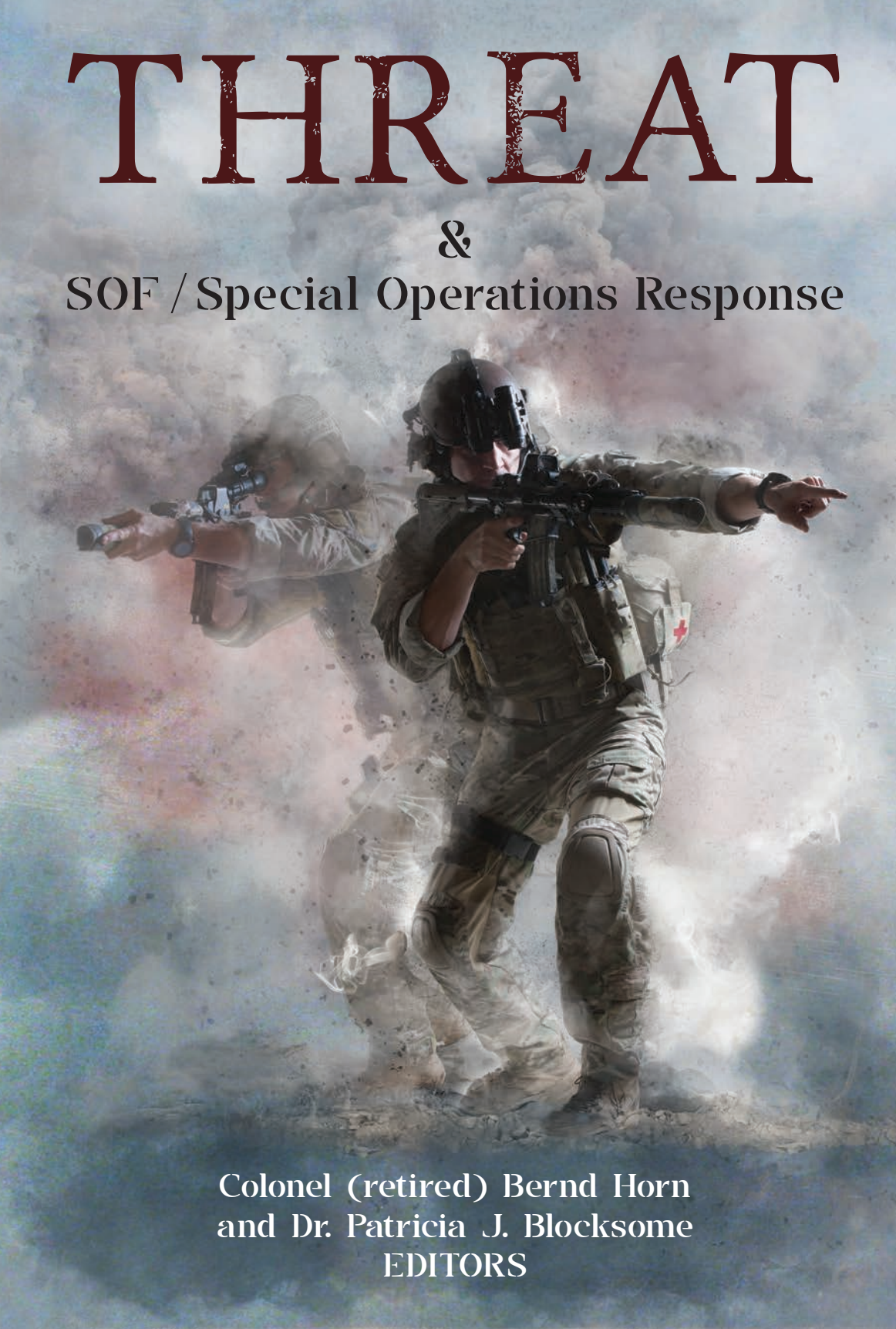
THREAT

&

SOF / Special Operations Response



Colonel (retired) Bernd Horn
and Dr. Patricia J. Blocksome
EDITORS

THREAT
&
SOF / Special Operations Response

Colonel (retired) Bernd Horn, PhD
and
Dr. Patricia J. Blocksome
EDITORS

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.
WPO32319

FRONT COVER: Artwork by Silvia Pecota
BACK COVER: "Cleared Hot" by Silvia Pecota

SECTION DIVIDERS:
PART I – "Landing by Moonlight" by Silvia Pecota
PART II – AI Generated artwork by Major Patrick Foley
PART III – "Cleared Hot" by Silvia Pecota

THREAT & SOF / SPECIAL OPERATIONS RESPONSE

CANSOFCOM Education & Research Centre

ISBN 978-0-660-69366-8 (print)
978-0-660-69365-1 (PDF)

Government of Canada Catalogue Number D2-474/2024E (print)
Government of Canada Catalogue Number D2-474/2024E-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 commands, units or organizations, the United States Government, United States Department of Defense, or any of its subordinate commands, units or organizations, or the editors.

TABLE OF CONTENTS

FOREWORD

What role will special operations forces (SOF) play in an emerging era in which the great-power competition expands the number of major participants from the two that dominated the Cold War – the United States and the Soviet Union – to three, with China now joining the top ranks? Like the Cold War, this era will also see the high-level competition being played out through various parts of the world, and with a fresh new energy from the non-state actors who have discovered the power that can be accessed via organizational networking. Thus, the 21st century "Great Game" will be conducted vigorously on three levels: directly among the leading powers; for influence and strategic gains in other nations ranging across the world; and with significant roles for non-state actors, from terrorist networks to private military companies. Back in 1991, a conference at the U.S. Army War College concluded that, in the wake of the dissolution of the Soviet Union, the world was going to see greater "volatility, uncertainty, complexity, and ambiguity" (VUCA).[1] Well, we know today that the Russians are definitely back, China has risen, and terrorist, insurgent, criminal, and hacker networks are posing all sorts of vexing new problems. In short, if the 1990s were the decade of VUCA, the 2020s are turning out to be a time that can only be viewed as "VUCA-squared."

This insightful volume provides a number of ways to answer the question about the utility of SOF in this challenging time. Beginning with chapters that track the evolution of SOF in the modern era and analyze the discourse about ways in which military elites may be best used, the volume then systematically examines emergent threats and potential SOF-based responses. It is especially noteworthy that the contributors first "look back" before peering ahead. SOF actions in World War II, Korea, Vietnam and other engagements receive their due, with one entire chapter devoted to the unconventional warfare activities of the "Jedburgh" teams that played important roles in support of D-Day and the Allied campaign to liberate France and the Low Countries. The rise of elite counter-terrorist units catalyzed by the tragedy at the 1972 Munich Olympics also receives close, careful attention.

As do the various irregular "threats" that the book considers. Prominent among them are China's employment of a wide range of cyber, space-based, and influence operations against Taiwan and its use of maritime militias both to expand its control of disputed seas and to prepare for their use in a future naval conflict. Russia's use of the Wagner Group, not as cannon fodder in Ukraine but in its more effective employment as a low-cost, high-leverage means of gaining influence in Africa, receives detailed treatment as well. As does the matter of economic-based statecraft manifested in terms of gaining control of corporate "beachheads" in critical areas – a particularly disturbing threat masquerading as "just business."

The final section of this excellent anthology consists of chapters focused on how SOF will be able to respond to the key threats now emerging. At a conceptual level, as one incisive chapter argues, the small size of SOF units and their continual exposure to what the author describes as "combat Darwinism," make for supple operators and the severe environments in which innovations are needed – and are more likely to be introduced and sustained. The chapters that follow in this last part of the book bear out belief in the laboratory-like ability of SOF to experiment and innovate. One particularly creative notion is for SOF to focus on gaining deep understanding of the social movements – active or latent – that may be mobilized and put to effective use in SOF's areas of responsibility. Doing this can help SOF improve the resilience of a society under external threat or, conversely, undermine the seeming stability of a potential aggressor. This approach may not fall under the rubric of "combat Darwinism," but it hearkens to an important "conceptual innovation."

Another area in which innovation is important is the organizational domain. In the chapter on cyber operations, a strong case is made that SOF should have organic capabilities for operating in cyberspace. Using the example of how the U.S. responded to the 1981 Iran hostage rescue debacle by developing dedicated special operations aviation assets to improve tactical mobility, strike, and related functions, the author argues that, before yet another disaster occurs, SOF should develop organic capabilities for moving skillfully in and striking from cyberspace.

Above all, this volume argues against "conventionalization" of the approach to grappling with the problems posed by the new era of great-power competition. One key chapter points out, for example, that if space-based communications and sensing systems are disrupted, senior leaders are likely to choose "a dangerous retrenchment into safe [i.e., conventional or closely conventional-related] mission sets with outdated technology." This decision could have profoundly deleterious effects for SOF effectiveness. Thankfully, the authors point to alternative designs for space-based support in the face of disruptive adversary operations. The remedies they suggest will no doubt prove useful to the "remote warfare" paradigm – which aims largely at the use of SOF to enhance the capabilities of local partners – considered in another chapter. A crucial goal the author considers is to reduce the information advantage that insurgents generally have over the governments they are attacking, so secure, available communications and intelligence will go a long way toward rebalancing, perhaps reversing, the informational scales, with operational results.

The anthology concludes by making a forceful case for the utility of special operations forces, emphasizing, among their other attributes: a high state of readiness for taking swift action; skill in the blurry situations that may lie between peace and war; and cultural attunement that facilitates both alignment with and improvement of local allies. One can only hope that, in this troubled new era, SOF will be seen as not only offering more usable options, but also more effective ones.

In closing, I would simply add that the contributing editors, Bernd Horn and Patricia "Misha" Blocksome, have brought together a formidable, international military and civilian team. The anthology's many innovative insights will provide strategic guideposts for the challenging times – sure to be complex and confusing – that are unfolding before our eyes. I am reminded of Winston Churchill's thoughts about future challenges as he pondered them soon after the great Allied victory over the Axis Powers. He was aware that the end of one challenge simply signaled the rise of the next when he wrote in the preface to his history of World War II:

> The human tragedy reaches its climax in the fact that after all the exertions and sacrifices of hundreds of millions of people and of the victories of the Righteous Cause, we have still not found Peace or Security, and that we lie in the grip of even worse perils than those we have surmounted.[2]

A similar sentiment was expressed long ages ago by the unknown Saxon author of *Beowulf,* who noted that victory over Grendel was short-lived, for an even deadlier threat soon arose in the form of the monster's enraged, more powerful mother. So, like Beowulf, we too must now gird up after victories in the Cold War and against al-Qaeda and ISIS, ready to master the even greater dangers looming up ahead.

John Arquilla ***Monterey, California***
Fall 2023

INTRODUCTION

COLONEL (RETIRED) BERND HORN &
DR. PATRICIA J. BLOCKSOME

The international security environment has always been dynamic. States have had to deal with known threats, as well as Black Swan events that were unanticipated and caught international actors by surprise and unprepared. Although state actors are normally diligent in attempting to identify, anticipate and react accordingly to threats, there are a multitude of unknowns. In addition, not all threats are equal.

A threat in this national security context is defined as state or non-state actor actions that can cause disruption, damage and potential ruin of another state's national security, economic, defence and political stability and/or sovereignty. Threats must be assessed against an adversary's intent, opportunity and capability. Clearly assessment is as much art as it is science and must be considered within the context of an ambiguous, dynamic and extremely complex security environment.

Response to threat(s) must be calibrated accordingly. Importantly, response need not be reactive. Rather, to be most effective response should be proactive so that potential menace can be deterred, disrupted or destroyed before it can negatively impact the intended target. Such proactive responses, however, are predicated on understanding current and emerging threats and how they might impact state and non-state actors. Therefore, assessment is a critical first step in developing a successful threat response. Responses to threats must also take into consideration one's own intent, opportunities, and capabilities, as well as escalation risks.

Special Operations Forces (SOF) and Special Operations (SO) have always been an effective means of responding to threats. Due to their character and nature, SOF and SO can provide unique opportunities and capabilities for

proactive threat responses that can meet policy-makers' intent. Consequently, the ways in which SOF can respond to the contemporary dynamic security environment deserve consideration.

SOF, from their modern inception at the start of World War II (WWII), are defined as "designated active or reserve component forces of national military services specifically organized, trained, and equipped to conduct and support special operations."[1] Special operations for the purpose of this volume are defined as "Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk."[2]

Notably, not all special operations are conducted by forces designated as SOF. In the current security environment activities such as cyber warfare and information operations, to name only two, have a major impact on influencing adversaries. These activities are not necessarily conducted by forces recognized as SOF. Nonetheless, the deployment of SOF and the application of SO have historically proven to be an effective means of dealing with threat both reactively, as well as proactively.

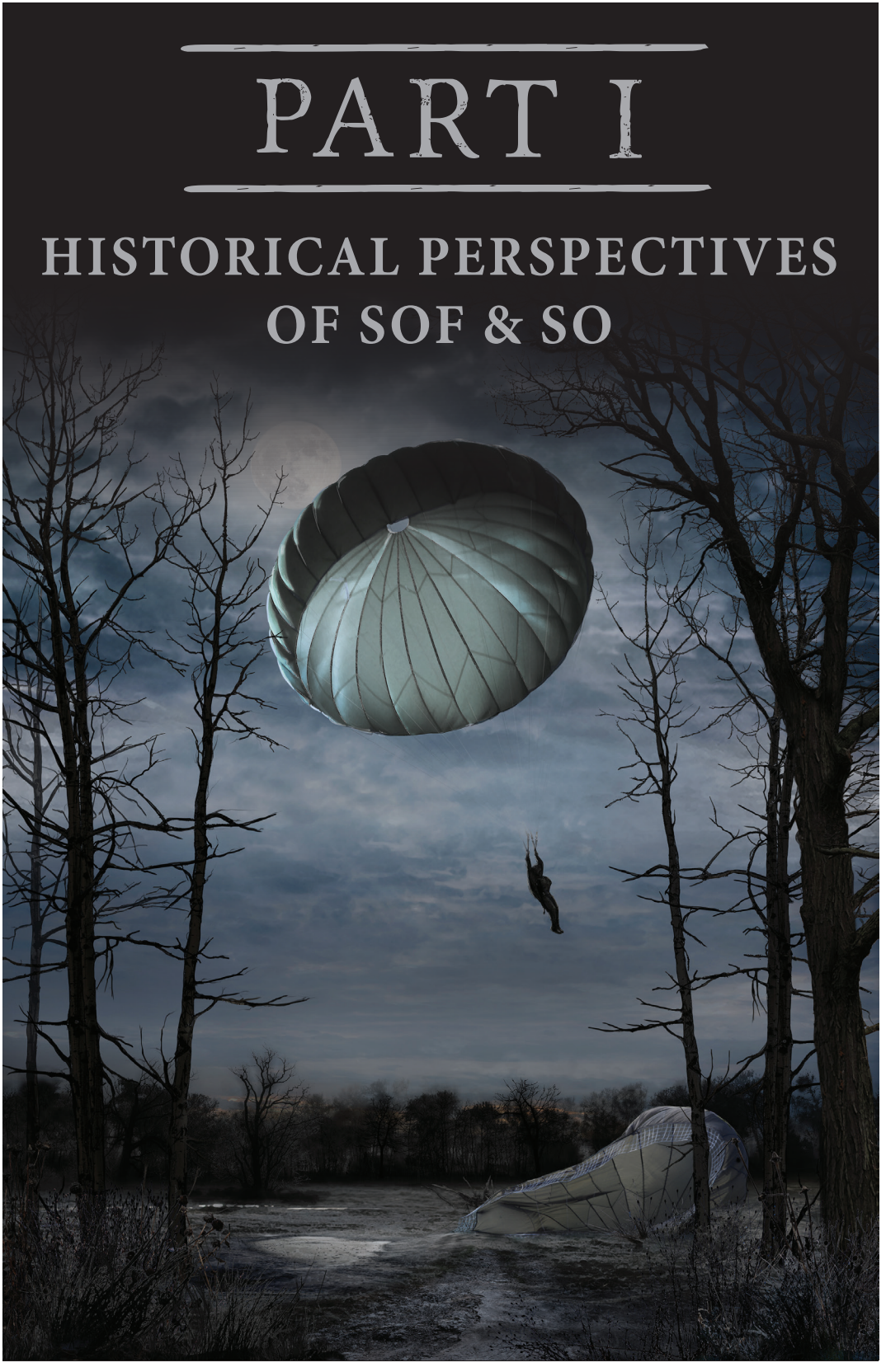
This volume examines the concept of threat in the current and emerging security environment and the potential and necessary SOF/SO responses. Part I presents historical background through an overview of SOF/SO evolution and doctrinal development, as well as a series of case studies in the contemporary setting to demonstrate how both have been used to respond to threat. Part II analyzes the concept of threat from a macro perspective of "below the threshold of armed conflict" to more specific threats. Finally, Part III examines potential SOF/SO responses to the myriad of existing and emerging threats that face partner nations.

This publication is neither meant to be a prescriptive solution, nor a silver bullet. Rather, it is designed to provide awareness and food for thought, discussion,

and application where applicable. In order to mitigate threats and strategic surprise, it is always prudent to anticipate, adapt and change as necessary to meet the dynamic international security environment. This volume is intended to assist with that process as those overseeing current SOF/SO look toward the future.

PART I

HISTORICAL PERSPECTIVES OF SOF & SO



CHAPTER

1

BORN FROM WEAKNESS: THE EVOLUTION OF SOF AND THE RISE OF SPECIAL OPERATIONS

COLONEL (RETIRED) BERND HORN

The identification and assessment of threat defined as actions that can cause disruption, damage and potential ruin of another state's national security, economic, defence and political stability and/or sovereignty, is normally at the forefront of the focus of states. As such, their military, security and intelligence apparatus are tasked, trained and equipped to deal with these threats. However, a failure to properly identify threat, surprise or unexpected "Black Swan" events or simply being overwhelmed by an opponent, creates gaps and shortcomings that endanger a state's ability to conduct itself as it desires.

Despite widespread historical institutional resistance and animosity, Special Operations Forces (SOF) and special operations (SO) have proven over time to be an effective foil to deter, disrupt and destroy real and/or emerging threats. World War II (WWII) demonstrated the value of SOF and SO. The Allies flush with victory at the end of World War I emplaced conditions on the militaristic Germany to eradicate the threat it had historically represented. Their failure, however, to adjust their outlook and approach to war led to a catastrophic failure, which led to the collapse of several Allied nations and the threat of a German invasion of England. From this state of utter weakness, modern SOF was born to fill a gap and mitigate the looming threat hanging over the Allies.

Over the following decades, although SOF remained a pariah to the greater military institution for much of that time, they continued to provide solutions to threats that were underestimated, misunderstood or simply outside of conventional capability. In the post-war period SOF became a counter-insurgency (COIN) force during the brush fire wars and insurgencies of the late-forties to mid-seventies. When widespread terrorism erupted in the West in the seventies, SOF became the pre-eminent counterterrorism (CT) force. The complex nature of the CT role necessitated SOF not only filling "a gap" but taking on the task as a core mission. In the aftermath of the terrorist attack on the Twin Towers in New York on September 11, 2001 (9/11), SOF were universally seen as the premiere CT/COIN force. Operations in Afghanistan, Iraq and elsewhere quickly earned it the title of "Force of Choice."

WORLD WAR II – THE BEGINNING

The speed and violence of the German invasion of Western Europe in the spring of 1940, caught the Allies still mired in their Great War mentality totally by surprise. The destruction of the West took forty-six days, but it was decided in only ten. With their backs to the sea, the British launched Operation Dynamo utilizing virtually any craft that could float. Between May 27th and June 4th, despite the German pressure, 338,226 personnel were evacuated from Dunkirk. But the cost was enormous.[1]

The frantic withdrawal resulted in the loss of virtually all Allied heavy equipment, weapons, and transport. The military expressed the stark reality of the shortage of arms to the British War Cabinet. The political leadership was informed that there were fewer than 600,000 rifles and only 12,000 Bren guns in the whole of the United Kingdom.[2] Britain, now braced for what seemed to be the inevitable conclusion to the German master plan – the invasion of England.

The British military high command, overwhelmed by the task that they faced, saw only a defensive battle in the short term. The threat of the German juggernaut was such that they argued that there were only two viable forms of offensive action, namely the traditional economic blockade utilizing the

superiority of the Royal Navy (RN) on the high seas and strategic bombing conducted by the Royal Air Force (RAF).

This response to the looming threat was not accepted by all. Importantly, on June 4, 1940, Winston Churchill was appointed prime minister. Churchill realized that threat had to be met face-on. Only through offensive action could a nation provide its military and citizens with the necessary confidence and morale to sustain a war effort. On the same day he was appointed prime minister he declared in the House of Commons, "we shall not be content with a defensive war."[3] That afternoon, he penned a note to his Chief of Staff of the War Cabinet Secretariat, General Hastings "Pug" Ismay. "We are greatly concerned," he wrote, "with the dangers of the German landing in England." He pondered rhetorically, "why should it be thought impossible for us to do anything of the same kind to them?" He then added, "We should immediately set to work to organize self-contained, thoroughly-equipped raiding units."[4] Churchill knew intuitively that threat had to be confronted and turned against the opponent. Winning a war meant maintaining the initiative. As such, Churchill mused, "how wonderful it would be if the Germans could be made to wonder where they were going to be struck next, instead of forcing us to try to wall in the island and roof it over!"[5]

Two days later, Churchill sent additional direction to Ismay. He explained:

> Enterprises must be prepared with specially trained troops of the hunter class who can develop a reign of terror down these coasts, first of all on the "butcher and bolt" policy; but later on, or perhaps as soon as we are organized, we could surprise Calais or Boulogne, kill and capture the Hun garrison, and hold the place until all the preparations to reduce it by siege or heavy storm and been made, and then away. The passive-resistance war, in which we have acquitted ourselves so well, must come to an end. I look to the Joint Chiefs of the Staff to propose me measures for a vigorous, enterprising, a ceaseless offensive against the whole German-occupied coastline.[6]

Notwithstanding the widespread resistance within the military, Ismay passed Churchill's direction to the Chief of the Imperial General Staff (CIGS), General Sir John Dill. The CIGS promptly assigned the task to one of his general staff officers, Lieutenant-Colonel Dudley W. Clarke. Clarke's mission was to propose schemes by which the offensive spirit of the Army could be fostered until it was able to resume the offensive in the conventional manner.

