464392/uk-special-forces-russia-china-secret-roel-mission-brigadier-mark-totten-ont>, accessed 19 July 2021.

24 David Martin, "Top military official discloses new details about China's hypersonic test," *CBS News*, 17 November 2021. <https://www.msn.com/en-ca/news/world/top-military-official-discloses-new-details-about-chinas-hypersonic-test/ar-AQMqQG?ocid=sapphireappshare>, accessed 18 November 2021.

25 Directed Energy Weapons is an "umbrella term covering technologies that produce a beam of concentrated electromagnetic energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to disable, damage or destroy adversary equipment, facilities, and personnel." Henry Obering, III, "Directed Energy Weapons Are Real ...And Disruptive," *PRISM*, Vol. 8, No. 3, 37. See also, Prakash Nanda "Face-Off: China's Development of Powerful Directed Energy Weapons (DEWs) Triggers A Global 'Laser War'?" *The Eurasian Times*, 23 November 2021. <https://eurasiatimes.com/face-off-chinas-development-of-powerful-directed-energy-weapons-dews-triggers-a-global-laser-war/undefined>, accessed 22 November 2021; and Abhishek De, "Explained: India has dismissed as 'fake' a report about China's use of 'microwave' weapons," *The Indian Express*, 26 November 2020. <https://indianexpress.com/article/explained/microwave-weapons-india-china-7056441/>, accessed 22 November 2021.

26 Most major actors have developed autonomous systems capable of reconnaissance and offensive operations. For instance, the Russians possess "Kamikaze drones," also known as "loitering munitions" that are totally autonomous that can "find, decide to engage, and engage targets on their own" without the need for human intervention" that can be launched from land or ships. Raymond McConoly, "Russian Navy Ships Get More Powerful with Kamikaze drones," *Naval Post*, 30 October 2021. https://navalpost.com/russian-navy-kamikaze-drones/?fbclid=IwAR3MBQilWkpfao4VvgHBe cPMuMxanYNA-_Pnm478n-DiIqT2lDuc-6LWqo, accessed 2 November 2021. Similarly the U.S. Air Force Research Lab (AFRL) is flying autonomous drones that are capable of navigating uneven, harsh terrain and independently finding and transmitting

target specifics, performing manned-unmanned teaming missions and operating a large number of functions without needing pilot control. These autonomous drones are designed to work in swarms and blanket an area with surveillance, test enemy defences, find targets over high-threat areas and potentially function as munitions to attack specific targets. See Kris Osborn, "Next-Level Autonomy Achieved: Meet the Air Force Avenger Drone. This will allow military personnel to expand the scope of their mission," *The National Interest*, 20 July 2021. <https://nationalinterest.org/blog/buzz/next-level-autonomy-achieved-meet-air-force-avenger-drone-189945>, accessed 20 July 2021; and Paul McLeary, "Navy, Marines Push Plans to Transform How they Fight," *Breaking Defense*, 16 April 2021. <https://breakingdefense.com/2021/04/navy-and-marine-corps-push-plans-to-transform-how-they-fight/>, accessed 20 April 2021. A final example is Britain that has tested operating swarms of drones underwater, on the sea and in the air. They have tested drones to conduct tactical re-supply as well as for reconnaissance and acquiring enemy targets. Ben Mitchell, Shane Jarvis and Max Channon, "Royal Marines Commandos operate 'drone swarms' in a first for Britain's armed forces," *WalesOnline*, 17 July 2021. <https://www.walesonline.co.uk/news/uk-news/royal-marines-commandos-operate-drone-21076315>, accessed 19 July 2021.

27 Christian Brose, "The New Revolution in Military Affairs," *Foreign Affairs*, 16 April 2019. <https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs>, accessed 25 April 2019. Notably, even Iran's Islamic Revolutionary Guard Corps (IRGC) has long-range ballistic missiles that travel 1,800 km and hit their designated targets. Maziar Motamedi, "Iran's Revolutionary Guard tests long-range missiles, drones," *Al Jazeera*, 16 January 2021. <https://www.aljazeera.com/news/2021/1/16/iran-revolutionary-guards-test-long-range-missiles-drones>, accessed 18 January 2021.

28 Brose, "The New Revolution...".

29 Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone," *JFQ*, Issue 97, 2020, 14.