To Clarke the solution was self-evident, it had to be a focus on irregular warfare, specifically special raiding operations. He believed this solution was the optimal concept under the present conditions. Therefore, he proposed that "commandos," the term taken directly from the Boer War experience, be established "trained in 'snatch and grab' night raiding from landing craft."[7] He believed that commandos conducting raids would disrupt the German war effort, destroy valuable resources and divert enemy personnel by requiring forces to be allocated to defend against the raids. Equally as important, the raids would restore the offensive spirit to the British Army.[8]

The CIGS briefed Churchill who took to the idea immediately. After all, it appealed to his character. Despite the ongoing resistance from many senior military commanders who felt that valuable resources were being frittered away for no valuable return at a time when the nation faced invasion, Churchill pressed on. In a remarkable display of military efficiency, by June 8, 1940, General Dill received approval for the creation of the commandos and that same afternoon, Section MO9 of the War Office was established.

Clarke's concept quickly came to life. He now established his "picked bands of guerilla fighters who would harry the long enemy coastline in order to make him [Germans] dissipate his superior resources."[9] He proposed the creation of twelve Commando units consisting of 500 men broken up into a headquarters and ten troops respectively.[10]

The theoretical construct for selection was sound. The nature of commando operations dictated that volunteers were to be the best possible material. As such, initially, officers and men were hand-picked from volunteers. "Great care," revealed one report, "was taken in the selection of officers and men and from

the outset they were specially picked units."[11] Recruiters wanted intelligent, young, exceptionally fit individuals who demonstrated courage, endurance, initiative and resourcefulness, as well as self-reliance and aggressiveness. Marksmanship and the ability to swim were also essential skills required. The selecting officers also tried to pick candidates who were mechanically inclined, able to drive motor vehicles and immune to air or sea sickness.[12]

The men drawn to the Commando idea very quickly coalesced the concept that was expected. Raiding was their primary role. In essence, they were to be trained to be "hard hitting assault troops" who could work in cooperation with the Navy and Air Force. As such, they were expected to capture strong points, destroy enemy services, neutralize coastal batteries and wipe out any designated enemy force by surprise as detailed by higher headquarters.[13] They were also told that they would have to become accustomed to longer hours, more work and less rest than the other members of the armed forces.

Predictably, the concept of commandos attracted a like-minded group of aggressive, action orientated individuals who quickly shaped the essence of the commando idea. Together they forged a "commando spirit" that comprised of determination; enthusiasm and cheerfulness, particularly under adverse conditions; individual initiative and self-reliance; and finally, comradeship.[14]

In December 1940, the castle grounds at Achnacarry became a Holding Unit and a special training centre until December of the following year when it officially became the Commando Depot. Its purpose was to achieve a level of uniformity and concentration in the early stages of a commando recruit's training. Once a commando recruit completed his basic course at the Depot, he was dispatched to the Commando Holding Unit where he underwent further advanced collective and combined arms training prior to being posted to an active commando unit. The standards were unrelenting. Individuals who failed to meet the requisite training requirements were immediately returned to their original units.

At its core, the training was designed to achieve a number of goals. Firstly, it was devised to foster in the commando soldier the offensive spirit – an

ever-present eagerness to "have a go" at the enemy. Secondly, it nurtured the belief that darkness and the night was an aid rather than a deterrent in "closing with and attacking the enemy." Equally important, it developed self-reliance and the ability of the soldier to act, whenever necessary, on his own initiative to accomplish the mission.[15]

The commandos were expected to be able to conduct assault landings before first light to seize and destroy coastal defence batteries or installations, and/or landings in the dark in rough weather and on rocky coasts in areas where defences were deemed to be weaker. They were also responsible for landings under cliffs with scaling operations to strike inshore in locations where the enemy least expected attacks. In addition, commandos were also given the task to penetrate behind the enemy lines either by infiltration in small parties or by landing on the coast from surface craft, submarines, or flying boats to conduct night assaults against headquarters, tank harbours, communications facilities or installations on the enemy's lines of communication, as well as ambushes of enemy forces moving forward to the battle area.

Furthermore, commandos were also tasked with the ability to infiltrate airfield perimeters to destroy aircraft, as well as to conduct raids to obtain identification and other information required on the enemy, or simply to create tension, disruption and anxiety with the enemy defences. Finally, they were also expected to create large scale diversionary raids, by one or two commando units, to induce the enemy to commit his reserves.[16]

Although the commandos began to attract the requisite amount and type of manpower, and despite their high-level sponsor, predictably, they quickly met resistance. "As ever," lamented Brigadier Anthony Farrar-Hockley, "a new concept, a new organization tends to be resisted, even at a peak of crisis in a nation's affairs."[17] Resistance emanated from both the War Office and particularly from operational commanders. Not surprisingly, many felt that the diversion of resources during the critical period of likely invasion was not sound. And even once this threat passed, many still felt that the investment in commandos and raiding was not worth the return.

Furthermore, directors and commanding officers were upset with the prospect of losing some of their best men who invariably volunteered for the special duty. "The resistances of the War Office were obstinate," Churchill whinged, "and increased as the professional ladder was descended." He explained that "the idea that large bands of favoured 'irregulars,' with their unconventional attire and easy-and-free bearing, should throw an implied slur on the efficiency and courage of the Regular battalions was odious to men who had given all their lives to the organised and discipline of permanent units." He added, "The colonels of many of our finest regiments were aggrieved."[18]

Despite opposition from the military chain-of-command the commando concept evolved. Ultimately, commando raids were successful and achieved their aim. They not only raised public morale, but they also forged a record for perseverance and toughness, as well as tactical, and at times, arguably, strategic success.[19] Equally important, in the process, the ground was prepared for the birth, if not near explosion, of other modern SOF. The idea of specially organized and specially trained units, made up of intrepid individuals who reveled in challenging and highly dangerous small unit action that called for innovation, individualism and independent action became more widely accepted, or at least tolerated, in an institution known for its conservatism and traditionalism.

However, this limited, if not conditional acceptance existed largely only at the beginning of the war when the threat to England and the Allies was most dire. During this chaotic period of despair when the threat of invasion and German military expansion seemed imminent, a few desperate men were able to fill a void – an ability to strike out from a position of seeming impotence. And so, special units were raised to meet the threat and cover for weakness, as well as to meet specific needs that conventional forces were seen as too unwieldy or poorly trained to accomplish.

As such, a myriad of other relatively small raiding and reconnaissance units such as the Long Range Desert Group (LRDG), the Special Air Service (SAS), the American Rangers, Phantom, Layforce, the First Special Service Force (FSSF), Popski's Private Army, the Special Boat Service (SBS) and a plethora of

others, as well as such entities as the Special Operations Executive (SOE) and the Office of Strategic Services (OSS), emerged to prop up the war effort until larger conventional forces could crush the German war machine.[20]

These SOF forces achieved great success. They tied down hundreds of thousands of enemy troops for defensive tasks; captured strategic materials such as German Würzburg radar components, enigma encryption equipment and code books; destroyed enemy material (e.g., aircraft, ships, locomotives and railway cars) and infrastructure (e.g., factories, bridges, rail lines); shut down the German atomic weapon program; and raised, trained and equipped, as well as in some instances led, secret armies and resistance networks. In fact, their effect was such that the German Führer, Adolf Hitler, felt compelled to issue the infamous Commando Order on October 18, 1942, which stipulated that any Allied commando or parachutist captured, whether in uniform or not, was to be summarily executed.

These SOF achievements, not surprisingly, garnered some support within the chain-of-command. One official report affirmed, "A force of some 2,000 strong [SOF] operated with such outstanding success that the Supreme Commander circulated reports to all United States theatres of war as an example of what could be achieved."[21] The same study noted, "The following points stand out clearly from the experience gained in operating SAS troops in this war:

a. *The dividends paid by introducing small parties of well trained and thoroughly disciplined regular troops to operate effectively behind the enemy lines can be out of all proportion to the numbers involved;*[22]

b. *That the operations of these uniformed troops are quite distinct from the irregular parties such as SOE, Secret Service or Political parties also introduced behind the enemy lines by dropping from the air; and*

c. *The SAS idea is as yet only in its infancy. The very fact that such operations have already paid dividends with the application of a very small allocation of troops, aircraft and naval craft should encourage us to enlarge the scope of this type of operation in the future.*[23]

The Report ended on a seemingly high point for SOF. It proclaimed, "Our experiences in this war, prove that we shall want SAS troops from the very start of the next war."[24]

Despite the accomplishments of Allied SOF, however, as the tide of the war shifted in 1942, so too did the emphasis of these specialist forces. Direct action raids were marginalized and strategic reconnaissance and unconventional warfare, conducted by the OSS, SOE and the SAS gained in relative importance.

Nonetheless, once the large conventional armies were established in Europe, particularly after the Normandy campaign in the summer of 1944 and the threat diminished, SOF forces overall were largely ignored and forgotten and relegated to the status of "a nuisance to real soldiering." Most conventional generals bridled at the thought of SOF, who were seen as aberrations, if not an embarrassment to professional soldiering. "To the orthodox, traditional soldier," Colonel Aaron Banks, a founding member of U.S. Special Forces, explained, "it [SOF] was something slimy, underhanded, illegal, and ungentlemanly. It did not fit in the honor code of that profession of arms."[25]

Not surprisingly with this prevailing attitude, due to the antipathy of the regular army, most, if not all, SOF organizations were either disbanded or relegated to reserve status at the end of the war.

The post-war era did not provide the war-weary and debt-ridden governments or their publics with a prolonged period of peace and tranquility. The onset of the Cold War in 1948 necessitated the creation of large peacetime standing armies for Western nations. SOF, however, did not figure large in these organizations. However, by 1950, most of the Western nations were in a hot war once again in Korea. And, although General Douglas McArthur refused to allow any "unconventional warfare forces to operate independently in 'his' theatre of operations" in Korea, much like he had done in the Pacific Theatre in the Second World War, very quickly the need for SOF capability became apparent.[26] Therefore, his headquarters had to scramble to develop the capability.

At the time, the Central Intelligence Agency (CIA) was responsible for all covert operations in Korea and they created partisan forces to operate against the enemy, as well as a Special Missions Group that was responsible for raids on the enemy's coastal railway system.[27] However, U.S. Far East Command (FEC) also created the capacity for SOF capability. They developed the Liaison Group from which all subsequent unconventional warfare organizations sprang for the remainder of the war. The initial forays were all intelligence gathering missions. Agents were inserted by parachute and foot deep behind enemy lines to report on Chinese and North Korean movements.

In addition, by 1951 FEC had created the Attrition Warfare Headquarters, which was quickly renamed the Miscellaneous Group, 8086 Army Unit, which was responsible for creating and controlling a large partisan force that was designed as a combat force not just another intelligence gathering body.[28] By the end of the year, FEC created the "Covert, Clandestine, and Related Activities – Korea" (CCRAK) organization to control all unconventional warfare operations in theatre. In addition to special reconnaissance and intelligence gathering and partisan warfare, British Royal Marine commandos and US Underwater Demolition Teams (UDTs) were also deployed to conduct sabotage missions against North Korean infrastructure such as railways, tunnels and harbor complexes.[29]

The U.S. Air Force also created additional capability in the form of the Special Activities Unit Number 1, which was given a series of tasks:

1. provide intelligence operations of a positive nature designated to meet the objectives of the command;

2. perform operations (sabotage, demolition and/or guerrilla) necessary to accomplish destruction of specific objectives;

3. assist allied agencies responsible for providing evasion and escape facilities to downed UN airmen; and

4. coordinate with other allied UN intelligence agencies as required by existing directives.[30]

In addition, they also established a Special Air Missions Detachment that was responsible for inserting agents deep behind enemy lines and resupplying partisan forces. Finally, they also stood up 22nd Crash Rescue Boat Squadron that operated in the waters around North Korea and China rescuing downed pilots shot up over enemy territory, as well as supporting guerrilla operations behind enemy lines.

Aside from the Korean War from 1950-1953, the Cold War also established the specter of two large heavily armed camps facing off in Europe. The fact that the seemingly aggressive and very belligerent Soviet Union maintained a buffer of occupied territories and peoples between itself and the West clearly presented an opportunity for unconventional warfare. This prospect was not lost on some strategic planners and commanders, particularly those with recent OSS and SOE experience and, as a result, SOF capability was once again mobilized, albeit a very small effort due to institutional opposition, to fill this specialized requirement.

As such, the evolutionary process begun in WWII from a primary focus on direct action raids towards special reconnaissance (SR) and unconventional warfare (UW) continued. The British and American examples provide a case in point. At the end of the war, the SAS was transformed into a Territorial Army unit – 21st SAS Regiment (Artists).[31] Their role was to provide lay-back patrols that would stay hidden as the Soviet forces swept by and then report on enemy movements and troop concentrations. The Americans resurrected their SOF capability in the same direction – SR and UW. In April 1952, the US Army created the Psychological Warfare Centre, at Fort Bragg, North Carolina, the name of which was later changed to the Special Warfare Centre. At roughly the same time, the 10th Special Forces Group (SFG) was activated. The following year the bulk of the 10th SFG was deployed to Bad Tölz, West Germany and the soldiers that were left behind in Fort Bragg were reorganized into a new unit, the 77th SFG.[32]

For the troops of the 10th SFG, the officers of which were largely drawn from WWII SOF organizations such as the OSS, Rangers and airborne units, their mission in Europe was extremely sensitive and secret. They were tasked, in

the event of the expected Soviet invasion, with developing and exploiting the resistance potential of the population in those areas behind the enemy lines, namely the Soviet occupied territories. In addition, the Special Forces (SF) teams were also responsible to conduct reconnaissance, and potential sabotage missions on their own as well. In essence, the teams were expected to train and advise resistance movements in the art of guerilla warfare, as well as conduct strategic reconnaissance to locate Soviet headquarters and nuclear weapon installations.[33] But this European focus, set in the context of a high-intensity conventional war akin to that of WWII, was somewhat misplaced. Indeed, the nature of conflict took on a completely different face.

During the Cold War, wars of nationalism and communist insurgency, two concepts that were often not always properly delineated by the West, ushered in a period frequently referred to as the savage wars of peace. Once again, the complex nature of such conflicts, which were of long duration, and that required political and not simply military solutions, and that were normally conducted in complex terrain that provided cover, concealment and protection for the less heavily armed and equipped insurgents overwhelmed the conventional capability. Regular soldiers were often unaccustomed to operating in hostile environments for prolonged periods of time. In addition, they had neither the training, nor the innovative, adaptable tactics or agility of thought to counter and defeat elusive, wily insurgents.

To the British this lack of capability became evident during the Malaya Emergency from 1948 to 1960. The immediate unwieldy, unsophisticated and limited response of conventional forces failed to destroy the guerillas or increase the level of security within the country. Although they succeeded in killing some insurgents they just as often alienated segments of the population through heavy-handedness. More importantly, the regular forces were incapable of operating in the austere and hostile jungles for any length of time. As a result, they failed to deny sanctuary and breeding grounds to the guerillas. Fortuitously, a recognized expert, Major "Mad" Mike Calvert, a former commando, Chindit battalion commander and wartime 2 SAS Brigade Commander, was summoned to investigate the problem and devise a solution. Not surprisingly, he recommended the establishment of a special unit, the

Malayan Scouts (SAS) as a means to penetrate the jungle and chase down the guerillas.[34]

Their success, combined with the growing realization that SOF, when employed correctly, revealed a "comparatively low cost in lives set against results achieved," provided a new lease on life for SOF.[35] Quite simply, frugal bureaucrats realized that SOF provided an inexpensive means of addressing threat and waging war against insurgents in distant jungles and deserts, often largely on their own. Savings realized by replacing generic capability backed with quantity, with specific skill sets reinforced by quality, became an attractive lure. Therefore, SOF began to evolve once again to a force that was concentrated on UW, COIN and Foreign Internal Defense (FID). For example, SOF forces were utilized by a myriad of nations during low-level conflict in Malaya, Oman, Brunei, Borneo, Aden, Indo-China, Algeria, and Chad, to name but a few.[36]

But once again, despite the arguable success of SOF during this period, they were never fully accepted by the larger institution. Ironically, the very attributes that furnished SOF with its greatest strength also generated enmity from the conventional forces. The ability to respond to, and outwit, their adversaries, as well as endure austere and hostile environments inherently required unconventional tactics, an independence of thought and initiative by the operators, mental agility, specialized training, as well as a level of aggressiveness, fitness and general toughness that exceeded that found in regular army units. Quite simply, these were the secrets to SOF success.

However, their success continued to generate antagonism and jealousy between themselves and the conventional military.[37] But paradoxically, it also produced the perception of a silver bullet. For instance, the eventual American involvement in Vietnam witnessed another explosion of SOF-type units as a component of the American response to the escalating and complex nature of the war. Already in May 1961, President John F. Kennedy briefed a joint session of Congress, "I am directing the Secretary of Defense to expand rapidly and substantially (…) the orientation of existing forces for the conduct of (…) unconventional wars (…) In addition, our special forces and unconventional warfare units will be increased and reoriented."[38]

Although President Kennedy was a huge SOF supporter, the entrenched views within the military made even his efforts difficult. However, the conflict in Vietnam soon stymied conventional military commanders. As unique tasks such as UW, long-range reconnaissance, interdiction and riverine operations emerged in the politically restrictive and environmentally hostile theatre of operations, new SOF units were created, or existing ones expanded exponentially, to address the requirement.

For example, the U.S. Special Forces (USSF), or "Green Berets," were dramatically increased in size. They were initially tasked with the CIA-funded Strategic Hamlet Program and later became responsible for the Civilian Irregular Defense Group (CIDG) program, which revolved largely around training indigenous populations in self-defence by raising local defence forces capable of defending their villages. In addition, the USSF soldiers also undertook basic civil affairs programs such as improving agricultural practices, sanitation and water supply. However, they also built and occupied fortified camps from which fighting patrols by USSF and CIDG soldiers could be mounted. The CIDG program was hugely successful but was later abused by the theatre command structure and its personnel used to form multipurpose rapid reaction forces and Mobile Strike Forces in support of conventional, as well as covert operations.[39]

The dramatic growth of SOF during this period was reflected in the fact that all three American Services were getting into the SOF business. In 1961, the U.S. Air Force re-designated existing units as "Air Commandos" and trained them specifically for counter-insurgency operations using diverse fixed-wing and rotary wing aircraft. A year later, the U.S. Navy created Sea Air Land (SEAL) teams and sent some to Vietnam where they initially acted in an advisory role to the Vietnamese Navy, but later became responsible for the interdiction of all waterway supply routes from North Vietnam and Cambodia, by ambush, patrols, sabotage, and mines. In addition, they were entrusted with conducting raids on Viet Cong bases and headquarters.[40]

Further SOF developments included the decision by Military Assistance Command Vietnam (MACV) in April 1964, to create the Studies and

Observation Group (SOG) that was tasked with strategic reconnaissance and special operations. Specifically, they were responsible for covert cross-border reconnaissance operations against the Ho Chi Minh Trail, inserting and running agents and complex deception operations in the North, psychological operations, and covert maritime interdiction, capture and destruction of North Vietnamese naval craft and fishing boats.[41]

Additionally, in 1965, 13 Long Range Reconnaissance Patrol (LRRP) companies (LRRP) were formed. Four years later, they were collectively designated the 75th Infantry Regiment (Ranger).[42] In addition, Projects Delta, Omega and Gamma were sequential programs undertaken to create battalion-sized SOF units comprised of both US and Vietnamese personnel that were capable of long-range reconnaissance and raiding. Australian and New Zealand SAS forces were also employed in this capacity.[43] Finally, throughout the conflict, SOF organizations and ad hoc task groups were also tasked with running rescue operations, 119 in total, to rescue American prisoners of war.[44]

Unfortunately, the sudden spike in demand was met in many cases by lowering selection standards, where in fact they existed, which inevitably led to a diminution of the overall standard of individuals serving in those units. For instance, the Special Warfare Centre, which on average graduated less than 400 individuals in a given year, ballooned to eight times that number. By 1962, the success rate, which was historically 10 per cent, rose to 30 per cent. Two years later the pass rate skyrocketed to 70 per cent. Incredulously, in 1965, Special Forces accepted for the first time 6,500 first-term enlistees, as well as second-lieutenants! Not surprisingly, the emphasis on quality – that is ability, namely experience, maturity and skill – was ignored in favour of quantity.[45]

In theatre, the SOF culture of lax discipline and deportment, as well as "unconventional" tactics, exacerbated by the type of inexperienced, and often immature, individuals who were now serving in SOF created difficulties. Rightly or wrongly, the reputation of SOF suffered. They became viewed by the conventional military, as well as by much of the public, as largely a collection of ill-disciplined cowboys and soldiers of questionable quality and planning ability who were running amok without adequate control mechanisms.