30 For example, China has already developed a motor-powered exoskeleton that can carry ammunition boxes weighing 50 kg. The light-weight exoskeleton suit, known as the portable ammunition support assist system for individual soldiers, can provide 20 kg of assisted strength to its user, relieve more than 50 percent of the burden and greatly reduce risks of waist injury. It takes less than 40 seconds to put on the suit and take it off. The suit's motor gives a reacting force to its user every time the user gets up after bending over, so the user can get up faster with less effort. Optional hooks can be used when carrying ammunition boxes, and they can not only help the user with a better grasp, but also give assisted strength. With the help of the exoskeleton suit, one person can carry ammunition boxes weighing 50 kg without much effort, and two people can carry more than 75 kg with ease. "Powered Exoskeleton to Help Chinese Soldiers Carry 50 kg Ammunition," *DefenseWorld.net*, 13 January 2021. https://www.defenseworld.net/news/28751/Powered_Exoskeleton_to_Help_Chinese_Soldiers_Carry_50_kg_Ammunition#.YACNVzmSmUm, accessed 14 January 2021.

31 Chris Dougherty, *More than Half the Battle. Information and Command in a New American Way of War* (Washington D.C.: Centre for a New American Security, 2021), 4.

NOTES

- 32 Richard Uber, "Penetrating Artificial Intelligence enhanced Anti Access / Area Denial," *Journal of Indo-Pacific Affairs*, Winter 2020, 57.
- 33 Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War. The Coming Age of Post-Truth Geopolitics," *Foreign Affairs*, January/February 2019. <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war>, accessed 9 February 2021.
- 34 Kris Osborn, "Special Forces Can Conduct Undersea Ops Without Making a Sound. You'll never hear them coming," *The National Interest*, 8 July 2021. <https://nationalinterest.org/blog/buzz/special-forces-can-conduct-undersea-ops-without-making-sound-189314>, accessed 8 July 2021.
- 35 United Kingdom. *Strategic Trends Programme. Future Character of Conflict* (London: MoD, ND), 2.

INDEX

A

- Advanced Force Operations (AFO) 18, 19, 114, 115, 117, 131
- Afghanistan 2, 19, 37, 63, 66, 69, 70, 89, 91, 103, 128, 133
- amphetamines 69
- anabolic steroids 69
- Artificial Intelligence (AI) 8, 56, 57, 64, 79, 80, 84, 86, 107, 118-122, 151 *notes*, 161 *notes*
- asymmetric 74, 76, 77, 91, 116, 148 *notes*
- Athar, Sohaib 10
- Australian Special Air Service Regiment (SASR) 27, 132
- autonomous weapons 12, 79, 84

B

- Babbitt, Colonel Joel 85, 86
- battle damage assessment (BDA) 28, 30, 114, 115, 131
- Billiere, General Sir Peter De La 111, 156 *notes*
- bin Laden, Osama 10, 135 *notes*
- biotechnology 79, 82
- Bourne Principle 96, 99, 103
- break-in 13-15, 17-21, 23-27, 29, 31-33, 56, 114, 117

C

- Cabanatuan, raid 15, 39, 41, 42, 46
- Canadian Special Operations Forces Command (CANSOFCOM) iii, 36, 38, 55, 127-129, 131, 138 *notes*, 141 *notes*, 146 *notes*
- Canadian Special Operations Regiment 93
- Chemical, Biological, Radiological, Nuclear (CBRN) 115, 117, 118, 120, 131
- China 1, 3, 8, 10, 13, 50-52, 54, 56, 60, 74, 120, 135 *notes*, 136 *notes*, 139 *notes*, 140 *notes*, 155 *notes*, 158-160 *notes*
- Clausewitz 64, 87, 109
- Cochlear implants 69, 148 *notes*
- cognitive plane 77, 78, 150 *notes*
- Cold War 7, 51, 61
- Command, Control, Communications and Computers (C4) 118, 119, 131
- conventional warfare 7, 9, 75, 134 *notes*
- Counter-Insurgency (COIN) 37, 89, 109, 114, 116, 123, 125, 131, 153 *notes*, 158 *notes*, 159 *notes*
- Counter-Proliferation 2
- Counter-Terrorism (CT) 2, 33, 37, 50, 51, 54, 56, 59, 88-90, 99, 108, 114, 116, 123, 125, 128, 131, 158 *notes*
- counter-unmanned aircraft system (C-UAS) 82
- Crimea 3, 51, 53, 61, 64, 74, 75