This legacy haunted the special operators for decades. SOF nonetheless had demonstrated, as it had always done, that it was in fact a force multiplier, a very economical tool and an excellent means of addressing threats for which conventional forces were ill-prepared. For example, the CIDG program was an unmitigated success and its forces were continually utilized. Additionally, throughout 1969, SOG maintained a kill ratio of almost 100 to one. This ratio compares to the conventional unit kill ratio of 15 to one. Moreover, the SOG kill ratio jumped to 153 to one in 1970. Equally important, the SOG activities required the North Vietnamese Army (NVA) 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 indigenous soldiers.[46] An NVA officer later conceded that SOG effectively attacked and weakened their forces and hurt their morale because they were unable stop the SF attacks."[47]

Nonetheless, much like the WWII experience, SOF units were still, if not increasingly, marginalized by the mainstream army. General Maxwell Taylor recalled that despite President Kennedy's urging, "not much heart went into [the] work [of placing greater emphasis on SOF]." Taylor, like many senior commanders, believed that SOF were not doing anything that "any well-trained unit" could not do.[48]

As such, although SOF missions had undergone an evolutionary shift, not much had changed. In the post-Vietnam era, the American SOF witnessed their budgets and organizations slashed unmercifully. By the mid-1970s the Navy was considering moving its remaining special warfare forces to the reserves, and the Air Force cut its Air Commandos, which were a separate air force during the Vietnam War, down to a few squadrons and a handful of aircraft.[49] The Army reaction was even greater. It slashed SOF staffing by 70 percent and its funding by 95 percent.[50] At its lowest point in 1975, the SOF budget represented one tenth of one percent of the total American defence budget.[51]

Not surprisingly, most operators, particularly officers and senior non-commissioned officers, felt that SOF employment was career limiting.

Predictably, not everyone, in fact very few, saw their utility in the Cold War paradigm of "Air Land Battle" which pitted large heavily armoured mass formations against one another on the North European plains. Low intensity warfare and insurgencies were seen as an inconvenient nuisance that distracted the military from the real business of high intensity warfare. A classified research project in the mid-1970s titled the "Multi-Purpose Force Study: US Army Special Forces," confirmed that "there is a pervasive lack of understanding, interest and support of unconventional warfare and Special Forces as a valid national response option."[52] Nonetheless, despite this reality, the allure of SOF still drew those individuals who were attracted to its reliance on individual initiative and adaptability, as well as its unconventional methodology and tactics.

But once again, despite the overwhelming institutional prejudice, the "unexpected" forced conventional-minded military commanders to turn to SOF yet again. A fundamental shift in the threat picture to Western industrialized nations erupted in the late-1960s and early-1970s and provided SOF with another area of specialization. Terrorism became recognized as a significant "new" menace. Bombings, kidnapping, murders, and the hijacking of commercial aircraft seemingly exploded and not just in the Middle East. European countries were thrust into a state of violence as both home-grown and international terrorists waged a relentless war that recognized no borders or limits. Israeli targets, particularly its national airline *El-Al*, were struck at Athens, Rome, Zurich and elsewhere. Other international airlines such as Swissair, TWA, Pan Am, to name but a few, as well as their passengers also became victims to terrorism. The murder of Israeli athletes at the 1972 Olympics in Munich, West Germany, became one of the defining images of the crisis, as did the 1975 terrorist assault on the headquarters of Organization of the Petroleum Exporting Countries (OPEC) in Vienna, Austria.[53] The scope of the problem was such that in the 1970s, in Italy alone, there were 11,780 terrorist attacks.[54]

But the problem went beyond a spill-over of Middle East conflict and politics. In Germany, groups such as the Baader-Meinhof gang (also known as the Red Army Faction), unleashed death and destruction. Holland was besieged

by Moluccan terrorists and Britain struggled with the Irish Republican Army (IRA) and the quandary of Northern Ireland. Even in North America, terrorism reared its ugly head. The Americans saw the growth of radical groups such as the Weathermen, New World Liberation Front and Black Panther Party, to name but a few. In Canada, the *Front de Libération du Québec* (FLQ) began a reign of terror that culminated in the October Crisis of 1970. In addition, foreign terrorists imported their political struggles and launched attacks against targets in Canada.[55]

One common theme quickly emerged. No country was immune to terrorism. The terrorist threat was a global phenomenon. Whether home-grown or imported, every state required a response. That realization spawned the next major evolutionary step for SOF. To fight terrorism required specific skills that were not resident within the military institution at large. As such, SOF were once again targeted to provide the solution. And who better than specially selected individuals who were capable of agility in thought, adaptability in operations and who possessed superior martial skills.

SOF were once again in demand. New units were created, or existing ones assigned new tasks. For example, the Germans established *Grenzshutzgruppe* 9 (GSG 9) in September 1972; the British assigned the CT role to the SAS that year same year; the French formed the *Groupe d'intervention de la Gendarmerie nationale* (GIGN) two years later; the Belgians created the *Escadron spécial d'intervention* (ESI) also in 1974; the U.S. formed its premier CT unit, the 1st Special Forces Operational Detachment Delta (SFOD-Delta) in 1977; and the Italians raised the *Gruppo di Intervento Speciale* (GIS) in 1978. In the end, most countries developed specialist CT organizations to deal with the problem.[56]

Arguably, however, the new CT role for SOF did not immediately raise their stock within the military institution. SOF were simply seen as taking on another "niche" designer task that was not fully recognized as a "real" mainstream military function.

The SOF "brand" received an additional boost during the 1982 Falklands War in the South Atlantic. British SAS and SBS raised the profile of SOF through

the recapture of South Georgia Island and direct action, particularly the raid on Pebble Island, which hearkened back to SAS airfield raids in North Africa of WWII lore. They also conducted vital SR and economy of force/diversionary missions. In the end, however, their successful performance did little to change the acceptance of SOF in the mainstream military.[57]

In fact, for the SOF concept, credibility would get worse before it would get better. On October 25, 1983, approximately 2,000 troops representing Delta Force, Navy SEALs, Army Rangers and U.S. Marines conducted Operation Urgent Fury and unleashed the invasion of Grenada, located in the Caribbean Sea.[58] The operation, although ultimately successful, resulted in 19 Americans killed and 123 wounded. Importantly, few of the SOF missions were entirely successful and many were criticized as poorly planned and/or unnecessary. To most analysts, despite the official reports and statements, Operation Urgent Fury, coming three short years after the debacle at Desert 1 (Operation Eagle Claw) in Iran, was yet another unmitigated failure. Simply put, shortcomings in intelligence, planning, the ability to operate in a joint manner and tactical mobility all conspired to sabotage the mission.[59]

These continuing issues with the cooperation, integration, performance and utilization of SOF in Operation Eagle Claw and Operation Urgent Fury finally broke the proverbial camel's back. As a result, American legislators now intervened and assisted those within the military institution in breaking down the barriers that impeded SOF. American senators Sam Nunn and William Cohen, both members of the Armed Services Committee, as well as Noel Koch, Principal Deputy Assistant Secretary of Defence for International Security Affairs were instrumental in pressing for change. In 1987, after a long struggle, and against persistent resistance and adamant protest from the Joint Chiefs of Staff, Congress mandated that the President create a unified combatant command. As a result, on April 13, 1987, United States Special Operations Command (USSOCOM) was activated.[60]

The creation of USSOCOM provided an important benchmark in SOF evolution. The Americans who, in the post-WWII era, were normally the trendsetters in military affairs, whether equipment, doctrine, organization

or technology oriented, recognized SOF as an independent joint command. SOF now had control over their own resources so they could better modernize their organizations. They had a single commander who could promote interoperability and ensure all SOF assets could operate effectively together. Finally, the provision of a "four-star" commander-in-chief and an Assistant Secretary of Defense for Special Operations and Low Intensity Conflict gave SOF representation in the highest councils of the Department of Defense (DoD). Quite simply, SOF had come of age. They were now masters of their own destiny and could grow their force accordingly, both from the perspective of people and equipment.

The universal image of SOF continued to grow. Internationally, SOF units scored repeated successes against terrorists. But of great importance, SOF forces gained important credibility during the Gulf War, which began August 2, 1990 and ended February 28, 1991. Coalition SOF conducted SR, direct action (DA) raids, economy of effort activities such as deception operations, and liaison/training missions with the less advanced non-NATO coalition partners. But, their most well-known, public mission was "Scud busting" – 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.[61] SOF were given the difficult task of locating and destroying the mobile launchers.[62]

In the end, of the 540,396 American troops deployed to Operation Desert Storm, approximately 7,000 were SOF personnel.[63] General H. "Stormin" Norman Schwarzkopf III, who actually despised special operators because of his negative experience with them in Vietnam and later in Grenada, slapped severe restrictions on their employment in theatre.[64] Yet, in the end, despite his initial reluctance to use SOF, he later singled out those forces as critical to the allied victory.[65]

Special operations forces were now on the rise. They had proved themselves effective in the murky war against terrorists, in the blowing sands of a conventional war in the Gulf, as well as in the savage peace that prevailed. Globally, they were used for the traditional roles of UW, SR and DA. However,

they now also specialized in CT, FID (i.e., training foreign militaries in CT and COIN in an effort to shape the environment before a problem in an at-risk state became so severe that it required a larger military intervention), counter-proliferation (i.e., combating the proliferation of nuclear, biological and chemical weapons; intelligence collection and analysis; support of diplomacy, arms control and export controls), civic affairs, psychological operations and information operations. They were also used to hunt down persons indicted for war crimes (PIFWC) in the Former Yugoslavia and Africa.[66]

Their importance increased because political decision-makers and senior military commanders began to realize the effective and efficient contribution they could make. Quite simply, relatively small, highly skilled and mobile teams and units that proved extremely effective in operations, and who presented a relatively small footprint, provided the political and military leadership with a scalable, viable response to global threats and problems. SOF could be employed in a myriad of potentially politically-sensitive operations but without the normally risk or negative optics of deploying a large number of troops. Mass could be replaced by quality. This realization was not only an economic factor but one of effectiveness. In the volatile, uncertain and ambiguous environment of conflict, SOF were normally more agile and adaptable than conventional forces. Their higher levels of intelligence, skill, agility and ingenuity compared to their conventional brethren provided a better chance of success.

The change in momentum became obvious. Using the Americans as a case study, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict reported, in 1992, that "our deployments between Fiscal Years 1991 and 1992 grew by 83%." This trend continued. "During 1997," SOCOM commander, General Peter Schoomaker, revealed, "SOF deployed to 144 countries around the world, with an average of 4,760 SOF personnel deployed per week – a threefold increase in missions since 1991."[67] During the Fiscal Year 1997 alone, SOF conducted 17 crisis response operations, 194 counter-drug missions, and humanitarian demining operations in 11 countries, and participated in 224 combined exercises for training in 91 countries. The following year, SOF conducted 2,178 missions outside the continental USA in 152 different countries. A point worth noting is that the incredible capability

and flexibility provided by the U.S. SOF, which numbered about 45,690 members at the time, came at the cost of only one per cent of their defence budget.[68]

However, it was the events of 9/11, the cataclysmic terrorist attack on the twin towers of the World Trade Center in New York on September 11, 2001, which arguably propelled SOF into the mainstream of recognized national military capability. Decision-makers were looking for a means of striking back swiftly and effectively. SOF very quickly proved themselves to be the "avenging angels."[69]

And so, SOF once again provided the answer to real and perceived threat. As part of Operation Enduring Freedom (OEF) in Afghanistan, it took only 49 days from the insertion of the first American SF teams with Northern Alliance (Anti-Taliban) forces to the fall of Kandahar and the rout of the Taliban and al-Qaeda. This ground was achieved with approximately 300 USSF and some CIA operatives with bags of money and precision close air support.[70] The USSF operators rallied and forged cohesive teams out of the unorganized anti-Taliban opposition groups and more importantly, using a small amount of sophisticated targeting equipment, brought the weight of American airpower down on Taliban and al-Qaeda fighters.[71]

As the Americans changed focus and put their priority of effort into the invasion of Iraq as part of Operation Iraqi Freedom (OIF) on March 20, 2003, SOF underscored their immense utility once again. One strategic assessment lauded, "raids by special operations forces were more impressive than the early air campaign." It went on to explain:

> [D]ozens of small special operations teams disrupted Iraqi command-and-control, seized oil infrastructure, prevented dams from being demolished and took hold of airfields in regions where Scud missiles might have been launched at Israel. They also provided information on the whereabouts of Iraqi leaders, permitting attacks against Saddam Hussein and the notorious General Ali Hassan Majid (Chemical Ali). Special Forces also disrupted internal Iraqi lines of

> communication in Baghdad and elsewhere, perhaps hastening the collapse of Iraqi forces once urban combat began.[72]

Another account revealed that U.S. SOF were:

> usually ahead of the tip of the spear: as US troops pushed toward Baghdad, secret combat teams zipped into Iraq aboard specially outfitted MC-130 Combat Talon planes that used highways as landing strips, surprising the enemy at its rear. On the road to Tikrit, they fingered Iraqi vehicles fleeing the capital for destruction by M1 tanks. And inside the capital the elite Delta Force slipped into Baghdad's back alleys and into its sewers to eavesdrop on communications, cut fiber-optic cables, target regime leaders and build networks of informants.[73]

Delta was actually the first SOF unit deployed on March 19, 2003, and they conducted a number of high-priority Sensitive Site Exploitation (SSE) on suspected chemical weapons facilities before heading for the Haditha dam complex where they "marked" armoured vehicles and anti-aircraft systems for destruction by coalition air. Upon being reinforced by a Delta squadron and a battalion of Rangers they seized the dam.[74]

Delta forces also deployed to the north and conducted ambushes on the highway to Tikrit to tie up Iraqi forces and capture high value targets (HVTs) attempting to flee to Syria. Furthermore, Coalition SOF in the Western theatre of operations also successfully conducted hostage rescue operations, saving in the process Private Jessica Lynch, three Italian contractors that were seized in April, as well as three non-governmental organization (NGO) workers.

In the Northern part of Iraq, Coalition 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.[75] These positions became even more vital once Turkey denied staging rights for conventional forces to deploy from its soil. In addition, USSF infiltrated Iraqi territory to monitor the Karbala Gap.

In the South, Coalition SOF seized national oil production facilities, provided SR, and captured key facilities and transport nodes. A Naval Task Group seized Umm Qasr, Iraq's only deep-water port, the oil production facilities of the Al-Faw Peninsula and two offshore platforms that the pipelines fed. A fourth covert SOF unit searched for weapons of mass destruction and HVTs within the Saddam Hussein regime. In addition, Coalition SOF also supported conventional forces and their seizure of Al-Rumaylah oilfields. USSF, specifically Operational Detachment Alpha (ODA) 563, worked with local Sheikhs and their militiamen to capture a bridge and then supported militia to take the town. The USSF then set up a police service and restored 80 percent of the town's electricity within a fortnight. They also reopened schools and hospitals.

Other Coalition SOF captured HVTs, including Palestinian terrorist leader Mohammed Abbas in Baghdad on 10 April 2003 and Iraqi deputy Prime Minister Tariq Aziz on April 25th. Delta and Naval Special Warfare Development Group (DEVGRU), also known as Seal Team 6, scored a huge success with the elimination of Uday and Qusay Hussein. They also captured Saddam Hussein and killed the al-Qaeda in Iraq (AQI) leader, Abu Musab al-Zarqawi. In addition, Coalition SOF conducted numerous SSEs on suspected Weapons of Mass Destruction (WMD) sites, as well as countless direct action raids, where they captured or killed over 100 AQI members including at least eight HVTs.

SOF were clearly on an up-swing. By 2001, 5,141 SOF personnel were deployed to 149 countries and foreign territories.[76] However, this number skyrocketed in the aftermath of 9/11 and the invasion of Iraq. As of May 2003, there were approximately 20,000 special operators, representing almost half of the entire special operations force of 47,000, involved in ongoing conflicts in Afghanistan and Iraq.[77] Moreover, U.S. SOF were joined there by a large number of Allied SOF contingents.

As American focus and effort in Iraq intensified, the situation in Afghanistan, however, deteriorated. By 2003, the Taliban and AQ were flowing back into the country and by 2005, they had plunged the country deep into a brutal insurgency. SOF once again became a central factor in the COIN campaign.

SOF quickly became the "invisible hand" in Afghanistan that conducted a war in the shadows, providing a significant impact to Coalition force protection, an increase in host nation governance and security, as well as destruction of enemy capability. Moreover, SOF became a vital contributor to the successful fight for the hearts and minds of the population.[78]

General Wayne A. Downing asserted, "SOF was structured for and conducted short-duration deployments and combat operations, but by 2005, SOF operators were conducting more operations in a week, at a higher rate of complexity, than their pre-9/11 predecessors conducted in a career."[79] For example, in the first three months of 2011, Allied SOF mounted more than 1,600 missions and captured or killed close to 3,000 insurgents.[80] Reportedly, SOF secured their target 80 per cent of the time, and less than one per cent of the raids led to civilian casualties.[81] By August 10, 2011, the International Security Assistance Force (ISAF) Joint Command reported, "there were 675 raids in 2009,1,780 in 2010, and 1,879 by August 2011 – 49 percent of the raids captured or killed the principal target; 45 percent in 2009/2010; and 84 percent of the raids achieved some success (i.e., captured or killed their target)."[82] Importantly, these figures represent only the kinetic aspect.

Throughout this period and extending beyond combat operations in Iraq and Afghanistan, SOF forces demonstrated their utility in conducting operations abroad whether combating terrorism and piracy, or conducting military assistance, SR or special warfare.[83] For example, SOF operations in North Africa (e.g., Mali, Niger, Chad, Mauretania, Senegal) were critical in bringing a degree of stability to a number of nations undergoing internal and external security problems, specifically the expansion of the al-Qaeda in the Islamic Maghreb (AQIM) organization, which uses the remote, wide-open space, as well as the vacuum in governance and security of the weakly governed states to operate training camps, bases and conduct terrorist attacks.[84]

The threat the AQIM, as well as others, represented a potential threat to explode into larger regional, if not international, crises. As such, international SOF organizations, under an American framework, undertook a program of training and advising security forces in a number of North African countries, as well as supporting the North African Union in taking a larger role in African

affairs. More to the point, in January 2013, British and French SOF assisted Mali defence forces in turning back an Islamic militant (AQIM) offensive to increase their hold on territory they had seized from the Mali government in the previous year. As they began their renewed offensive pushing south to the capital of Mali, government forces backed by Western nations halted and then turned back the militants. During the combat operations French and British SOF advised, supported and even commanded Malian troops who did much of the heavy lifting in terms of fighting.[85]

Moreover, in 2014, in an era where virtually all Western countries and their publics were fiscally constrained, war weary and reluctant to deploy ground forces or become embroiled in a military intervention that could turn into a quagmire, SOF saliency once again resonated and they became a key player in the concerted effort of an international coalition to stop, neutralize, if not destroy, the Islamic State terror organization that swept through major parts of Syria and Iraq declaring the creation of a Caliphate. Their brutal terror tactics, crimes against humanity, wealth and access to modern military technology, as well as their ability to sway adherents through a sophisticated communication strategy that made expert use of social media and the internet, made them an immense international security threat.[86] Action had to be taken, yet, nations were reluctant to get involved in yet another potentially long, costly conflict.

SOF once again filled the gap because of their ability to provide governments with viable policy options, without representing an irrevocable ground force commitment. Former USSOCOM commander, Admiral William H. McRaven captured SOF's versatility. He explained, "SOF are rapidly deployable, have operational reach, are persistent and do not constitute an irreversible policy commitment."[87]

Key to the SOF response to the continuing global crises was a formal SOF interconnected approach. In many ways, under McRaven's tenure as Commander USSOCOM, the SOF global network, which has always been an informal web, was promoted and nurtured as a more formal network of like-minded international SOF organizations. As such, it yields a viable response to the global terrorist threat. In an era of persistent, complex conflict within the

context of globalization (i.e., proliferation of cheap, accessible information and technology, as well as worldwide access) political and military decision-makers have realized SOF is a strategic implement of great utility. Steven Bucci, the director of the Center for Foreign Policy Studies at the Heritage Foundation, captured this realization of SOF as the new "force of choice." He asserted:

> The world is more dangerous than it's been before with a lot of potential threats out there and SOCOM [SOF] is offering policymakers ways to address those threats at a very low level with a low footprint in ways that can hopefully defuse those threats before they turn to violence.[88]

The respective national investment in SOF by nations is telling. Using the U.S. as an example, analysts have summarized, "U.S. Special Operations Command (SOCOM) has grown tremendously since 2001. Its manpower has nearly doubled, its budget has nearly tripled, and its overseas deployments have quadrupled."[89] Importantly, the American experience is not unique; rather, it is indicative of the evolution of SOF. In the United Kingdom during their 2010 Strategic Defence and Security Review, British Special Forces were spared cutbacks that resulted in the defence budget falling by approximately 7.7 per cent to around £33.5B between 2010-11 and 2014-2015.[90] In the Canadian context, the Canadian Armed Forces have experienced four major iterations of defence cuts since 2010. SOF was spared in three of the rounds of cuts and only superficially impacted in the fourth. Significantly, it received in-year funds to meet all its commitments and is still in a period of growth in an era where other Services are looking at divestment.