INDEX

culture, SOF 16, 88, 104-106

cyber warfare 73, 75, 77

cyberspace 14, 76, 150 *notes*

D

Darwin/Goose Green, Falkland Islands
24, 25

decision cycles 77, 119

deep fakes 64, 112

Delta Force 27

direct action 15, 18, 19, 27, 31, 38, 50,
54, 62, 110-115, 117

directed energy (DE) weapons 79, 82,
120, 159 *notes*

disinformation 24, 26, 63, 122, 123, 161 *notes*

Donbas 30, 75

Douhet, Giulio 65

drones 56, 60, 68, 120, 147 *notes*, 155 *notes*,
159 *notes*, 160 *notes*

E

economic war 75, 77

exoskeleton 68, 69, 70, 121, 148 *notes*,
160 *notes*

extremism 2, 76

F

F-35 Lightning II 8

Falkland Islands War 23, 38

Federal Republic of Yugoslavia (FRY) 22,
28, 131

Fifth Army (U.S.) 35

First Gulf War 108, 111

First United States Army Group (FUSAG)
26, 131

Foreign Internal Defense (FID) 116, 117,
131, 158 *notes*, 159 *notes*

Franks, Tommy, General 19

future operating environment (FOE) 4,
12, 38, 39, 41, 50, 52, 59-61, 83, 131

G

Gerasimov, General Valery (Russia) 9, 11,
14, 75, 135 *notes*, 136 *notes*, 149 *notes*,
150 *notes*

glide vehicles 81, 107

Global War on Terrorism (GWOT) 88-90,
104, 131, 154 *notes*

Gulf War, 1991 29, 39, 46, 79

H

high-intensity war 3, 59, 87, 89, 96, 101-
103, 107-109, 114, 116, 119, 122, 125

Ho Chi Minh trail 68, 146 *notes*

horizontal escalation 61, 114, 116

Horn, Bernd iii, 12, 107, 127, 133 *notes*,
134 *notes*, 136 *notes*, 139 *notes*, 140 *notes*,
156 *notes*

Howard, Michael 125

human infrastructure 94, 95

human performance augmentation 15, 59,
68, 70

Hussein, Saddam 27, 46, 47, 112, 113,
137 *notes*, 146 *notes*

INDEX

- Hybrid-Electric Drive (HED) 83, 131, 152 *notes*
- hybrid-electric technology 79, 83, 84, 86
- Hyper-Enabled Operator (HEO) 84, 131, 150 *notes*, 152 *notes*
- hypersonic missiles
- Zircon (Russian) 8
 - DF-17 (Chinese) 8
- hypersonic weapons 9, 79, 81, 151 *notes*
- I**
- Indo-Pacific Theatre 121
- influence activities 119, 122
- Intelligence, Surveillance, and Reconnaissance (ISR) 22, 23, 29, 79, 92, 114, 115, 131
- invasion of Iraq (*see also* Second Gulf War) 27, 28, 112
- Iran 28-30, 47, 50, 51, 57, 139 *notes*, 145 *notes*, 147 *notes*, 154 *notes*
- Iraq 19, 27, 28, 37, 46-49, 53, 64, 66, 69, 70, 89, 103, 108, 112, 113, 128, 133 *notes*, 137 *notes*, 139 *notes*, 149 *notes*, 157 *notes*
- irregular warfare 53, 76, 114, 116, 117, 122, 128, 146 *notes*, 157 *notes*, 158 *notes*
- Islamic State of Iraq and Syria (ISIS) 64
- Israeli SOF 17, 19
- J**
- Joint All Domain Operations (JADO) 9, 132, 135 *notes*
- Joint Force 3, 5, 17, 21, 22, 29, 31, 32, 56, 89, 115, 116, 118, 119, 122, 124, 137-139 *notes*
- Joint Forcible Entry Operations 13, 136 *notes*, 137 *notes*,
- Joint Special Operations University (JSOU) iii, 53, 127, 128, 132, 134 *notes*, 141 *notes*, 145 *notes*, 146 *notes*, 153-155 *notes*, 158 *notes*
- Joint Terminal Attack Controller (JTAC) 48, 111, 112, 115, 132
- Joint Theatre Entry 13, 136 *notes*, 137 *notes*
- Joint Vision 2020 (U.S.) 9
- K**
- Kaliningrad 21
- Kiselev, Valeriy 11
- Krueger, Lieutenant General Walter 40
- L**
- legal warfare 75, 77
- Lethal Autonomous Weapon Systems (LAWS) 80, 81, 132, 151 *notes*
- Libya 75
- light tactical all-terrain vehicles (LTATV) 85
- logistics 8, 15, 59, 61, 62, 65, 67, 68, 70, 79, 81, 85, 148 *notes*
- M**
- MacCalman, Alex 84, 85, 150 *notes*, 152 *notes*