SOF's evolutionary ascent shows no signs of abating. Traditional missions continually expand and new tasks are assigned to meet new and emerging threats. In general, contemporary SOF normally conduct the following core tasks:

- Counter Terrorism;
- Maritime Special Operations;
  - Maritime Counter Terrorism;
  - Opposed Boarding;

- Direct action;
- Special Recovery Operations;
  - Personnel Recovery Operations;
  - Hostage Rescue Operations;
  - Noncombatant Evacuation Operations;
  - Material Recovery Operations;
- Combating Weapons of Mass Destruction;
  - Counter-Proliferation;
  - Non-Proliferation;
  - Weapons of Mass Destruction Elimination;
- Special Protection Operations;
  - Close Personal Protection;
  - Special Force Protection;
- Sensitive Site Exploitation;
- Special Reconnaissance;
- Special Warfare:
  - Irregular Warfare;
  - Military Assistance;
  - Stability Activities;
  - Counter-insurgency; and
  - UW;
- Special Aerospace Warfare;
  - Special Operations Air-Land Integration;
  - Airborne Reconnaissance and Surveillance; and
  - Airborne Fire Support.[91]

As encompassing as these tasks are, the complexity of the contemporary and future operating environments will see SOF required to continue their evolution and further push these tasks to include greater emphasis on power projection; network penetration and disruption; interdiction of ground and sea Lines of communications; disrupt anti-access/area denial networks; build and maintain

the global SOF network; and building indigenous SOF capacity to ensure allied and friendly countries can effectively deal with the threat of violent extremist groups, foreign fighters, insurgents and narco-terrorists themselves.[92] After all, it is SOF's ability to adapt and meet unexpected threats with agility, swiftness and extreme effectiveness that has earned them a reputation for strategic utility.

CONCLUSION

The level of chaos, ambiguity and uncertainty in the contemporary operating environment of the new millennium has created numerous threats and significant security challenges for all states. In this turbulent global stage, SOF evolved from a WWII force of desperation to a force of choice. SOF's ability to provide significant strategic utility to political and military decision-makers, specifically to meet new and emerging threats, created the rise of SOF Power (i.e., the marriage of capability and cost to produce enormous effect).

In essence, SOF have been able to offer decision-makers a myriad of timely, precise and tailored options in response to a complex, chaotic and ambiguous national security challenges. The high-readiness posture, small footprint, skill level and deployability of Special Operations Task Forces and SOF Teams allow for a rapid and determined response, domestically or internationally. SOF have also served as a catalyst to unify, extend the reach and maximize the effects of, other instruments of national power.

Importantly, SOF have consistently proven to be a strategic resource that provides political and military decision-makers with a wide range of precise kinetic and non-kinetic options to deter, pre-empt, disrupt, react or shape strategic or operational effects domestically or abroad. SOF represent a highly trained and educated, adaptive, agile-thinking force capable of dealing with the threats that have not yet been identified. Undeniably, SOF have proven to be a valuable national strategic asset for advancing national interests at acceptable risk and cost. As Richard Fadden, the Canadian National Security Advisor asserted, "the continued growth of SOF is inevitable."[93] As a result, SOF have finally moved from the margins of military institutional acceptance to a mainstream national military capability.

CHAPTER

2

THEORY AND STRATEGIC UTILITY OF SPECIAL OPERATIONS

DR. PATRICIA J. BLOCKSOME

The late Brigadier Maurice Tugwell and Professor David Charters define special operations as "Small-scale, clandestine, covert or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy."[1] This commonly used definition hints at the issues surrounding both the theory and strategic utility of special operations. In terms of theory, what, exactly, are 'unorthodox' operations, and how can they be defined? Similarly, the phrase 'significant political or military objectives' implies that the concept of special operations is intertwined in some way with strategic utility. Are all special operations strategic in nature? If so, it would follow that any unorthodox operations with merely tactical or operational aims are thus disqualified. Yet can the strategic effect of a special operation be known – not just hoped for – prior to its execution?

This chapter examines these two questions on the theory and strategic utility of special operations. It reviews several of the leading theories of special operations, dividing them into two clusters, one focused on the unorthodox, or non-conventional nature of special operations, and one focused on the strategic aims of such operations. An understanding of the non-conventional nature of special operations must look to social constructions of orthodoxy

and unorthodoxy to understand how operations can be classified as 'special'. In addition, the concept of strategic utility is challenging in that strategic effect is often not known till after the operation is complete, and that some special operations may be tactically or operationally effective but not have direct strategic effects. However, extant theories on the strategic utility of military operations do provide an avenue to understand the ways in which special operations may provide a unique form of strategic effect.

THEORIES OF NON-CONVENTIONALITY

Whilst the terminology of 'special operations' is relatively new, the concept itself is not; as scholar Robert Graves notes, "Special operations have been present from the earliest stirrings of organized conflict, a point well made, from a literary perspective, by chroniclers of the Trojan War."[2] Both Sun Tzu and Clausewitz have works dedicated to the description of military activities that would fit comfortably within the current paradigms of special operations. Sun Tzu's *The Art of War* describes deception [covert] operations and information warfare.[3] In Book Seven of *On War*, as well as in other lectures and writings, Carl von Clausewitz discusses popular resistance and what we would today call insurgency.[4] Despite a recency bias in the extant scholarly literature, special operations have existed concurrently with organized military activities throughout history.

The theories described below focus, for the most part, on Western understandings of conventional and non-conventional military operations, predominantly built on case studies from no earlier than the 1800s. This emphasis is perhaps understandable as the formalization of 'special operations' as a distinct branch of military operations predominantly arose during World War II, with the creation of the Special Operations Executive and the Office of Strategic Services.

This recency bias can be problematic. As Dr. Christopher Marsh and his research team point out, using contemporary Western doctrinal definitions of special operations risks issues with selection bias in both exclusionary and inclusionary ways.[5] Should units not designated as 'special' at the time of their

creation, but later viewed as undertaking special operations, be included for analysis? Should units that are designated as 'special' by their militaries but having mission sets that are not generally recognized as special by Western military standards be recognized?

If there is no agreement to what special operations encompass, how then can we theorize about the definition and role of special operations? Admiral Eric T. Olsen, a former commander of U.S. Special Operations Command (USSOCOM), argued that "'special operations are defined negatively,' i.e., in terms of what they are not rather than what they are. Specifically, special operations are operations that are not conventional operations."[6] This statement hints at an enduring dichotomous relationship between conventional and special operations; if conventional military operations can be defined as such, then every non-conventional military operation, by default, is a special operation.

While there is no grand unified theory of special operations, several scholars writing on the topic have taken similar foci on understanding the character of special operations vis-à-vis other types of operations. The following brief discussion of their extant theories is not exhaustive, but it does represent the key points within their works.

In *Explorations in Strategy*, renowned strategist Colin Gray offers the following definition: "Special operations are operations that regular forces cannot perform, and special operations forces are selected, equipped, and trained to do what regular forces cannot do. To restate the point from a different perspective, special operations lie beyond the bounds of routine tasks in war."[7] In like manner, Dr. John Arquilla describes special operations as "that class of military (or paramilitary) actions that fall outside the realm of conventional warfare during their respective time periods."[8]

Tom Searle, a former special forces officer and current defence analyst, argues that special operations can best be understood as military operations "outside the box" of conventional military operations as doctrinally understood by the U.S. military.[9] Searle's theory limits the discussion of that relationship

primarily to U.S. doctrinal capability examples and does not generalize the inside/outside box theory to non-Western or non-contemporaneous forces.

In a similar vein, Professor Harry Yarger defines U.S. special operations as "military operations conducted by SOF [special operations forces]," in contrast to conventional operations which are performed by conventional forces.[10] However, Yarger also claims that "conventional forces may be called upon to conduct special missions that require unique preparation and arrangements but 'special operations' involve SOF."[11] The underlying difference between special missions and special operations is unclear. Additionally, Yarger risks a tautology; are special operations forces defined as special because they carry out special operations? Yarger's theory is also potentially limiting in that it removes the possibility for special operations forces to carry out missions that are not special.

As with Searle, Yarger focuses specifically on U.S. special operations, and both authors assume clearly defined mission sets and formal distinctions between conventional and non-conventional military forces. Approaching the same question from a much wider lens, Dr. Richard Rubright offers a non-military specific definition, arguing that special operations are not undertaken only by military forces.[12] He offers a broad definition, that "special operations are extraordinary operations to achieve a specific effect," and that governmental unit, military or otherwise, can carry out such extraordinary operations.[13] Rubright's definition, however, requires context as to what the 'ordinary' is which will be contrasted to his extraordinary. What might be an extraordinary operation for a police unit is not likely to be similar to that of an intelligence or military unit.

All of these theories identify, in some shape or form, the unorthodox, or non-conventional nature of special operations. While this may help in understanding how a specific state deduces which of its military operations are special, it still does not answer the larger question of how to understand special operations across military cultures and time. In order to contrast non-conventional special operations against conventional or orthodox operations, we must understand where conventionality comes from. How do militaries

develop their *a priori* understandings of what is conventional? I argue that an understanding of conventional miliary operations and the non-conventional nature of special operations must look to social constructions of orthodoxy and unorthodoxy.

In their seminal work, *The Social Construction of Reality*, sociologists Peter Berger and Thomas Luckmann describe how societies develop 'truths' through social processes of interaction and institutionalization.[14] Their theory helps to explain why it is so difficult to come to an agreement on what special operations are. Because each society constructs for itself an understanding of what war is, and what military operations are and are not normal within warfare, the norms of conventional warfare will be different for each society.

Since special operations are defined negatively via conventional operations, it follows that special operations will also be constructed as a norm within each society that they arise. It is important to note that these social constructions of conventional and special operations are not static. As societies change over time, so do their understood realities.[15] Therefore, any military's definition of special operations will be informed by both the societal and military culture in which their normative conventional military institutions arose, as well as the historical context and current operating environment which may or may not provide impetus to change those norms.

This sociological argument dovetails nicely with political scientist Jack Snyder's theory of strategic culture.[16] Snyder argues that historical, institutional, and political factors shape strategic thought, which in turn shapes military thinking. Since states have different strategic cultures, they will view military problems from their own unique perspectives, and thus different states will respond differently to the same strategic issue. As Snyder describes it, strategic culture can be used to understand when "a distinctive approach to strategy becomes ingrained in training, institutions, and force posture."[17] If strategic culture, as a form of social culture, can have a direct impact on the organization and employment of military forces, then it follows that strategic culture may have a role in shaping special operations missions and forces. Gray would agree with this approach, as he notes "Special operations are not, or not only, the

expression of a culturally free-floating craft, but rather of particular political and strategic cultures."[18]

This social construction explanation for special operations provides insight into the reasons why an overarching strategy of special operations is so difficult to achieve. Each society will designate forces and operations as special, or non-conventional, given their own cultural conventions at a specific point in their history. In sum, then, special operations can best be understood as an expression of the sociocultural warfare norms of a given society, and any research on special operations must be informed by the context in which those operations were conceived.

THEORIES OF STRATEGIC UTILITY

The second question raised by the definition provided in the introduction to this chapter is in regard to the strategic utility of special operations. Several scholars seem to agree that strategic effect has a critical explanatory role in theories of special operations. They contend that the role that strategic utility plays is vital in understanding the value proposition of special operations.

Admiral William McRaven, another former USSOCOM commander, asserts that the key defining feature of special operations is 'relative superiority' which enables smaller forces, in certain circumstances, to achieve the advantage against larger forces.[19] His theorizing is focused primarily on time-limited duration, hyperkinetic raid-style operations. It offers an explanation of why that specific type of special operation may have strategic utility but fails to explain other types of contemporary special operations such those that require cultural understanding or persuasion of societal groups, sometimes called 'political' or 'special' warfare.

Dr. Robert Spulak, expanding on McRaven, defines special operations as "missions to accomplish strategic objectives where the use of conventional forces would create unacceptable risks due to Clausewitzian friction."[20] While certainly broader in scope than McRaven's focus on surgical strike-style operations, this theory is limited in a different way; if special operations are only available for strategic missions, then any military operation, no matter

how non-conventional, does not qualify to be a special operation if it does not have a strategic effect.

This is a striking limitation, as it can be challenging to determine in advance if an operation will have a strategic effect. As Gray explains, "*Strategy* is all about the consequences of (military) behavior. It is not about the actual conduct of behavior; for that one must turn to the realm of *tactics*. …It has to be fundamentally incorrect to conceive of and refer to allegedly inherently strategic missions, because all missions have some strategic value, be it ever so modest or even negative."[21]

In line with Gray, Dr. James Kiras does not follow Spulak's hard requirement for strategic utility but argues that special operations forces, "by inflicting moral and material attrition in conjunction with conventional forces," can enable strategic effectiveness.[22] Interestingly, Kiras' focus on special operations' role in attrition campaigns is in direct opposition to that of McRaven, whose focus on raids aligns him more with annihilation campaigns.

The sum of these scholars' work raises several questions. Do special operations by their very nature provide strategic utility, or is this something that special operations forces seek to achieve but which cannot be determined until after the fact? Is strategic utility a necessary component of a definitional theory of special operations? Per Tugwell and Charters' definition, do operations require significant political or military objectives in order to be classified as special?

These questions can potentially be answered by drawing on the larger literature of military theory, particularly the concept of strategic utility, writ large. As Kiras argues, "A specific theory of special operations may be unwarranted as other, existing military theories may already prove necessary and sufficient for special operations."[23] Arguably, strategic utility is something that all military operations and forces seek to achieve, and all face the challenge of crossing, as Gray puts it, "the bridge that relates military power to political purpose."[24]

However, even though special operations have the same challenges with strategic effectiveness that conventional operations face, this does not mean that scholars do not identify unique aspects of strategic utility in special operations.

Gray calls special operations forces "a national grand-strategic asset," directly linking them to considerations of strategic utility.[25] He categorizes special operations as having strategic utility in two ways, "economy of force and expansion of strategic choice."[26] Similarly, Colonel Bernd Horn offers several reasons why special operations forces could have strategic utility, noting that "Their ability to produce on short notice, courses of action in a number of domains, regardless of location, desirable outcomes with a high probability of success, gives them great saliency to political and military decision-makers."[27]

I contend that special operations can have particular strategic utility if that utility is tied to their unorthodox antecedents. As discussed in the previous section, special operations can be understood as non-conventional within the society from which they spring. This non-conventionality is suggestive, implying activities that, while still within the range of acceptability for a given society, are not the norm. In other words, special operations by their very nature are likely to be somewhat less-common choices. These more creative or flexible possibilities for operations provide, as Gray puts it, the expansion of strategic choice. Put broadly, special operations offer unique strategic utility simply due to their nature as alternative courses of action from conventional military operations.

CONCLUSION

This chapter began by asking two questions: what, exactly, are special operations, and what is their strategic utility? The argument laid out in this paper is that the answer to both of these questions is tied to understanding the social construction of special operations as a distinctive unorthodox form of military operation. Understanding how a society perceives conventional military operations provides the baseline for appreciating what non-conventional operations are. Thus, special operations form the other half of a dichotomous relationship with conventional operations, and the division between those two types of operations can only be understood within the sociocultural context of the society from which they come. In accordance with this basis, it follows that the strategic utility of special operations is tied to their non-conventional nature. Because special operations offer alternatives

to conventional operations, they expand the scope of possibilities for military actions available to political leaders. In summary, a sociological basis for understanding special operations provides a way to not only understand how operations become special, but also how that specialness can provide useful strategic effects.

CHAPTER

3

JEDBURGH TEAMS – LESSONS FOR UNCONVENTIONAL WARFARE

COLONEL (RETIRED) J. PAUL DE B. TAILLON

In no previous war, and in no other theater during this war, have resistance forces been so closely harnessed to the main military effort.

General Dwight D. Eisenhower (1945)

When Great Britain entered the war on 3 September 1939 and the United States later on 7 December 1941, both militaries were designed for conventional conflict and focused essentially on attritional warfare; interestingly, both countries had substantial experience in what was respectively described as imperial policing and small wars. For the professional soldier prior to World War II, the type of operations that would theoretically take place in the enemy's rear area, now formally recognized as unconventional warfare (UW),[1] was neither a focus of mainstream professional military thought nor a concept demanding any formal study. Notwithstanding, these described 'behind enemy lines' UW operations are presently captured under the umbrella of the term Irregular Warfare (IR) which embraces a spectrum of activities to include Counterterrorism, Foreign Internal Defense (FID), Counter-Insurgency (COIN) and Stability Operations (SO). There were a number proponents and practitioners who conducted UW during the world wars of the 20th century.[2]

The UW experience demonstrated the substantial advantages that these operations offered, particularly in the forced dispersal of enemy troops, the requirement to secure and effectively protect the population centres, vital governmental, economic and military installations, as well as the lines of communication amongst others within the target country. For some military professionals, 20th century UW campaigns highlighted the most effective force structure, as they are considered to be 'relational-manoeuvring forces.' These effective guerrilla organizations were adept at ascertaining the enemy's weaknesses or vulnerabilities and then adjusting their internal composition, enabling them to engage and attrit the enemy effectively.[3]

Britain's Great War experience in the employment of the Arab revolt to assist conventional military operations during their Middle East campaign (1916-1918), under the auspices of Lieutenant-Colonel T. E. Lawrence, whose guerrilla army of Arab tribesmen created havoc throughout Ottoman-occupied territory in Arabia was notable. As well, the Imperial German campaigns in East Africa (1914-1918), General Paul von Lettow-Vorbeck and his force of 14,000 Askaris held in check a military force of 300,000 consisting of Indian, British, Belgian and Portuguese soldiers who were much-needed on other fronts, set a standard not before realized in UW. Both of these officers epitomized the economy of effort in their respective application of guerrilla strategy. The UW concept was further explored and applied in World War II through a panoply of Allied special forces (SF) and special operations (SO) organizations developed to oversee unconventional warfare in the form of raising and facilitating guerrilla organizations and to support and coordinate their operations.

This chapter will focus upon the concept of supporting resistance groups, in this case the French Maquis, by multinational Jedburgh teams consisting of British, American and French personnel who were to be deployed in the wake of D-Day on 6 June 1944 within the German rear echelon. The terms guerilla, resistance, resistance fighters, paramilitary and Maquis will be used interchangeably.

BACKGROUND

By mid-March 1943, Supreme Headquarters Allied Expeditionary Force (SHAEF), under the command of General Dwight D. Eisenhower, and its joint staff commenced planning for the strategic inevitability of an invasion of the European continent. At this time both, the United States and Russia were heavily involved in this global conflict and an invasion of occupied Europe was politically and militarily envisioned and being forcefully pressed. Understandably, the location of the invasion and the preparation for subsequent follow-on operations were in the nascent planning stages as it would take time to formulate, coordinate and execute the myriad of preparations necessary for an opposed landing in Europe.

Predicated upon ongoing intelligence and low-level guerrilla operations being conducted from 1941 by the British in Europe, there were strong indications, indeed optimism, that an Allied force would encounter a friendly population actively interest in supporting their liberators.

THE ASSESSMENT CHALLENGE

Planners realized that these nascent resistance organizations were already providing smatterings of intelligence, conducting sabotage and small order paramilitary activities in some German occupied countries, mainly under the auspices of the British clandestine services, particularly the Special Intelligence Service (SIS), also known as MI6 and the newly created Special Operations Executive (SOE). The question arose: if properly organized, equipped and trained, could these resistance elements effectively assist allied efforts in the post-invasion campaign?

As with any resistance movement, certain challenges would have to be recognized and addressed to ensure that the resistance could be assisted and equipped to undertake a spectrum of operational initiatives in support of the allied forces during the liberation of the continent. One of the initial questions to be addressed was what assistance would the French resistance, known as the Maquis, require to undertake effective guerrilla operations against their German occupiers? Another critical issue was how could the

Allies employ the Maquis to the best advantage? Should these resistance organizations be restricted to undertaking sabotage operations or directing local populations away from danger areas, should they be assigned to provide assistance to the civil authority, or was there a more important and effective way to participate in the Allied plan? Another perplexing concern for the staff was could these resistance groups pose an additional planning and organizational dilemma in an already complex multidimensional military operation? If so, should they be directed to abstain from activities, thereby keeping them completely out of the fight?[4] These questions and many others had to be raised and examined by the Allied senior staff, as well as the leadership and planners of the British SOE and the American counterparts of the Office of Strategic Services (OSS).

GUBBINS THE VISIONARY

Major-General Colin Gubbins was a well-regarded British regular officer and avid student of unconventional warfare. He was one to promulgate these 'unconventional ideas' about the potential application of resistance forces where he soundly and persuasively argued for the exploration of the theory of creating military teams assigned specifically to liaise, assist, coordinate and, if necessary, direct indigenous guerrilla forces.

Gubbins was specifically selected for the position as head of the SOE, predicated on his experience with unconventional warfare in the form of terrorism and guerrilla activity in Ireland and Russia, as well as his intellectual curiosity and broad mindedness to ponder new ideas and concepts. He drew from the experiences of the Second Anglo-Boer war, combating highly mobile and effective Boer guerrillas, the exploits of Lieutenant-Colonel T. E. Lawrence[5] and the highly successful German guerrilla campaign in East Africa led by General Paul von Lettow-Vorbeck.[6]

Gubbins noted the dearth of study of unconventional warfare, or as it was described at that time irregular warfare, which had an impact upon the development of the SOE:

> To anyone who has studied the Russian Revolution or, nearer to home, the Sinn Fein insurrection, or the Palestine rising, or the Spanish Civil War, the crippling effect of subversive and para-military warfare on regular forces was obvious. Yet these campaigns, or nationalist risings, were not studied at any of the higher colleges of war; they were irregular and not really deemed worthy of serious attention. This shortcoming was the root of SOE problems.[7]

Through his wide-ranging and intensive study, he amassed many of the basic principles of unconventional warfare that embraced the importance of sound and effective organization, the importance of situational awareness, the criticality of intelligence, the recognition of local operational requirements pertaining to language and culture,[8] and the necessity of effective leadership. His intellectual independence departed from some of the students of irregular/unconventional warfare, as he sought a coherent strategic vision that would see the integration of resistance efforts to facilitate and support aims and objectives of a conventional military campaign.[9] This integration and concentration of effort, as well as appreciating the economy of force of unconventional warfare underlines important aspects represented in the principles of war, amongst others.[10] Gubbins believed that all necessary means within his purview should be directed and massed for a concentrated effort in support of maximizing the opportunities for success for the Allied liberation.[11]

To achieve this, the French resistance would have to be coordinated in sequence with the Allied ground campaign. The quandary for the conventional and special operations planners was how the Allies could employ such guerrilla forces to the best advantage during the post-invasion campaign.

SUPPORTING THE MAQUIS

The SOE had, since its establishment 22 July 1940, by the Minister of Economic Warfare Hugh Dalton as directed by British Prime Minister Winston Churchill, who famously said "set Europe ablaze," built up a network of Allied contacts and operators while conducting intelligence gathering and sabotage activities and managing a variety of low-level psychological operations within France and parts of occupied Europe.

The question was should the SOE network and operators continue with these tasks or ought they embark upon the development of expanding links with the Maquis, who were operating mainly in the French countryside. Should the liberation of the continent begin, the expectation was that the resistance, if properly prepared and equipped, might successfully rise up. Their objectives would be to attack German communications and logistics hubs, and to interdict and attrit their ground units which would inevitably be hurried to the invasion site with the objective to thwart the amphibious landings on water's edge, thereby nullifying the invasion and any possibility of subsequent follow-on operations. Understandably, the former strategy already in operation would have a high nuisance value in the practice of mining roads, bridges and power stations, but realistically such operational initiatives were seen as providing little tactical impact on the military outcome. Another conundrum for planners was the apprehension that large formations of untrained, ill-disciplined resistance fighters would be expected, indeed urged, to engage experienced German military units. Understanding that the resistance fighters would have the advantage of local knowledge and the likely succor of the resident population, another issue arose. It was the view that French resistance fighters without support and guidance would quickly be engaged and eradicated by the more tactically practised German units that had the advantages in armoured vehicles, artillery, mobile reserves and air support. The conflict confronting Allied planners was essentially the choice of 'pinpricks' in the form of sabotage, minor interdiction activities, and psychological warfare upon the Germans, but also the potential of dislocating local French support due to the risk of indiscriminate reprisals as a consequence of Maquis activity.[12] The other option was harnessing the resistance as a coordinated support element to assist the Allied conventional forces in their ground campaign.

Gubbins and his staff recognized the advantages that would accrue should the Maquis orchestrate the destruction of German telephonic communications thereby forcing the Germans to revert to radios. This action would enable their signals to be intercepted and jammed by the Allies. Meanwhile, the well-orchestrated destruction of German fuel and logistics stocks, as well as the delay, interdiction and attrition of supply convoys and vitally

needed reinforcements would have a material impact upon the battlefield, as well as inflicting serious psychological effects on the German soldiery. Such assignments were considered a priority for the Maquis.

There was, however, a subtle yet important complication that haunted this plan, predicated on the domestic frictions of French politics, especially between the resistance elements who supported General Charles de Gaulle's Free French[13] or the Vichy regime of Marshal Philippe Petain[14] and those who were inspired Communists. It was recognized that political obstacles would have to be handled gingerly by those assigned to work with these respective resistance groups.

Appreciating the inevitable invasion of the continent and the importance of making sure that the Maquis would be capable of partaking effectively in such a mission set, Gubbins penned a note to SOE's Security Section outlining in brief the concept and requesting a cryptonym:

> A project is under consideration for the dropping behind of enemy lines, in co-operation with an Allied invasion of the Continent, of small parties of officers and men to raise and arm the civilian population to carry out guerrilla activities against the enemy's lines of communication. These men are to be recruited and trained by SOE. It is requested that 'Jumpers' or some other appropriate code name be allotted to this (sic) personnel.[15]

Soon after this request, the SOE's Security Section assigned the codename JEDBURGH to this SOE initiative.

THE JEDBURGH CONCEPT IS PUT TO THE TEST

As the Jedburgh concept paper was being disseminated and navigated through the British War Office, the Commander in Chief Home Forces, General Sir Bernard Paget was orchestrating a comprehensive and demanding exercise codenamed Spartan. Taking place in the early spring of 1943, this exercise comprising of some 250,000 men and 72,000 vehicles would not only test

the capabilities of Allied ground forces but would also be the first field test on the efficacy of the embryonic Jedburgh concept.

This event was an important conventional exercise as it was formulated to assess the ability of an Allied invasion force confronting experienced German defenders who were in well-prepared defensive positions. After four years of occupation, the German troops intimately knew the terrain and could expect the 'possible reinforcement' by armoured and mechanized panzer grenadier reinforcements from their reserves.

When General Headquarters Home Forces (GHQHF) command and staff requested the SOE to provide twelve Jedburgh teams for Spartan, it provided Gubbins, his staff and official observers an ideal opportunity to fully evaluate the Jedburgh concept. It would further enable them to ascertain what missions would be appropriate for these teams, so as to magnify their tactical and operational level impact when inserted into the opposing force's (OPFOR) exposed echelon.

Adding to the complexity, at this time, there were no Jedburgh teams in existence and no associated command, control and communications elements available for deployment. To fulfil the headquarters prerequisite for this now critical confirmation exercise, a hastily organized staff was summoned, consisting of SOE staff officers supported by instructors and wireless operators, many of whom were assigned for exercise purposes as Jedburgh team operators. This rapid assembly group enabled the provision of a command and liaison team for the 1st Canadian Army Headquarters (1CAHQ) as well as generating eleven 3-man operational teams assigned for the exercise under the codename of BOYKINS. Participating as resistance fighters were 400 soldiers from the Royal Welch Fusiliers who were keen to participate in their new role.

To assist in the deployment of the Jedburgh teams, SOE staff officers led by Lieutenant Colonel Peter Wilkinson, were charged with drafting a spectrum of real and notional incidents and activities to be incorporated into Spartan. It must be acknowledged that the Jedburgh teams and supporting elements

at this time had been 'cobbled together' and some SOE staff elements had never had the advantage of operating within higher formation headquarters. From a command and SOE point of view, this was a tremendous act of faith which provided the opportunity for the application of a new and untested concept within a major exercise. In a more peripheral way, it indicates how special operation visionaries, operators and supporters are, arguably in many cases, strategic change agents.[16]

One of the key players in Spartan was the Canadian Army General Andrew McNaughton[17] who was willing to experiment and embrace new and untried tactical concepts. The exercise comprised of an advance to contact, as well as a scenario devoted to the conduct of mobile defence against an Allied army group which included a breakout phase. Of note, both the Allied and OPFOR forces were not permitted any aerial or ground reconnaissance beyond the forward edge of the battle area; hence both Allied and OPFOR commanders had to plan and conduct their respective operations with no detailed topographic, terrain information available other than what could be gleaned from the maps provided to them.

McNaughton was assigned the command of the Allied Second Army comprising of 1st and 2nd Canadian Army Groups including 12 Corps, consisting of one armoured brigade and six divisions. Also allocated to McNaughton were 11 Jedburgh teams. McNaughton, a former artillery officer with a strong scientific and engineering bent, was an advocate and his openness to the Jedburgh concept aided in ensuring a fair test of this new and unproven concept. In tandem, GHQHF supported the employment of espionage and counter-intelligence activities in the exercise, as well as the incorporation of a guerrilla force that would have to be addressed by the OPFOR commander and his subordinates. Throughout the exercise, Gubbins' staff officer Lieutenant Colonel Peter Wilkinson, kept 1CAHQ commander McNaughton and his staff fully briefed as to Jedburgh exploits and their aid to the resistance.

For the purpose of the Spartan exercise, the teams were assumed to have been inserted prior to and in the wake of the invasion. Throughout the course of the field test, the assigned Jedburgh teams monitored road activity, reporting

the volume and nature of traffic and, when opportune, conducted interdiction missions. The teams were also tasked with demolishing bridges and installations, planning and coordinating attacks upon demolition guards, conducting direct action missions against headquarters and communication centres, as well as the interdiction and destruction of supply convoys. The targeting of OPFOR personnel assigned to traffic control was also within their exercise remit.

One of the objectives was to establish the survivability of the Jedburgh teams and their designated resistance fighters who would be operating with little support behind enemy lines. It was assumed that the resistance would continually be challenged by an aggressive, robust and effective German signals and intelligence[18] capability specifically focused on locating and severing Jedburgh communications.

Throughout the duration of Exercise Spartan, the resistance elements and Jedburgh personnel were continually gauged on their tactical value in interdicting the OPFOR while, concomitantly ascertaining how these teams could best be employed to maximum tactical effectiveness. The exercise and SOE command element needed to ascertain timing i.e., when best to deploy the teams to utmost effect upon the lines of communication and, importantly, ascertain the Jedburgh operator's longevity against an occupation force that embodied a highly effective intelligence, counter-intelligence and radio interception capability combined with an aggressive battle-hardened enemy in pursuit.

During Exercise Spartan, McNaughton and his Chief of Staff, Guy Simmonds, a favourite of Field Marshal Bernard Montgomery, fully appreciated the potential of the Jedburgh concept.[19] The teams were assessed as having successfully attacked, disrupted and destroyed a number of headquarters, having demolished numerous supply dumps, compounded with the destruction of several important bridges and the obliteration of numerous enemy vehicles and other important OPFOR installations. As Colin Gubbins biographer put it: "The concept was validated at the Spartan wargames of March 1943, which convinced the British Army that SOE could, with limited

expenditure, stimulate resistance and provide reliable support to an advancing conventional force."[20]

For Gubbins, Wilkinson and his staff, the Jedburgh concept was a proven success.

LESSONS OF SPARTAN

The post operational report brought to the surface several important observations and conclusions[21] that were extracted from the deployment of the Jedburgh teams. Firstly, it became quite clear that these teams should be assigned a specific area of operations, as well as the precise tasks that would assist the Allied ground force operations. Moreover, these teams would have to be inserted in close proximity to the respective operational area. Furthermore, timing was recognized as a significant factor, as the time span between the Army commander designating and assigning Jedburgh missions had to account for the respective initiation, planning and execution phases of a task which required a 72-hour mission cycle. This was predicated upon the time requirements of preparing the personnel to be inserted, to contact and to liaise with the local Maquis organization, set up communications, and request supply drops of weapons, ammunition and other stores, if necessary. This cycle would include the conduct of ground/target reconnaissance that would enable the planning, briefing of resistance members, rehearsals and finally mission execution.

From the staff point of view, it was recognized that the immediate rear area of the German lines would be well monitored and patrolled by the occupation forces, hence the Jedburghs and the Maquis should operate deeper in the exposed flanks and rear echelon where there would be a smaller German presence. Another lesson drawn from Spartan was that commando and airborne forces could be employed to execute a *coup de main* mission if deemed necessary. It was the command perception that their fitness, training, discipline and tactical prowess to work effectively under operational duress could augment and/or address missions of complexity beyond the capability of the Jedburgh teams and their associated resistance forces. Finally, the invasion planners argued for the preparation of a contingency plan for the evacuation

of the Jedburghs should the Allied post-invasion campaign encounter serious difficulty or, in the worst-case scenario, face defeat. Thankfully such a plan was never required; nevertheless, it was prudent of the planners to be prepared for such a contingency and note it in the lessons learned.[22]

TEAM SELECTION AND TRAINING

The lessons drawn from Spartan formed the basis of a secret document that was promulgated on 6 April 1943 by the head of SOE's Planning Section, Colonel M. W. Rowlandson. This document became the Jedburgh basic directive that was issued on 20 December 1943, formalizing the intention of producing 300 Jedburgh teams by 1 April 1944.[23] This number of teams was never realized, arguably due to time and dearth of qualified personnel with the requisite language and cultural skills, notwithstanding an intensive program of selection and operational training that commenced with the subsequent 'marrying up' of three-man Jedburgh teams drawn initially from within the SOE and OSS, and other select volunteers.

The primary selection understandably sought military personnel with recent combat experience who knew how to handle small arms[24] and were proficient in instructing others in weapons, basic demolitions and tactics. In tandem, an important practicable requirement was that radio operators had to be exceptionally proficient in their signals trade. The Jedburgh teams had an additional imperative to incorporate one French-speaking teammate ensuring that at least one Jedburgh member was capable of communicating in French to liaise, instruct, coordinate, train and, if necessary, direct Maquis members. Hence the ability to communicate effectively in the French language and for a lesser extent cultural understanding, was seen as mission critical. This requirement and others were clearly specified in the OSS Special Services Field Manual which states that:

> SO [special operations] agents and operatives are selected for their intelligence, courage, and natural resourcefulness in dealing with resistance groups. In addition they must have stamina to be able to live and move about undetected in their area of operations. Normally,

> they should be fluent in the local language and be a native of a nationality acceptable to the authorities and people of the area.[25]

Before the first teams were to be formed in mid-March 1944, the SOE/OSS were confronted with a serious challenge as there was a dearth of French-speaking personnel to be incorporated in the Jedburgh teams. Fortuitously, this gap was remedied due to the reinforcement from North Africa and the Middle East of 73 Free French officers. This timely and operationally critical addition added significantly in French language capability and cultural awareness, and improved the Jedburgh credibility once they deployed, as the Maquis would be now working hand-in-hand with their compatriots.

One interesting peculiarity that was contrary to the disciplined mindset so typical of conventional military organizations of the era, was the evaluation of personnel who would, as required, question authority and have no compunction in speaking up when necessary. It was assessed that this personality quirk or characteristic was a quality that would foster activities in line with the Jedburgh mission.[26]

Those interested in volunteering for the Jedburgh assignment commenced their journey with an extended and intensive interview with three psychiatrists focused on ascertaining the personality type and mental fitness for this specific UW mission. This examination was followed by preliminary training in Scotland consisting of physical hardening, demolitions, weapons and tactics and by technical courses in Gloucestershire, Leicestershire and Woking. This preparation continued until 3 February 1944, when Milton Hall became the main Jedburgh training facility. Radio operators continued on their intensive wireless training and instruction, as well as a parachute course and for those qualified a para refresher that was run at Altrincham, Manchester. In the wake of the training, the graduates were given an arduous five-day field test exercise in Sussex under simulated combat situations.[27]

The final selection of Jedburgh personnel initially was made by Lieutenant Colonel Spooner, a British Army officer, and first commandant of the Jedburgh training school. It is notable that attention was also paid to the opinions and preferences of the Jedburghs as to the selection of fellow teammates. It was

assumed that enabling the operators to choose their teammates would facilitate and enhance harmony amongst and within the teams.[28] The preparation for the Jedburgh missions continued unabated focusing upon "…guerrilla warfare tactics and skills: demolitions, use of enemy weapons, map reading, night navigation, agent circuit operations, intelligence, sabotage, escape and evasion, counterespionage, ambushes, security, the use of couriers, and hand to hand combat…"[29] in anticipation of their demanding assignment. A valuable insight comes from a base document entitled the "Jedburgh Tasks and Training Priorities" which bluntly identifies the training priorities of the Jedburghs and likely mission set:

Training Priority A

1. Rail cutting
2. Attacks on enemy road vehicles and transport parks.
3. Misdirection and dislocation of road traffic.
4. Delay and dislocation of panzer divisions.

Training Priority B

1. Destruction of telecommunications.
2. Liquidation of enemy commands and staffs.
3. Interference with enemy's logistics.
4. Attacks on Luftwaffe.

Training Priority C

1. Destruction of electric power facilities used for military purposes.
2. Demolition of minor bridges, or major bridges already prepared for demolition by the enemy.
3. Prevention demolitions by the enemy.
4. Observation reporting of enemy positions, headquarters, military supply dumps, and installations.

Training Priority D

1. Attacks on railway facilities such as roundhouses and turntables.
2. Attacks on railway engines and rolling stock, without causing long-term damage.[30]

This training list clearly illustrates the expectations in the mission set for Jedburgh teams' assignment.

CLANDESTINE SERVICES – MISSION COORDINATION ISSUE

In the run-up to the invasion of Normandy on 6 June 1944, British intelligence and military leaders were confronted with a serious dilemma. The Secret Intelligence Service and the SOE were challenged with how to work together effectively and concomitantly assist the upcoming invasion in France given their seemingly overlapping responsibilities and competing missions. The Jedburgh concept and mission were seen to be problematic by various MI6 bureaucrats and their operators, as well as within SOE itself, as their respective personnel were already engaged in operations in the field. To clarify and address these concerns, Gubbins promulgated the idea that satisfied the Allied objective of harnessing the French resistance while responding to the objections of those clandestine services already operating on the continent. Gubbins' compromise ensured there was no confusion with ongoing MI6 and SOE missions already in place.

While MI6 focused on deriving intelligence from occupied Europe, the SOE had created a number of networks in the urban areas of France enabling them to provide logistical support to local resistance and undertake clandestine operations such as military, transport and industrial sabotage missions designed to annoy, frustrate and vex the German occupiers. An exploration of this mission set did not, however, embrace or reflect the type of mission undertaken by the Jedburgh missions during Spartan which demonstrated that this new concept was seen as an exceptional 'economy of force' operation while considered to be potentially valuable force multipliers.

To differentiate these missions from ongoing MI6/SOE clandestine operations, the personnel assigned were to be in military uniforms. These teams by necessity evolved to be a unique multinational force with an American, British (Commonwealth) or French member, with a trained wireless operator.

Gubbins soundly argued the components of this concept to obtain an appropriate undertaking for the Jedburghs – to seek out, liaise with and support the Maquis who were conducting operations throughout the French countryside. The Jedburgh teams would be positioned to conduct liaison, undertake as necessary the supply and training of the French Maquis and the setup communications to Special Forces Headquarters (SFHQ) and facilitate, coordinate and if necessary, direct, Maquis operations. In short, to lay the groundwork for the day when the French resistance would surface and conduct a spectrum of military activities such as interdicting and severing lines of communication, delaying and destroying reinforcements and hamstringing German logistical support. Such activities, if well orchestrated and aggressively pursued, would compel the German forces to divert much-needed military personnel destined to reinforce the front, instead they would be assigned to rear area security.

Another more subtle, yet effective, aspect of conducting unconventional warfare in the depth of the German rear was the ability to impart a degree of fear, paranoia and psychological dislocation amongst the German rank-and-file, promulgating the notion that no one was safe even in rear. This facet of psychological warfare has an important feature in the conduct of unconventional warfare.

CHANGE OF ROLE

The Jedburgh concept was a dramatic shift for the SOE in tasking, tactics, organization, personnel and operational design. This unconventional warfare concept demanded the adoption of a much more overt (uniformed) and fulsome support role to an indigenous resistance movement than had been previously envisioned since its inception in 1941.[31]

Consistent with this, the teams were inserted well behind enemy lines, sometimes up to 40 miles, with little combat power due to the small numbers within each team. Teams were provided with a variety of small arms for protection and demolitions to be distributed to facilitate the disruption of enemy lines of communication, which required little training on the part of the French Maquis.

The Jedburghs were able to maximize their tactical effectiveness through their ability to communicate with SFHQ, prompt weapon and supply drops to arm and sustain their Maquis comrades. This facility brought the realization and recognition that the Jedburgh teams were true force multipliers in the unconventional sense. Predicated upon their innate capabilities and the really insignificant numbers of Jedburgh personnel, their operations were proven to be low cost in terms of the human resources invested and the supply of arms and ammunition provided, in comparison to the activities generated by the Maquis which was considered to be highly effective.

Thirteen Jedburgh teams were para inserted behind German lines post-invasion in June 1944, 10 of them in Brittany, which General Eisenhower declared was a priority area for Allied operations, hence a priority for Jedburgh teams to support the resident Maquis. Another 70 teams were inserted between July and September, with the majority to the areas of the northeast and northwest of the Massif Central. This area is the mountainous region of central France from where resistance units of the now-named Free French Forces of the Interior (FFI) effectively harassed withdrawing German troops who were falling back from the Allied forces who invaded southern France towards the French German border. There were 286 Jedburgh operators consisting of 90 British (Commonwealth), 103 French, 83 Americans, five Belgian and five Dutch who were infiltrated into France and then into Belgium and Holland between June and October 1944.[32]

THE JEDBURGH TEAMS ARE BROUGHT INTO PLAY – OPERATION FRANCIS

Commencing the night of 5/6 June 1944, Jedburgh teams began their respective deployments throughout occupied France, up to the German withdrawal in September 1944. To garner an insight as to the typical challenges that a Jedburgh team had to overcome during the post D-Day time period, this paper shall highlight the activities of one Jedburgh team: Operation Francis was inserted on the night of 9/10 July 1944 with the designated area of operations being the Finistère region of Brittany, France.