INDEX

media 8, 10, 15, 59-65, 123, 134 *notes*,
135 *notes*, 147 *notes*, 152 *notes*

microwave weapons 159 *notes*

mobility 67, 83, 94, 103, 118, 120, 150
notes

moral plane 76, 77

multi-domain operations 77, 153 *notes*

N

National Security Strategy (U.S.) (NSS) 1,
50, 129, 132, 133 *notes*, 145 *notes*

neuroprosthetics 69, 148 *notes*

non-state actors 4, 50, 76, 77, 127

nootropic drugs 69

Normandy 25, 26

North Atlantic Treaty Organization
(NATO) 2, 7, 13, 15, 22, 28, 29, 53, 60,
75, 112, 132, 133 *notes*, 138 *notes*, 139
notes, 155 *notes*

North Korea 50, 144 *notes*, 145 *notes*

Norwegian Independence Company 42, 43

O

Ogarkov, Nikolay 11, 136 *notes*

OODA Loop 84

operation

Bodyguard 25, 26

Desert Storm 9, 15, 67, 157 *notes*

Iraqi Freedom 19, 67

Freshman 43

Gunnarside 42-45

Mikado 11, 156 *notes*

Paraquat 110

P

Pebble Island 110

People's Liberation Army, Chinese 8, 9,
21, 27, 30, 132

performance enhancing drug (PED) 70

Persian Gulf 111, 112, 143 *notes*, 157 *notes*

private military contractors 75

private military corporation (PMC) 60,
132

psychological operations (Psyops) 63-65,
115, 117, 132

Q

quantum technology 79, 82

Quds Force (Iran) 53, 93

R

Ranger Regiment (U.S.) 92

recruiting 64, 95, 100-102

Resistance Operating Concept 53, 90,
134 *notes*, 146 *notes*, 153 *notes*

risk 2, 4, 9-12, 15, 16, 20-25, 27, 29, 30,
33, 37, 39, 49, 55-57, 59, 61-63, 70, 81,
92, 107, 108, 116-118, 122, 136 *notes*,
156 *notes*