The team was commanded by 33-year-old Major Colin Ogden-Smith[33] who had previously served in the SOE's Small Scale Raiding Force (SSRF). Married with a small child, prior to the War he had managed his family's business and subsequently joined the British Army, gaining combat experience during his service with 7 Commando. By the spring of 1943, the SSRF was stood down and he was assigned to the SOE in North Africa; by October that same year he had been repatriated to England. Although Ogden-Smith was not a fluent French speaker, he was nevertheless talent spotted and recruited for the teams due to his substantial military experience, understanding that he would have a French speaking teammate. His team consisted of Sergeant Arthur Dallow the British radio operator, and they were joined with a third member, French Lieutenant Guy Le Borgne, known by his nom de guerre, Guy LeZachmeur. In the wake of their selection and training, the three-man Jedburgh team assigned to Operation Francis was para inserted at 0210 hours on 10 July 1944. Although the drop zones were usually well marked, these initial insertions were always of concern. Some members of the team landed in a wood while Ogden-Smith became separated from his teammates. A reception committee from the local Maquis rendezvoused with the Jedburghs but unfortunately Ogden-Smith could not be located and was separated for a period of four days. He cunningly went to ground, managing to evade numerous German patrols that seeded the area. Fortunately, he was discovered by the Maquis and reunited with his teammates. A focal point for their area of operations was the town of Brest where many of the German troops (Russian mercenaries) were garrisoned. Undertaking a survey of the resistance groups in his area, Ogden-Smith quickly ascertained that the local resistance was ill-equipped to undertake guerrilla operations against the local occupation forces as they had few small arms and equipment. He signalled back to SFHQ requesting an urgent weapons and supply drop.

Although the communications between SFHQ and London were described as 'patchy', enough detailed information enabled a three-airplane resupply mission to drop a large quantity of small arms and munitions on the night of 15 July. As the weapons canisters were being collected a contingent of 300 Russian mercenaries under German command, arrived and launched a concerted attack upon the local Maquis. Although the resistance fighters

were able to retrieve the weapon canisters under fire and quickly evade their pursuers, 24 resistance fighters and an estimated 50 Russians lost their lives in the short but intense contact.[34] This surprise encounter was highly suspicious, and likely this resupply mission had been compromised. The Germans had an effective German counterintelligence network and their operations leveraged spies and informants throughout the region, including some that may have had connections to the local resistance and their local activities.

In concert with their primary tasking, Ogden-Smith's team carefully navigated their way through the locale, distributing weapons while conducting a needs analysis for further resupply of the local Maquis. During this period, his team had a number of encounters with local German units and a deadly game of hide and seek became a potentially deadly feature of their presence. This situation became acute in the wake of 26 July when German forces continued to aggressively seek out the Jedburghs and the accompanying Maquis elements operating within the German rear area. Fortunately, Ogden-Smith, his teammates and the Maquis remained successful in evading their German pursuers, all the while patiently waiting direction from London.

Allied orders arrived on 3 August, when Ogden-Smith's three-man team was fortunately joined by a detached French Special Air Service member Sergeant Maurice Miodon, along with three French resistance fighters who took shelter in a farm situated in the small village of Querrien in Finistère.

Similar to the suspected compromise of Ogden-Smith's initial resupply drop, the team and their accompanying personnel were believed to have been betrayed to the Germans who rapidly responded with a company size reaction force and immediately surrounded the farm where they were in hiding. During the ensuing firefight Ogden-Smith took a serious wound to the stomach while his comrade Miodon was wounded by grenade shrapnel, shattering both his arm and leg. Although in pain and seriously wounded, Miodon bravely provided enough suppressive fire to cover the withdrawal of the remaining team members and dispatched a number of German attackers before he ran out of ammunition. Miodon subsequently surrendered to the Germans and was summarily executed. Meanwhile Ogden-Smith self-administered a strong

dose of morphine and, mortally wounded, succumbed to his wounds. In reprisal, the Germans killed the farmer and burned the farm after ransacking the buildings and bodies. The bodies were left on display, then buried where they fell. Due to the heroism of Miodon, the others were able to escape.

In the wake of this attack on the Jedburghs, the Maquis were well supplied with arms and ammunition and commenced operations on 3 August. Predicated upon the efforts and activities of Ogden-Smith and his teammates in Operation Francis, a well-armed and substantial force of 700-Maquis fighters could now be put in the field to undertake their assigned operations. The task of this resistance group was the harassment and interdiction of the German forces in retreat from Lorient. The Maquis besieged and subsequently liberated the town of Quimper on 8 August while conducting operations until 25 August when their assigned area was deemed secure but not before the destruction of a number of German convoys, equipment and installations. The support and sacrifice provided by the Jedburgh team assigned to Operation Francis enabled the resistance in their area of responsibility to successfully undertake operations, facilitating the Allied post-invasion ground campaign. It became quite clear to the proponents of this unconventional warfare concept as well as their conventional counterparts that the ability to liaise, supply, mobilize and assist French resistance fighters enabled them to conduct a spectrum of successful rear area operations against the German occupation forces and their lines of communication.

Of the more than 90 teams deployed to France, the Jedburgh concept was proven to be an operational success. Gubbins, in a lecture, postulated that the Jedburgh success was predicated on the fact that:

> Our plans, worked out in the greatest detail with his (Eisenhower) staff, involved over a 1, 000 attacks on the German lines of communication through-out Belgium and France in the first week. These were to start on the night of 5/6 June before even a single Allied soldier had landed. For our part, this meant expanding our field force to meet this plan, parachuting the necessary arms and explosives, and allotting individual targets to the various networks we had

> established. We also had to present the plan to our field force in such a way that capture of any part of it by the enemy would not give away the vital sector where the initial bridge-head was to be secured. Of the thousand or more targets aimed at more than nine hundred were destroyed. These were mainly rail, bridge, viaducts, and tele-communication centres, which put the whole enemy system in chaos.[35]

DIRECT COMMUNICATIONS

A critical aspect that impeded the potentially broader success of the Jedburgh missions was the dearth of communications between the Jedburgh teams in the field and the conventional ground forces they were to support. It was the opinion of planners at that time, that a direct command, control and communications (C3) relationship could result in the misuse of the Jedburghs. The requirement was for the field army commanders' requests to be directed to London and from London to the fielded Jedburgh teams and the reverse for any response communication. This resulted in lost time and the lost tactical opportunities.

APPRECIATION OF INNOVATION

Throughout the Jedburgh concept, many of the key commanders, concept supporters and special operations personnel were intellectually open and courageous enough to explore new venues in the application of unconventional warfare. The ability to challenge traditional military thinking and the doctrinal approach of the time underlined the importance of independent thought, critical thinking and the exploration of new ideas, methodology and technological innovation and application. Gubbins acknowledged, "To the initial lack of imagination in government circles generally as to the potential of this 'fourth arm', if I may call it so, and to the hostility both veiled and open which not surprisingly followed the creation of SOE, when at best it was not taken seriously and at worst it was snubbed."[36]

PSYCHOLOGICAL OPERATIONS

One of the more subtle aspects regarding the effectiveness of Jedburgh teams was that it is a form of psychological warfare and inhibited to a degree the German ability to operate freely throughout what was deemed to be the security behind the front lines. The German vulnerability throughout the rear area created a sense of psychological displacement, fear and to some extent paranoia with the accompanying erosion of morale within the occupying forces. This was combined with the production and distribution of French leaflets,[37] exploiting the underlying hatred by the average Frenchman against their Germanic occupiers. This psychological effect in concert with Maquis operating throughout the French countryside highlighted in the study entitled, "The Jedburghs" which noted: "In a telephone conversation with a general on Hitler's staff, just five days after the Normandy landings, the German commander-in-chief in the West explain how the morale of his troops was suffering as the FFI (Free French Forces of the Interior), "feeling the end approaching, growing steadily bolder."[38]

MISSION FOCUS

The success of Jedburgh operations in France in the wake of the Normandy invasion was appreciated by the American General Dwight Eisenhower who, prior to the invasion, clearly established that these three-man units were to concentrate upon designated operational areas in France. This concentration of effort enabled the teams to successfully undertake the mission set assigned. The success provided by the Jedburghs had unforeseen consequences when the Allied concentration of effort was redirected towards Germany in 1944. The SOE/OSS had little ability in providing a comparable level of support nor the quality of intelligence and UW assistance for Allied operations as there was a dearth of German resistance prior to and when the Allies pushed into the heart of the German Reich.[39]

IMPORTANCE OF COUNTER-INTELLIGENCE

The experiences of Operation Francis and similar missions for this period demonstrated that the potential for 'security compromise' was a constant in

France and elsewhere. German military intelligence/counter-intelligence capabilities were effective and, combined with rear area security and German field police operations, posed a persistent threat to Allied intelligence and special operators throughout the war. The potential and ever-present compromise of drop zones, safe houses, secure caches, contacts, clandestine agents and operators reinforced the importance of maintaining secure communications, formalized cell structures, secure vetting of all personnel, strict operational security (OPSEC) and the operational requirement of "need to know." SOE/OSS agents and resistance elements faced challenges and risks from double agents, compromised or faulty communications, and even rival political actions. For the Jedburghs in France, this included pro-de Gaulle, pro-Vichy or Communist elements amongst others, which at times became political competitors. In certain cases, these factions were not above entering or sabotaging each other in the hope of garnering future political advantage. The situation underlines the importance of sound and robust intelligence and counter-intelligence capability so as to foil potential infiltration and compromise.

THE ADVANTAGE OF TIME

Although the achievements of the teams were substantial, the Jedburgh operations in France and elsewhere could have been capable of achieving more had they been inserted some weeks earlier. This would have provided abundant time for the Jedburghs to liaise, assess, assist, coordinate and plan assigned missions. Moreover, it would have furnished opportunities to nurture important personal relationships, enhance situational awareness as it relates to the Maquis unit and their members, as well as, identifying nnotable personalities, key players, garner insights as to local politics as well as assessing targets in the designated operational area. As one author argued:

> Their (Jedburgh) achievements were substantial … but it was generally agreed in post- operational reviews that they could have achieved far more if they had been dropped in some weeks earlier. The delay was due to doubts about the survival capacity of small groups in uniform if dropped in some weeks before the anticipated date of enemy withdrawal from France.[40]

PERSONNEL SELECTION

The Jedburgh operations in France should be viewed in strategic terms as a capital investment, a total of 278 operators were infiltrated into France and assisted in training, supplying and advising some have estimated 100,000 French resistance fighters against German occupation forces.[41]

The Jedburgh operators were physically fit and highly trained for their missions. They underwent rigorous physical and psychological testing prior to their selection and deployment. Careful attention was paid to ensure that recruits incorporated mental resilience, and motivation to undertake the assigned mission. Jedburgh personnel acknowledged that they had volunteered for a very dangerous assignment and that their success and personal valour would be kept classified. They were well advised that should they be captured the likely outcome was their death.

IMPORTANCE OF SUPPORT

Drawing from the Jedburgh success as well as other corresponding unconventional warfare campaigns, no resistance organization can be sustainable and successful against an effective military without outside assistance. This embraces the spectrum of advisors, financial support, food, intelligence, training, provision of secure areas, weapons and equipment amongst other operating necessitates. There is also the historic realization that the conduct of unconventional warfare may bring about massive retaliation against the civilian population and this was a concern and reality that Gubbins acknowledged.

IMPORTANCE OF LANGUAGE AND CULTURE

The SOE and OSS Jedburgh experiences emphasize the importance of personnel having a substantial understanding of the language and culture of their area of operations. The SOE/OSS had the advantage of talent spotting many regional and technical experts, as well as recruiting a broad range of individuals having skills, capabilities backgrounds and experiences that were seen to be potentially employable in UW operations. Through family, social

institutions, universities and networks the SOE and OSS recruited from far and wide their managers, experts and operators.

What is striking about the Jedburgh concept was the cost-benefit analysis which came from the creation of small multinational teams each with a specific mission set. A particularly vital addition to the Jedburgh team was the valuable incorporation of an officer native to the area of operations. Although this had not been originally planned, there was a realization that teams composed mainly of British or Americans could be made more effective with a native language speaker. It was the staff assessment that a native speaking officer would greatly assist in the establishment of good working relationships with the respective resistance groups in France and elsewhere.

TALENT SPOTTING EXPERTISE

In the future, it may behoove special operations communities to expand their ability to reach out to rapidly acquire new expertise or exploit existing skill sets and experience that reside in individuals retired from the active/reserve force or through civilian/government/academic networks. The importance today of cyber operations, financial tracking, social anthropology, regional expertise, amongst others may necessitate approaching experts in these fields above and beyond those within public service or governmental or contracting agencies. It would be prudent to ascertain their interest in assisting government/military/intelligence organizations through the provision of advisory services, informational or expertise reach back as required. Although this initiative would require a thorough vetting of selected personnel, it would provide a depth of skill sets and knowledge that could be vital in the nation's defence. It must be remembered that neither special operations nor expertise, can be mass-produced, nor competently created after an emergency occurs. Moreover, it may be necessary to recruit people older than 39 and be gender blind to achieve what is deemed to be an operational/information requirement.

As many Western nations open their doors to immigration, the multicultural/multinational makeup provides an ideal recruitment opportunity. The Lodge-Philbin Act passed on 30 June 1950, allowed the recruitment of foreign

nationals into the United States military. This initially enabled 2,500 non-resident aliens, subsequently increased to allow 12,500, to enlist. These volunteers were guaranteed U.S. citizenship and an honourable discharge on the successful completion of five years service. Hence there may be a requirement to extend and expand the current American legislation entitled "Military Accessions Vital to National Interests (MAVNI) law which encourages the recruitment of foreign nationals or recent immigrants who seek American citizenship through volunteering for military service. This could expand recruitment into special operations and is reminiscent of the SOE and OSS who sought to recruit native speakers to bring these vital operational skills into the fight. Concomitantly, it would be utilitarian to have potential candidates undertake the appropriate psychological and aptitude assessments to ascertain if their characteristics would meet the special operator profile. The continuous strengthening of recruitment efforts so as to promulgate the word specifically through ethnic neighbourhoods and enclaves in the West could generate substantial interest particularly when matched with opportunities such as officer training and private educational programs such as ROTC or military academies.

The employment of women and those of the 2SLGBTQI+[42] community should not be overlooked as skill sets and talent are found throughout all society. The extraordinary women of the OSS/SOE, who undertook vital operations with intelligence and special operations organizations in World War II brought unique skills to the teams that contributed to their success.

REFLECTING THE JEDBURGH EXPERIMENT

The Jedburgh concept was a bold experiment designed to conduct unconventional warfare in a post invasion scenario – that of supporting and intimately operating with a resistance organization within an occupied country. This concept was a strategic departure from the essentially attritional Anglo-American warfighting tradition. This now well-proven unconventional warfare concept remains strategically significant as it is recognized as an important dimension of irregular warfare.

The experience of the Jedburghs still resonates today in the manner in which contemporary militaries recruit, train, select and employ special operators in unconventional warfare. It also supports the concept of retaining a core competency in unconventional operations, not only within the special operations forces but in the Profession of Arms writ large. To do so, it is important to develop a broad appreciation and expertise in UW by institutionalizing the lessons learned from past conflicts and through the preservation of a baseline of UW expertise amongst the military, intelligence and academic communities, amongst others.

As noted in Operation Francis, an early insertion and deployment may have provided the time necessary to gather, assess and share a better understanding amongst the Jedburgh teams as to who they were supporting, while enhancing their understanding of the operational environment. The inability to communicate directly with the conventional forces that the Jedburghs were supporting was problematic. It is most likely that such communications would have facilitated the overall coordination and synchronization of the Jedburgh/Maquis operations in respect to the Allied ground force. Direct contact would likely have provided better intelligence and local and regional knowledge that could have been exploited in expediting the operations.

In contemporary terms, as it relates to the hybrid threat, it was quite clear that in Operation Francis the Jedburghs should have been given adequate time to garner a more comprehensive understanding as to some of the local political, cultural and historical factors under which they were operating. It was important for them to conduct a more fulsome assessment of their area of responsibility – intelligence preparation of the battlefield – and to better assess the requirements of the resident Maquis.

One of the Jedburgh veterans, the American Aaron Bank, was so impressed with the concept in the training he received, he employed them in the training of U.S. Army Special Forces units. Moreover, a number of the 10th Special Forces Group, who were displaced persons in the wake of World War II, were recruited into the U.S. Army under the Lodge-Philbin Act.

The 2021 departure from Afghanistan underlines to the casual observer that after 20 plus years of war, the West did not have a complete understanding of the complexities of this ancient tribal society, nor its environment, nor our enemy and their capabilities and objective. For the most part NATO and other Allied forces did not encourage, develop or retain a functionally effective ability to communicate with the population that came from diverse ethnic and cultural groups. As witnessed with the Jedburghs, the language and cultural expertise provided direct tactical and operational advantages, which has since become the *sine qua non* of special forces involved in supporting and conducting unconventional warfare.

To enable our nations and Allies to be ready to address both anticipated and unanticipated threats, we need to learn from the Jedburgh experiment to leverage our citizenry and harness their unique skills and knowledge. We need to have in place well-trained and deployment ready specialists in multiple languages and cultures who have the adaptability and courage to help us win the next conflict, and not be left unprepared or making hasty retreats.

CHAPTER

4

CASE STUDY: MUNICH 1972 AND THE RISE OF COUNTERTERROISM

COLONEL (RETIRED) BERND HORN

A fundamental shift in the threat picture to Western industrialized nations erupted in the late 1960s. Political violence, or more accurately terrorism, became recognized as a significant "new" menace.[1] Bombings, kidnapping, murders, and the hijacking of commercial aircraft seemingly exploded onto the world scene. Not only in the Middle East, but also in Europe, countries were thrust into a state of violence as both home-grown and international terrorists waged a relentless war that recognized no borders or limits.

Up until this point, security officials, analysts and scholars viewed terrorism through the lens of revolutionary struggle. However, by the end of the 1970s, they came to realize that terrorist organizations were also defined by nationalist and separatist groups outside of the colonial or neo-colonial framework. Importantly, the use of terrorism also encompassed radical, and completely ideologically-motivated organizations. These groups adopted terrorism to draw attention to their causes. Not surprisingly, terrorists quickly realized that they could turn local issues into international security problems. As one expert explained, "Originally reflecting a largely left-wing ideological foundation, today's terrorists are increasingly likely to be motivated by campaigns of ethnic nationalism or religious extremism."[2]

The singular event that is considered by experts to be the beginning of modern international terrorism occurred on July 22, 1968, when three Palestinian terrorists from the Popular Front for the Liberation of Palestine (PFLP) hijacked an Israeli El-Al Boeing 707 flight flying from Rome to Tel Aviv, carrying ten crew and thirty-eight passengers.[3] This attack was the first hijacking that was intended as a political statement. Quite simply, the terrorists seized the aircraft with the sole purpose of exchanging the hostages for Palestinian terrorists imprisoned in Israel.

The choice of airline carrier was also important as it was Israel's national airline, and therefore, symbolic in its own right. In addition, the crisis, which entailed the possible death of the hostages and destruction of the aircraft forced the Israeli government to deal directly with the terrorists, something the government had promised never to do.[4]

This event and subsequent hijackings had a dramatic effect. In fact, a Canadian Security Intelligence Service (CSIS) report claimed, "the incident is widely regarded as a principal initiator of the deadly continuum of international terrorist attacks, which have exerted significant political influence during the past three decades."[5] As the Palestinian Liberation Organization (PLO) observer to the United Nations (UN) explained in 1976, "The first several hijackings aroused the consciousness of the world and awakened the media and world opinion much more – and more effectively – than 20 years of pleading at the United Nations."[6]

It was another event, however, that underlined the true scope of the terrorist threat that effusively galvanized the West into ramping up its counterterrorism capabilities. And, most nations looked to SOF to address what was seen in many respects as an existential threat.

Ten days into the 1972 Munich Olympics, in the murky hours of dawn on September 5th, eight Black September terrorists infiltrated the athlete village in Munich, Germany. At 0430 hours, with the help of a group of actual athletes who were sneaking back into their quarters after a night out, the eight terrorists, dressed as fellow athletes, climbed the six-foot high chain-link fence that surrounded the athletes' village. The attackers then entered the building

holding the Israeli athletes using stolen keys. The terrorists knew the exact layout of the building, as well as which rooms housed the Israeli athletes. As the attackers tried to gain entry into the first room a struggle ensued as Moshe Weinberg, the wrestling coach heard the noise at the door and seeing masked armed men immediately shouted for help and attempted to block the door. Yossef Romano, a weightlifter, came to his assistance but both men were shot and killed almost immediately. Although some Israeli athletes were able to escape, nine became hostages.[7]

The terrorists demanded the release of 234 Palestinian prisoners held in Israel as well as the release of Andreas Baader and Ulrike Meinhof of the Red Army Faction held by the Federal Republic of Germany (FDR). They imposed a 0900 hours deadline after which, if their demands were not met, they would execute one hostage ever hour. To reinforce their demands, they dumped the body of Weinberg into the street.

The FDR had no counterterrorist unit and they refused the assistance of the Israel's special commando unit Sayeret Matkal. Instead, the Munich Police Chief, supported by the Libyan and Tunisian ambassadors to the FDR negotiated with the Black September leader. The terrorist turned down "an unlimited amount of money" for the release of the hostage but did extend the deadline numerous times.[8]

The Munich police attempted one clumsy rescue attempt; however, it failed when the terrorist watched the approaching policemen, dressed as athletes scaling the outside of the building on TV. The authorities had failed to cut off the electricity or prevent a mob of television crews from filming the scene of the drama.

The Israeli government refused outright to negotiate with the terrorists. Israeli Prime Minister Golda Meir stated, "If we should give in, then no Israeli anywhere in the world can feel that his life is safe."[9]

With negotiations stalled, at 1800 hours the terrorists demanded transport to Cairo, Egypt. FDR authorities agreed and safe passage by helicopter from the Olympic Village to Fürstenfeldbruck Air Base, approximately 25 kilometres

away, was arranged. The offer, however, was a trap. The initial plan was to ambush the terrorists in the parking garage that led to the location where a pair of helicopters would pick them up. Sensing a trap in the spacious, secluded and deserted underground parking lot, the terrorists demanded a bus to take them to the helicopters, which would fly them to the military air base.

The two helicopters landed at 2230 hours, approximately a hundred metres from the Boeing 727 jet that was to take them to Cairo, Egypt. On board, pretending to be aircrew were six Munich police officers. Unexplainedly, before the terrorists arrived, they decided to abandon their position without informing their chain-of-command.[10] Therefore, when a number of Black September members disembarked to inspect the airliner, they found it abandoned and realized it was a trap. They immediately ran back to the helicopters to warn their fellow terrorists. Although the policemen in the airliner departed, there were still five German police officers, deployed around the perimeter and control tower. They had been chosen based on their experience in shooting competitions to be used as sharpshooters.[11] At approximately 2245 hours, in dismally poor light, from a great distance, "sharpshooter" number three opened fire as the Black September members ran by the control tower. He missed. Central command then ordered the "sharpshooters" to engage the terrorists. A raging gun battle ensued.

Two terrorists were quickly killed and three were wounded. Significantly, the terrorists took cover beneath and behind the helicopters and returned fire. The four German helicopter aircrew made a run for it. Two made it to safety while the other two were seriously wounded. The hostages remained in the helicopters tightly bound and blindfolded. The terrorists shot out the floodlights that had illuminated the battleground. The firefight eventually petered out and a tense stalemate ensued with sporadic gunfire punctuating the night.

The standoff lasted for about 75 minutes. Then at around midnight, unable to dislodge the terrorists the Germans launched an infantry attack using six armoured vehicles, which arrived late because they had become stuck in traffic. This decision proved to be fatal. Now faced with the threat of being over-run the terrorists no longer held back. They opened fire on the hostages in one of the helicopters killing four and then lobbed a grenade into the other

helicopter, which exploded in a ball of flame, killing the other five Israeli athletes. In sum, one policeman, nine hostages and five terrorists were killed.

The drama finally ended at approximately 0030 hours, on September 6th.[12] Three terrorists were captured and the rest were killed. One of the architects of the attack later explained the purpose of the operation was "to capture the world's attention by striking at a target of inestimable value," namely at Israel's star athletes. The Olympic setting was assessed as providing unparalleled exposure and publicity."[13]

Following the blood bath, the Olympic games were suspended for 34 hours and a memorial was held on September 6th for the fallen. Subsequently, the Israeli, Egyptian, Philippine and Algerian teams left Munich.

The failure of the FDR and Munich police to deal with the crisis was epic. The police "sharpshooters" had no experience; they used assault rifles rather than specialized sniper rifles; they had neither telescopic scopes, nor night vision sights; or communication gear to speak to one another or other elements of the security forces. In addition, there were insufficient personnel to contend with the crisis. Finally, there were no tactics, techniques, or procedures (TTPs) in place to deal with a problem of this scope.

Israel's displeasure with the lack of security, particularly since they had voiced concern prior to the Olympics, was soon exacerbated.[14] Several weeks later, on October 29, 1972, Palestinian terrorists hijacked Lufthansa Flight 615, which was flying from Damascus via Beirut and Ankara to Munich and Frankfurt.[15] The FDR quickly conducted a hostage exchange releasing the three captured Black September terrorists who participated in the Munich massacre.

Not surprisingly, the latest turn of events further enraged Israel. In response, Israel launched Operation Wrath of God, a covert Mossad mission to kill all those responsible for the attack in Munich. A number of terrorists were killed in the subsequent months; however, the operation was suspended when an innocent man was mistakenly killed in Norway in 1973. The operation was finally terminated in 1979, when the Mossad assassinated the Black September chief of operations, Ali Hasan Salameh, by a car bomb.[16]

The murder of Israeli athletes at the 1972 Olympics in Munich became a defining moment regarding how terrorism was, and would be, viewed in the West. General (retired) Ulrich Wegener, the first commander of *Grenzschutzgruppe* 9 (GSG 9) revealed:

> It was this incident [1972 Munich massacre] that fully revealed the tactical weakness and deficiencies of the security forces of the Federal Republic of Germany. This event also constituted the first turning-point in the anti-terrorist campaign of the FDR. It was against the tragic backdrop of Munich that the first real progress was made in the war against terrorism. Two weeks later, the federal government decided to establish a tactical special operations force for specifically designed to combat terrorism, and so it was the GSG 9 was born.[17]

Experts on terrorism agreed that the 1972 Munich Olympics caused a distinct change in the manner in which Western governments began to think about international terrorism as a threat. Khaled Elgindy, a senior fellow at the Middle East Institute and the director of its Program on Palestine and Palestinian-Israeli Affairs, observed "these kinds of violent attacks actually succeed in putting the issue on the international agenda,"[18] Susan Marquis, a senior Department of Defense civilian, in her study of U.S. SOF, revealed that American military commanders assessed after the Munich Olympics that their lack of "a credible counterterrorist capability could, and would eventually, dramatically embarrass the United States." As a result, the U.S. "concentrated on building an army counterterrorist force."[19]

Their concern of the growing threat was realized a few years later when on December 21, 1975, terrorists assaulted a meeting of oil ministers from the Organization of the Petroleum Exporting Countries (OPEC) in Vienna, Austria. Six terrorists led by the infamous Carlos the Jackal raided the meeting and killed three individuals and took sixty-three others hostage including eleven OPEC ministers. The Austrian government provided safe passage to Algeria where the hostages were released unharmed.[20]

For those states that were not yet fully committed after the 1972 Olympics, the latest attacks galvanized the need for special capabilities to deal with

counterterrorism. Not surprisingly, the reaction to the tragedy at the Munich Olympics set in motion the establishment of SOF organizations created or evolved to deal with the "new" threat. The effectiveness of SOF to respond was soon proven. In 1976, Israeli special forces successfully rescued hostages in Entebbe, Uganda. A year later, in 1977, GSG 9 effectively freed hostages from a hijacked plane in Mogadishu, Somalia. The British SAS demonstrated its CT capability in 1980 when it rescued hostages held by terrorists at the Iranian embassy at Princes Gate, in London. And, a final example, France's *Groupe d'intervention de la Gendarmerie nationale* (GIGN) freed hostages aboard an Air France flight in 1994. The movement to meet the terrorist threat with special forces was quite widespread. The Belgians stood up the Directorate of Special Units (DSU) in 1972,[21] the French GIGN was established in 1973, the U.S. created Delta Force in 1977, and the Italians created the *Gruppo di Intervento Speciale* (GIS) in 1978, to name a few.

Although not the first terrorist event in the West, the attack by Palestinian terrorists at the 1972 Munich Olympics was cataclysmic. The attack and the tragic loss of life underlined the gravity of the "new" terrorist threat. Significantly, the botched rescue attempt emphasized the need for specially trained and equipped forces to deal with this dangerous threat. In response, countries turned to SOF to meet, counter and defeat the increasingly escalating and intensifying threat. SOF not only filled the capability gap that had emerged, but took on the role, arguably changing how people began to view and identify SOF. Counterterrorism became a core task for SOF, one which would become all consuming in the aftermath of the September 11, 2001 (9/11) terrorist attacks on the Twin Towers in New York.

PART II

WHAT ARE THE THREATS (Existing/Emerging)

CHAPTER

5

WAR, NOT WAR – WAR IN THE SHADOWS: BELOW THRESHOLD THREATS

COLONEL (RETIRED) BERND HORN

Strategic competition started neither with the Cold War, nor with the current iteration of strategic competition. Throughout history, empires, alliances and nation states have always competed for influence, access and advantage. The great Prussian strategist Carl von Clausewitz wrote, "Is war not just another expression of their [competing governments] thoughts, another form of speech or writing. Its grammar [conduct of war], indeed, may be its own, but not its logic [policy]."[1] Although competition between global competitors is ageless, the context, circumstances and "grammar" of the competition has evolved into a much more complex and challenging affair. The prominent Soviet military strategist Aleksandr Svechin wrote:

> It is extraordinarily hard to predict the conditions of war. For each war it is necessary to work out a particular line for its strategic conduct. Each war is a unique case, demanding the establishment of a particular logic and not the application of some template.[2]

And so it is with the current iteration of strategic competition. The shift ushered in by the American 2018 National Defense Strategy (NDS) galvanized conventional military commanders. For many, if not most, it hearkened back to the "good old days" of the Cold War, which focused on large mechanized

armies. In fact, former U.S. Secretary of Defense Mark Esper speaking to the U.S. Naval War College remarked that "times have changed" and he asserted that the U.S. "needed to focus on conventional war."[3]

Esper did not have difficulty in convincing his military commanders. The pivot created renewed interest in large exercises and increased funding for conventional military capability, as well as new modernized armaments. However, the key is to fully understand the competition space and balancing resources correctly. A return to a traditional warfare model mindset has clear dangers, as does ignoring the capability of current rivals and rogue states. The bias to refocusing primarily on "old school" conventional warfare could hold serious consequences.

Dr. Daniel Nexon observed, "Competition isn't a strategic goal. It's a means to an end. The decision to compete with another great power should always be over something specific; it should center on the efficacy of competition, the value of the object at stake, and how the specific objective contributes to long-term goals."[4] As such, framing a national policy around great power competition obscures the reality that most, if not all countries (including the U.S. and China), share extensive interests (e.g., economic, global issues such as climate change, counterterrorism, nuclear non-proliferation, pandemic prevention). Competition is not simply a military problem.

However, for too many conventional military commanders and some politicians the renewed Great Power Competition (GPC), or more accurately strategic competition, is seen as a return to "high-intensity" combat hearkening back to the Cold War stand-off between super-powers.[5] However, some, like the former Chairman of the Joint Chiefs of Staff (JCS), General Joseph Dunford, admitted, "We're already behind in adapting to the changed character of war today in so many ways." He argued that the U.S. national strategy with regards to GPC must recognize that the binary peace/war distinction is flawed. Rather, nations must understand conflict as a continuum, as a "range of different modes of conflict with increasing levels of violence, from measures short of armed conflict (Gray Zone) through conventional warfare." He noted that by failing to fully understand the true breadth of

our adversaries' stratagems and their strategic narratives, the Western alliance has ceded influence and access to China and the West's ability to compete with its adversaries' narratives.[6] The result has been that both China and Russia have been able to commence dismantling, if not demolishing, the rules-based international order.

It is this failure, if not unwillingness, to come to grips with the true nature of strategic competition, specifically, understanding the competition space and balancing resources correctly, that disadvantages the West. Political decision-makers seem too quick and too dependent on the military to deal with an ever-increasing gamut of missions in a constantly evolving complex international forum. As a result, they are competing with a limited tool set, while their competitors utilize the entire array of national resources. Although the military is an essential component of strategic competition, it is but a single actor in a nation's armoury.

Although competitors such as China and Russia maintain large military forces and continue to improve and expand their arsenals, they remain careful to avoid actions that would possibly activate the conventional war "trip wire."[7] Rather they maintain the military capability as a substantial, viable and overt threat, but compete on various levels under the threshold of a "hot" or "shooting war." They utilize "Hybrid Warfare," defined by NATO as "a wide range of overt and covert military, paramilitary, and civilian measures (…) employed in a highly integrated design."[8]

NATO political-military expert Chris Kremidas-Courtney described Hybrid Warfare as "the mix of conventional and unconventional, military and non-military, overt and covert actions employed in a coordinated manner to achieve specific objectives while remaining below the threshold of formally declared warfare."[9] The National Coordinator for Security and Counterterrorism (NCTV) of the Netherlands further refined the definition of Hybrid Warfare stating, "it is understood as conflict between states, largely below the legal threshold of an open armed conflict, with the integrated use of means and actors, aimed at achieving certain strategic goals." It characterizes this form of warfare by:

- The integrated deployment of multiple military and non-military means, such as diplomatic, economic and digital means, disinformation, influencing, military intimidation, etc., that belong to the toolbox of state instruments;
- Orchestration as part of a strategy/campaign;
- The intention of achieving certain strategic goals; and
- Important features, namely deception, ambiguity and deniability, which accompany the actions (or could do so), making it difficult to attribute them and respond to them effectively.[10]

Jānis Bērziņš, the director of the Center for Security and Strategic Research at the National Defense Academy of Latvia, explains the shift from "traditional" to "Hybrid Warfare" as the transition:

- from direct destruction to direct influence;
- from direct annihilation of the opponent to its inner decay;
- from a war with weapons and technology to a culture war;
- from a war with conventional forces to specially prepared forces and commercial irregular groupings;
- from the traditional battleground to information/psychological warfare and war of perceptions;
- from direct clash to contactless war;
- from a superficial and compartmented war to a total war, including the enemy's internal side and base;
- from war in the physical environment to a war in the human consciousness and in cyberspace;
- from symmetric to asymmetric warfare by a combination of political, economic, information, technological, and ecological campaigns; and
- from war in a defined period of time to a state of permanent war as the natural condition in national life.[11]

Importantly, the different interpretations of Hybrid Warfare, or how analysts see competition/conflict in the current security environment, puts the emphasis on non-military actions. It should be no surprise then that a recent study concluded that "in a future, large-scale conflict, Chinese forces will likely employ a modern and unique irregular warfare concept, focused on information and influence, tightly integrated with conventional capabilities. A return to great power competition does not portend a shift away from irregular warfare to conventional warfare, but rather an amalgamation of the two."[12] Quite simply, adversaries have discovered, and more importantly, will continue to refine and evolve, methods to achieve their political, economic and military objectives while remaining in "Phase 0", the American doctrinal period describing pre-conflict. The fact that the U.S. and its allies are extremely hesitant to go to war further emboldens and provides adversaries with a competitive edge.[13]

In essence, the new competitive landscape, blends conventional, irregular, asymmetric, criminal and terrorist means and methods to achieve a political objective. This actuality makes the opponent largely irrelevant. Whether a state or non-state actor, adversaries will make use of the proliferation of technology and information that has accompanied globalization. Instruments such as cyber warfare, economic coercion or even blackmail, exploitation of social/societal conflict in a target country and the waging of disinformation campaigns and psychological warfare are all in the inventory. Criminal behaviour and terrorism are also in the repertoire of opponents.

General Valery Gerasimov, Chief of the General Staff of the Russian Federation, markedly identified the weakness of modern states. He insisted that history has shown that "a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."[14] This state of affairs is due, in his estimation to the fact that "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[15]

Similar to Gerasimov, General-Lieutenant, Andrey V. Kartapolov, in 2015, then-chief of the Russian General Staff's Main Operational Directorate, published an article in the *Journal of the Academy of Military Science* that described the "new-type war." It clearly highlighted the fact that the military was not seen as the only actor in the renewed GPC. Kartapolov argued that the framework of conflict included:

- political, economic, informational, and psychological pressure;
- disorientation of the political and military leadership;
- spreading dissatisfaction among the population;
- support of internal opposition in other countries;
- preparing and deploying armed opposition;
- deployment of special forces;
- conduct of subversive acts; and
- employment of new weapon systems.[16]

Rather than a kinetic solution to conflict, Gerasimov and Kartapolov argue that the focused application of political, economic, informational, humanitarian, and other non-military measures, when applied in a coordinated manner with internal discontent and protest can wield significant results. In addition, all these actions are also combined, at the right moment, normally to achieve final success, with concealed military action, often "under the guise of peacekeeping and crisis regulation." Gerasimov insisted, "Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."[17]

From a strategic perspective, the methodology of rivalry in strategic competition entails the mobilization of a wide range of a state's resources, primarily

nonviolent, to achieve a desired political end state. The use of violence is not remotely desired. A "Hybrid Warfare" approach is seen as a methodology of achieving the political end state without tripping the threshold of war, which would allow an opponent the recourse to legally use force and/or attract international intervention.[18] Hybrid Warfare creates a perfect ambiguity that paralyzes opponents since they are not even aware that they are under attack.

The case of the Russian annexation of the Crimea and the conflict in Ukraine in 2014 is a perfect example. Russia was able to skillfully manipulate the U.S. and its NATO allies to remain largely passive while Russia dismembered the Ukraine.[19] It was so successful that the Supreme Allied Commander Europe (SACEUR) at the time, General Phillip Breedlove, proclaimed that Russia's use of Hybrid Warfare in Eastern Ukraine represented, "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[20]

Consequently, the challenge is recognizing that strategic competition/GPC, as well as dealing with rivals and rogue states, is on a completely different playing field. Although conventional military capability will always be required, as both a deterrent and back-stop to military aggression, the majority of the never-ending competition/conflict will be waged on economic, informational, political, societal and technological planes. Experts have argued that "China and Russia compete across five primary domains of competition: population/political warfare, economic statecraft, cyber operations, armed conflict and international institutions."[21] As a result, underlying his point was the fact that to continually compete, you must compete on the same playing field as your opponents. That means, you must wage competition/conflict on the same domains/planes as your adversaries.

Table 5.1 provides a summary of several key "Below-Threshold" activities that are currently utilized by state and non-state actors to pursue strategic competition designed to achieve influence, access and advantage in the global struggle for national political objectives.

TABLE 5.1 – Summary of Below-Threshold Activities

SERIAL	ACTION	EFFECT
1	**POLITICAL** • influence / control international institutions • use international agreements, organizations to push desired action when advantageous and ignore when not • exert diplomatic pressure • create regional blocs • utilize economic treaties, foreign aid, security arrangements, forums, and creation of international organizations to compete with opponents to gain and influence • support to regimes • interfere in internal politics of a target country • isolate adversaries diplomatically • sharing / leaking intelligence	• disorientation of target society, political & military decision-makers • create doubt • gain access and influence • create power blocs • create advantageous political, economic, military partnerships (and deny same to opponents) • subvert internal political cohesion • create distrust
2	**ECONOMIC** • sanctions • predatory lending • boycotts / restrict imports • blackmail / threat to sell state debt • sponsor economic development / funding as means to gain access • restrict critical exports (e.g., rare earth minerals, energy) • employ predatory practices (e.g., steel production) to expand market share / force competitors out • purchase key real estate / corporations / resources • restrict access to markets	• disrupt opponent's economy • force concessions from other states / corporations • gain access to strategic real estate and resources • control market dynamics • enhance intelligence gathering capabilities • enhance ability to undermine opponent economies

3	**INFORMATIONAL** • disinformation • deception • PSYOPs • establish radio and other media in target countries • impersonate real news organizations (i.e., mimic name, logo, visual branding of real outlets)	• create doubt, wrong understandings, assessments, and decisions • shake thinking, conviction and will of target audience • diminish trust, credibility and legitimacy of target government / leaders • produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behaviour • inform, shape and influence public perception • generate public support • maintain internal morale • shape public discourse • sow division and distrust in opponents' societies / alliances
4	**CYBER** • denial of service • ransomware • hacking • interference in elections	• Erode trust in government services / financial institutions • Create chaos and turmoil and economic / financial losses • Disrupt critical infrastructure • Theft of innovation, trade secrets, intellectual property, personal / economic / political / military data • public release of sensitive and / or embarrassing information
5	**SABOTAGE** • destroy opponent infrastructure, shipping, resource industry / supply chain, etc. • disrupt political alliances / agreements • target adversaries	• create economic loss • create disruption of supply chain • potential ecological disasters • erode trust in government / military to protect national interest • create suspicion and tension between international partners • kill adversaries

6	**SUBVERSION** • disinformation campaign • agitation • fifth columnists • open educational / cultural centres with a specific covert hostile agenda in target countries	• support internal opposition • create dissatisfaction with target leadership / government • impact economy and societal stability • access intelligence • shape public perceptions
7	**RESOURCE CONTROL** • limit / deny access • buy up resource suppliers / supply chain	• create economic / resource crises • restrict competition / gain monopoly • disrupt opponent's economy
8	**TERRORISM** • support, fund, train, direct agents / proxies to conduct terrorist attacks against opponents	• ability to harm opponents while maintaining plausible deniability • cause target countries to undertake expensive security operations / infrastructure • create climate of fear in target countries • destroy adversary assets (e.g., political /military / economic / cultural infrastructure)
9	**CRIMINAL ACTIVITY** • conduct / support criminal activity • assassinations / kidnappings • harassment of citizens • create political unrest • steal sensitive information	• create fear • silence critics • sow distrust in government ability to protect its citizens • gain access to sensitive materials
10	**ESPIONAGE** • military, economic, political	• gain / loss of sensitive technological, military, economic and political information

11	**BULLYING** • threatening economic action (e.g., boycotting / block importation of goods, denying access to market / population and or commodities) • mobilization and deployment of maritime militia, joint military exercises close to opponent territory	• force compliance • deny access to commodities, resources, geographic regions • force expenditure of adversary's limited military resources
12	**BRIBERY** • appoint adversary business and political leaders to Boards of Companies (with generous salaries) • provide grants to universities to gain access to their research • ignore corruption and human rights abuses to gain access to target nations • pay directors of international organizations to vote in support of desired decisions	• undue influence is used in elite circles to promote specific interests • defuse ability to criticize / take consolidated action against opponent country • able to access sensitive research data • able to gain access / deny to competitors target countries that have strategic value (e.g., locations, resources) • potential to alter discourse / public perception
13	**BLACKMAIL** • sell state debt • undertake actions that can undercut an adversary (e.g., flood market with commodities to lower prices, restrict access to commodities / markets • target key decision-makers (leverage their vices)	• coerce targets to adopt desired behaviour / make decisions conducive to blackmailer requirements
14	**USE OF PROXIES** • direct to conduct acts of terrorism • provide money, equipment, logistics, weapons and training to proxies / surrogates	• target opponent countries (with plausible deniability) • ability to achieve political objectives indirectly

15	**MILITARY ACTION** • Special Warfare[22] • confrontations without engaging with firepower over political issues (e.g., aircraft testing air defences / reactions; border disputes; weaponizing the Spratly Islands, Maritime Militia to overwhelm opponent coast guard / navy capabilities) • overt testing of new military technology • widely publicized military exercises • escalate actions to deescalate tensions	• strengthen allies ability to resist interference / maintain stability • disrupt adversaries' internal stability • disrupt adversaries' international initiatives • exhaust opponent resources • create fear of escalation prompting opponents to become paralyzed with inaction

Table 5.1 provides merely a snapshot of below threshold activities and their potential effects.[23] This summary, however, is intended to simply provide an overview of those activities that competitors can undertake as part of the ageless strategic competition in the international arena. Problematic for the West is its mind-frame that conflict is primarily a military event. It has never been able to reconcile, as has its opponents, that it exists in a world where, for many, conflict/competition is a continuous ongoing process to achieve specific political objectives.