risk acceptance 16, 118, 122

Rumaylah Oilfields 113

INDEX

- Russia 1, 3, 13, 20, 30, 50-52, 54, 56, 60, 64, 74, 140 *notes*, 146 *notes*, 149 *notes*, 155 *notes*, 157-159 *notes*
- S**
- sabotage 3, 42, 44, 45, 50, 52, 53, 55, 98, 104, 107, 110, 114, 116, 128, 134 *notes*, 142 *notes*, 157 *notes*, 158 *notes*
- San Carlos, Falkland Islands 24, 25, 111
- satellites 108, 119-121
- SCUD missile(s) 19, 47, 112
- SEALs (U.S. Navy) 87, 93, 112
- Second Gulf War (*see also* Invasion of Iraq) 112
- Second Nagorno-Karabakh War 60
- Second World War (*see also* World War II) 15, 25, 73, 111, 114, 122, 139 *notes*
- Selous Scouts (Rhodesian) 92
- Sensitive Site Exploitation (SSE) 113, 117, 132
- sensors 19, 21, 23-25, 29, 31, 48, 49, 60, 65, 84, 107, 114, 118, 120, 122, 148 *notes*
- Short-Range Air Defence (SHORAD) 82, 132
- social credit system (China) 135 *notes*, 136 *notes*
- social media 10, 15, 59-65, 70, 123, 147 *notes*
- social media attacks 62, 64, 65
- South Georgia Island 110, 156 *notes*
- Soviet Union 7, 51, 108
- space 3, 4, 8, 14, 75, 76, 77, 95, 103, 119-121, 128, 134 *notes*, 151 *notes*, 159 *notes*
- Special Air Service (SAS) 23-25, 27, 28, 48, 49, 87, 109-111, 132, 138 *notes*, 144 *notes*, 146 *notes*, 156 *notes*, 157 *notes*, 159 *notes*
- Special Boat Service (SBS) 23, 24, 28, 109, 110, 111, 132, 159 *notes*
- Special Forces (SF) 18, 21, 28, 30, 93, 109, 111, 128, 132, 137 *notes*, 138 *notes*, 140 *notes*, 141 *notes*, 149 *notes*, 152 *notes*, 154-159 *notes*, 161 *notes*
- Special Operations Command North (SOCNORTH) 134 *notes*
- Special Operations Executive (SOE) 42, 43, 45, 132
- special reconnaissance 15, 21, 54, 62, 111-115, 117, 138 *notes*
- sustainment infrastructure 94, 95
- swarming 80, 120
- T**
- talent management 100, 102, 103, 106
- tempo 8, 9, 11, 18, 27, 33, 41, 50, 55, 57, 102, 107, 118, 119, 121, 123-125
- time management 96, 97, 100, 102
- training
- collective 98, 99
 - entry-level 100, 101
 - individual 98, 99, 102
 - individual-collective 98, 99
 - joint 99

INDEX

training management 98, 99, 100, 102,
106

Trenchard, Hugh 65

U

Ukraine iii, 10, 18, 30, 51, 53, 54, 64, 74,
75, 108, 120, 135 *notes*, 146 *notes*, 150
notes, 155 *notes*, 157 *notes*

Umm Qasr 113

unconventional warfare (UW) 3, 38, 50,
51, 53, 62, 78, 111, 113, 114, 116, 117,
132, 145 *notes*, 157 *notes*, 158 *notes*

V

Vemork, heavy water plant, Norway 39,
42, 43, 46, 57

W

wargames 121, 122,

weapons of mass destruction (WMD) 46,
50, 113, 132

William Mitchell 65

World War II (*see also* Second World
War) 35, 39, 42, 128

CANSOFCOM ERC BOOKS

Special Operations Forces: A National Capability

Dr. Emily Spencer, ed., 2011

Special Operations Forces: Building Global Partnerships

Dr. Emily Spencer, ed., 2012

“By, With, Through.” A SOF Global Engagement Strategy

Dr. Emily Spencer, ed., 2014

In Pursuit of Excellence. SOF Leadership in the Contemporary Operating Environment

Dr. Emily Spencer, ed., 2017

The Birth of the Ranger Tradition. Irregular Warfare During the Lake Champlain Theatre of Operations, 1754-1760. A Battlefield Study Guide

Colonel (retired) Bernd Horn, PhD, 2017.

Thinking for Impact: A Practical Guide for Special Operations Forces

Dr. Emily Spencer, 2018

“We Will Find A Way.” The Canadian Special Operations Legacy

Colonel (retired) Horn, PhD, 2018.

Now Set Europe Aflame! The SOE and the Canadian Connection

Colonel (retired) Bernd Horn, PhD, 2019.

Risk & Decision-Making

Colonel (retired) Bernd Horn, PhD, ed., 2019.

Risk: SOF Case Studies

Colonel (retired) Bernd Horn, PhD, ed., 2020.

The (In)Visible Hand: Strategic Sabotage Case Studies

Colonel (retired) Bernd Horn, Dr. James Kiras and Dr. Emily Spencer, 2021



Up until the February 2022 Russian invasion of Ukraine, the idea of a quickly manifesting high-intensity war was unfathomable to most. Awareness of how such a conflict would severely impact the stability and prosperity of the interconnected world, as well as the accessibility, proliferation, and lethality of modern technology, seemed to make the prospect of conflict so devastating that no rational state would risk engaging in all out war. However, the Russian assault on Ukraine underlines the point “never say never.” Through design or miscalculation, the occurrence of a major conflict between peer, near-peer, and/or regional powers can never be discounted. As such, this volume examines the challenges and potential roles that SOF will face in the event of high-intensity, conventional warfare.



ISBN 78-0-660-43779-8