Although a robust conventional military component will always be required, the military equation is but a small fraction of what is required to compete in strategic competition. To vie on an equal footing, competition must be seen beyond the traditional warfare scenario. As Katherine Zimmerman, an analyst with the American Enterprise Institute in Washington, assessed, "It's [U.S.] not losing militarily, but in the soft-power space."[24] RAND researchers have worked towards developing a better understanding of the competition space. They have defined hostile measures as "State activities other than high-order conventional or nuclear attack applied against other states at any time, and in any context, with the hostile intent of gaining advantage and reducing that state's capabilities, stability, or advantages.[25]

In the end, the prize of strategic competition is access, influence and the attainment of one's political objectives and the denial of the same to adversaries. For too long, the West has missed the nuance of strategic competition. Lieutenant General Ken Tovo, a former Commander of U.S. Army Special Operations Command, acknowledged:

> [Our adversaries] did what any good adversary would do. They searched for our weaknesses, and invested heavily in asymmetric techniques, Hybrid Warfare. It's an ability to get right to the heart of a nation's power, its people. And arguably, our adversaries are doing this better than we are.[26]

As such, it is time to do better. The West must ameliorate its understanding of the type of "conflict"/competition in which it is engaged. It must mobilize, synchronize and leverage its entire repertoire of national assets at its disposal and engage equally with its adversaries in the sub-threshold activities to achieve its national objectives.

CHAPTER

THE PURSUIT OF CHINESE FOREIGN POLICY TOWARDS TAIWAN THROUGH INFLUENCE, CYBER, AND SPACE OPERATIONS

MAJOR PATRICK D. CUNNINGHAM

Central to Chinese Foreign Policy are three core tenets: "the great rejuvenation of the Chinese nation by 2049," the cultivation of a global "community of common destiny" to support national rejuvenation efforts, and the core interest of "reunification" with Taiwan.[1] To achieve these goals, the People's Republic of China (PRC) is determined to "harness all elements of its national power to place the PRC in a leading position," to include the use of information and execution of operations in the information environment (OIE).[2] As the PRC employs influence operations in an effort to sway public and political opinion surrounding "the Taiwan issue," the People's Liberation Army (PLA) has also modernized significantly and established the Strategic Support Force (PLASSF) in 2015 to secure "information dominance" across multiple domains.[3]

Information is clearly is an element of national power that the Chinese Communist Party (CCP) values dearly. Given that the PRC believes that "China's complete reunification is a process that cannot be halted," that "complete reunification is critical to national rejuvenation," and that "China must be and will be reunited," the PRC's use of OIE as an arm of its foreign

policy towards Taiwan merits examination.[4] This Chapter will provide an overview of Chinese foreign policy towards Taiwan, explain why Taiwan is fundamentally important to the PRC, and then examine how the PRC employs influence operations, offensive cyber operations, and space-based capabilities against Taiwan in efforts to further its foreign policy objectives of national rejuvenation, reunification, and the cultivation of a community of common destiny.

TENETS OF CHINESE FOREIGN POLICY TOWARDS TAIWAN

Before delving into the operational use of influence operations, offensive cyber operations, and space-based capabilities as tools of statecraft against Taiwan, it is important to first examine leading principles of Chinese Foreign Policy towards Taiwan. The PRC's grand strategy revolves largely around achieving "national rejuvenation" by 2049, inherently pursuing "national reunification" to achieve rejuvenation, and developing a "community with a shared destiny," especially in the Asia-Pacific.[5] As Ryan Hass, a Senior Fellow for Foreign Policy at the Center for East Asia Policy Studies, states, "Beijing's focus now is on accelerating the country toward its mid-century destination of "national rejuvenation" and running over anyone or anything that dares to stand in its way."[6] Haas also argues that "Beijing will measure progress by how well it is able to drive the United States and others away from operating militarily on China's immediate periphery" and that the PRC will likely "strengthen efforts to deter countries from intervening in future Taiwan military scenarios."[7] With Taiwanese elections approaching in 2024, Beijing will likely "pursue policies designed to influence voter attitudes in Taiwan" as it has done in every Taiwanese election since at least 1996.[8] Each of these factors underscore the intensity with which the PRC values "national rejuvenation" and reunification with Taiwan, as well as the necessity of PLA modernization, "informatization," and "intelligentization."

An understanding of the PRC's terminology – specifically "national rejuvenation," "reunification," and a "community of common destiny" – is helpful in fully comprehending China's aims and how "the Taiwan issue" fits

in. Though the goal of "national rejuvenation" can be traced back to the founding of the CCP in 1921, Xi Jinping's modern reference to the term corresponds to a "strategic plan" for "achieving lasting greatness for the Chinese nation."[9] In the words of the 2022 *China Military Power Report* (CMPR), national rejuvenation "is a determined pursuit of political, social, and military modernity to expand the PRC's national power, perfect its governance, and revise the international order in support of Beijing's (…) national interests."[10]

Regarding "national reunification," China argues that a divided China is a weak China and that full reunification, including the resolution of the "Taiwan question," is one of the fundamental conditions of national rejuvenation.[11] In the recently released 2022 Taiwan White Paper, China asserts that "Taiwan is a part of China," that "this is an indisputable fact," that "Taiwan has never been a state," and that "any attempt to distort these facts and dispute or deny the one-China principle will end in failure."[12] By setting these logical conditions, the PRC attempts to claim historical legitimacy over Taiwan and support an overarching deterrence by a denial campaign against any "external forces" or "Taiwanese separatists" who seek to prevent the PRC's reunification with Taiwan.

Within the 2022 Taiwan White Paper, Xi Jinping's major policies to advance the "peaceful reunification of China in the new era" are espoused, as is a theme of national commitment to reunification, and the prosperous future that reunification would bring to cross-strait relations, Asia, and the world. Xi Jinping's five "major policies" to advance the peaceful development of cross-strait relations include:

- collaboration to "promote China's rejuvenation and its peaceful reunification";
- seeking a "two systems solution to the Taiwan question and making innovative efforts towards peaceful reunification";
- honoring the "one-China principle and safeguarding the prospects for peaceful reunification";

- increasingly integrating cross-strait development for peaceful reunification; and

- "forging closer bonds of heart and mind between people on both sides of the straits" to strengthen "joint commitment to peaceful reunification."[13]

Each of Xi Jinping's policies within the Taiwan White Paper notably concludes with an emphasis on "peaceful reunification," but also states that "China's complete reunification is a process that cannot be halted" and is "critical to national rejuvenation" because "the fact that [China and Taiwan] have not yet been reunified is a scar left by history on the Chinese nation."[14] According to China, the future of Taiwan lies in China's reunification, and "the wellbeing of the people in Taiwan hinges on the rejuvenation of the Chinese nation."[15]

Finally, Chinese leaders increasingly visualize regional security in terms of a "community of common destiny" where shared interests and trust will transform zero-sum "Cold War mentality" integrations into a pattern of "win-win relations" that cultivate national rejuvenation and reunification.[16] As one of Xi Jinping's signature concepts, "a community of common destiny" suggests that Chinese elites expect that weaker countries will "defer to Chinese wishes as the [PRC] grows more powerful." Despite this "Chinese dream," many Asian countries are concerned about China's ability to use "divide and conquer tactics" to consolidate regional power.[17] By reshaping the world order in China's favour, mitigating the chances of a return to a post-Cold War mentality, and eschewing "dangerous concepts like human rights or universal values," China can actualize a "community of common destiny" – thereby setting conditions for national rejuvenation and reunification with Taiwan.[18]

THE PRC'S OBSESSION WITH TAIWAN: PROPAGANDA, NATIONAL HONOR, AND REGIME SURVIVAL

Simply put, the PRC is focused on national reunification with Taiwan for three interrelated reasons:

- decades of CCP propaganda have molded public opinion towards demanding reunification with Taiwan;
- many Chinese believe that Taiwan must be reunified for the "century of humiliation" to end; and
- any perceived "loss of Taiwan" is a direct threat to CCP regime survival.[19]

In the words of Susan Shirk, the Chinese public "cares intensely about Taiwan because the CCP has taught them to care – in school textbooks and the media (…) public opinion about Taiwan has been created by fifty years of CCP propaganda."[20]

The CCP has also taught the Chinese public to view Taiwan as the physical manifestation of the "century of humiliation" and deeply tied to the notion of national honour. China regularly messages that the century of humiliation will not end – and by extension, national rejuvenation will not be actualized – until China is strong enough to achieve reunification. Because the PRC's focus on Taiwan is not only about territory but also national honour, the "myth" linking political survival of the CCP regime to Taiwan "is so pervasive that it creates its own political reality, especially in the [CCP] headquarters." Underscoring the resilience and perseverance of this "national honour narrative" are the words of Jiang Zemin, former General Secretary of the CCP, President of China, and chairman of the Central Military Commission. In the summer of 1999, shortly following the U.S. bombing of the Chinese embassy in Belgrade, Jiang reportedly told the PLA: "we are going to give you everything you need so that next time you are asked [to take Taiwan by force] you can say, yes. Go back and develop the capabilities to solve the Taiwan problem by force if peaceful methods fail."[21]

Success or failure on the "Taiwan issue" is likely to directly impact CCP regime survival. Although PRC relations with the U.S. are mostly about "saving face and national interests" and their relations with Japan "evoke strong nationalist feelings," relations with "Taiwan [are] a question of regime survival – no regime could survive the loss of Taiwan." If the PRC's leadership believe the

regime's survival is at stake, they would likely "feel compelled to react militarily (…) even if that means confronting America's military might – unless they can be persuaded to do something else that looks just as forceful to the public and other leaders." Plausible options that the PRC has utilized in the past to look tough or assuage domestic concerns over appearing weak could include making a statement about "China's right to use force" instead of using it, while another might be economic sanctions."[22] Underscoring the massive importance the CCP has tied to Taiwan, some in China even believe that "if Taiwan goes independent it will trigger other secessionist movements in Tibet, Xinjiang, and (…) Inner Mongolia, and national unity will be threatened."[23] With such existential consequences surrounding the improper "handling" of Taiwan, the CCP's concerns over Taiwan's impact on regime survival are not likely to dissipate anytime soon.

COMPLICATIONS TO NATIONAL REUNIFICATION: TAIWAN AND BACKFIRED SIGNALING

Complicating the CCP's reunification aspirations of course, is Taiwan itself – and the bulk of its people who overwhelmingly reject unification.[24] Despite Jiang Zemin's theoretical "two-track approach" – which proposed not only a buildup of military strength, but also "united front tactics" to build popular support in Taiwan, promote Taiwanese trust towards the Chinese government, and "put pressure on [pro-independence] politicians – the number of Taiwanese who believe that "Taiwan should eventually move toward unification" has fallen dramatically from 20 per cent in 1996 to five per cent in 2022.[25]

While Jiang Zemin believed that his "two-track approach" would likely elicit applause from Washington for a "statesmanlike stance" and prompt U.S. pressure on Taiwanese "troublemakers," it backfired as Taiwanese citizens watched mainland China become increasingly autocratic, develop a harsh and intrusive surveillance state in Hong Kong, and execute a systematic genocide against the Uighurs in Xinjiang.[26] Despite the PRC's efforts, Taiwan is moving further away from the mainland politically instead of closer.[27]

Still, most Taiwanese prefer the current status quo; maintaining their image as a "fully sovereign country" but not wanting to rock the boat with Beijing through a formal declaration of independence that would likely elicit a PLA response.[28] Chen Shui-bian, a former Democratic Progressive Party (DPP) political activist in the early 2000s, claimed that because the Republic of China is "already a sovereign, independent country, there is no need to actually declare independence." Instead of formal declaration, the Taiwanese employs incremental mental changes to cement their sovereignty. These include incorporating "salami tactics" such as revisions in passport covers, textbooks and education, as well as the naming of its political offices to "proclaim the island as a sovereign state."[29] In 2020, a study found that 70 per cent of Taiwanese already believe that Taiwan is a sovereign state and by 2022 that number jumped to 76 per cent of Taiwanese believing they were "already independent under the status quo."[30]

China's attempts to compel reunification through forceful signaling has largely backfired and suggests that the PRC's continuous influence campaigns against Taiwan to promote reunification reflect at least partial acceptance that reunification won't come from force alone. A lesson that many Chinese took from the 1996 and 1999 Taiwan crises is that "using military force alone against Taiwan is bound to fail. Force can backfire by estranging the Taiwanese, making them more dependent on the protection of the Americans, and reinvigorating the military alliance between the [U.S.] and Japan (…) [and that] bringing [Taiwan] back into the fold will take carrots (…) as well as sticks."[31]

If China launched an invasion across the Taiwan strait in the modern era, not only would the PRC incur tremendous economic, diplomatic, and military costs, but states on China's periphery would also likely become increasingly hostile. Even a "pyrrhic victory" would likely "galvanize a surge in military spending and pronounced bandwagoning against Beijing" from South Korea, Australia, India, Vietnam, the Philippines, and Japan.[32] In fact, this outcome is reinforced by Japan's recent reactions to China's forceful signaling during U.S. House Speaker Nancy Pelosi's visit to Taiwan in August of 2022. PLA military drills 70 miles from Japanese territory – consummated by the firing of ballistic

missiles into waters controlled by Japan – were largely seen as "a warning that the country risks being dragged into any future conflict in the region."

More deeply, this PLA aggression reinforced a sense of urgency within Japan to raise the defense budget, heighten defense capability, and potentially "institute new rules that would for the first time allow pre-emptive military steps if Japan is at risk," none of which further Beijing's further policy goals.[33] Japan's Defense Minister, Nobuo Kishi, remarked that the PLA drills represented "serious threats to Japan's national security and the safety of the Japanese people" and many Japanese security analysts interpreted China's actions as a "direct warning" meant to convey that any allegiance with the U.S. or Taiwan will be met with force.

Any effect at intimidation has yet to be seen as many Japanese don't understand why China is taking aim in their waters, and at a time when recent Pew Research Center survey found that 87 per cent of Japanese "held an unfavourable view of China," Beijing's undying campaign of aggression and threats of force are backfiring: coalescing Japanese and Taiwanese efforts against it.[34]

PRC INFLUENCE OPERATIONS AGAINST TAIWAN: ELECTION INTERFERENCE AND DISINFORMATION

Considering evidence that Chinese threats and use of force routinely backfire, Beijing must also pursue "peaceful reunification" through non-kinetic means, including sustained influence operations. PRC influence operations are coordinated at a high level and across a range of actors that include the PLA Political Work Department, United Front Work Department (UFWD), International Liaison Department, the Ministry of State Security (MSS), and the PLASSF.[35] Beijing has attempted to influence Taiwanese elections since at least 1996 and gradually increased after 2008, believing that the election of Ma Ying-jeou as Taiwan's president in 2008 "offered the best opportunity to begin movement to unification."[36] However, Tsai Ing-Wen, who represented widespread anti-reunification sentiment through the DPP, was elected president in 2016. As a result, PRC influence operations greatly intensified in

an effort to secure her defeat in 2020.[37] However, Tsai Ing-Wen was ultimately elected. PRC influence operations that focused on swaying the election towards the Kuomintang (KMT) party ultimately failed for several reasons:

- a growing Taiwanese national identity;
- fortified cognitive defenses;
- Tsai's compelling election campaign, and
- underwhelming PRC influence efforts that relied heavily on bot networks and ineffective tactics.

Despite the PRC's poor performance in swaying Taiwanese elections, their efforts merit study because PRC information warfare is unlikely to subside, and doing so can illuminate an PRC information strategy over time. For example, a robust study undertaken by independent researcher Edward Barss revealed several key findings in PRC election interference methodology. He noted that China takes a long-term and individual approach to influence and focuses heavily on influencing Taiwanese elites through organized crime, or ordinary businesspeople (*Taishang*) who work in mainland China, as well as religious organizations, youth, and politicians to develop a "parallel cross-strait network outside the scope of normal diplomatic relations and beholden to Beijing."[38]

The PRC leverages much of its election interference influence campaigns through the UFWD, which is principally tasked with "influencing the CCP's political enemies" and "[uniting] socialist countries and those who support unification." It also oversees "cultural exchange programs designed to change political opinions and recruit spies." Additionally, the UFWD also leverages many Non-Governmental Organizations (NGOs) to target various sectors of Taiwanese society and seek to cultivate long term influential relationships that nudge the political aims of reunification closer.[39] For example, the UFWD-affiliated Alumni Association of the Huangpu Military Academy, which shares the same phone number as the China Council for Promotion of Peaceful Unification, targets Taiwanese military officers to develop intelligence contacts.[40]

The UFWD deliberately targets the aforementioned *Taishang* in unique ways beyond traditional propaganda. UFWD workers are instructed to visit *Taishang* (Taiwanese business people who do trade on mainland China) during holidays, when family members take ill or have economic difficulties. It also provides special incentives for Taiwanese businessmen to join the Chinese People's Political Consultative Conference, which offers "improved status and protection in mainland China."[41] Through these precise targeting efforts, the PRC clearly hopes to elicit influential support for reunification from the mouths of powerful people in Taiwan.

Indicators of Taiwanese individuals corroborating with the CCP and UFWD include meetings with UFWD organizations, a deep financial relationship with mainland China, and actions supporting Beijing's agenda in Taiwan.[42] Financially speaking, the CCP spends roughly 300 million U.S. dollars annually on UFWD activities in Taiwan, with twice that amount spent in 2019 on influence operations leading up to the 2020 Taiwanese elections. Despite a robust monetary investment in UFWD influence operations, Tsai Ing-Wen ultimately won a "landslide victory" in 2020 and secured 57.1 per cent of all votes.[43]

Beyond election interference efforts, the PRC also seeks to spread disinformation and reinforce three key narratives throughout Taiwan in an attempt to support reunification efforts. The three most predominant narratives promoted by the PRC in Taiwan are that Taiwanese democracy is weak, Chinese autocracy is strong, and that, in an emergency, Taiwanese people want to be "Chinese."[44] Interestingly, this focused messaging echoes a more refined version of three key narratives the PRC seeks to permeate across the Indo-Pacific: Chinese dominance is the historic norm and is inevitable, the CCP's objectives are permanent and unchanging, the CCP and PLA cannot be deterred and will pay any price to achieve Beijing's objectives, and that the U.S. is an increasingly weak, unpredictable, and unreliable ally.[45]

China also seeks to fuse these Taiwan-focused narratives with other forms of visible pressure, such as offshore military drills, the execution of cognitive warfare and attempts to create a "mindset of surrender" within the Taiwanese. In

addition, China seeks to reinforce the inevitability of the PRC-led "community of common destiny." In 2021, the PRC spread rumours that the U.S. was refusing to give COVID-19 vaccines to Taiwan, that Taiwan was falling behind the world, and that China was actually providing vaccines to Taiwan. This effort was aimed at creating Taiwanese perceptions of dependency on China, as well as to stoke fears of U.S. abandonment in times of crisis.[46]

Its influence campaigns were pervasive. In 2018, Chinese disinformation networks pumped false stories of the Taiwanese government's inability to rescue its citizens from Japan's Kansai International Airport after a typhoon, while also messaging that Taiwanese individuals who "identified themselves as Chinese" were allowed entry on an armada of rescue buses sent from Beijing.[47] However, this specific disinformation operation also backfired on the CCP. Instead of sowing seeds of panic, confusion, and doubt, the "Kansai Airport fable" inspired the creation of a Taiwanese disinformation-awareness outlet known as Doublethink Lab. Doublethink Lab, much like the Taipei-coordinated Information Operations Research Group (IORG), CoFacts website, and LINE website, seeks to identify and expose Chinese information operations (IO) and "design programs to educate the public about them."[48]

A PRIMER ON THE PLA STRATEGIC SUPPORT FORCE

Crucial to understanding Chinese views of cyber and space operations, and more deeply understanding how the PRC is poised to conduct OIE to support Chinese Foreign Policy is an understanding of the PLASSF. For any military, a key element of excelling in joint, all-domain warfare is maintaining an effective force that can operate seamlessly within the information environment, cyberspace, and space domains. Founded in 2015, the PLASSF represents the PRC's approach to securing "information dominance," as it synchronizes the PLA's cyber warfare, electronic warfare, satellite communications, satellite reconnaissance, and psychological operations (PSYOP) units and capabilities.[49] While the PLASSF represents one of the PRC's most nascent capabilities, its recent creation signals the PRC's increased interest in successfully operating within the information domain to support national rejuvenation and reunification.[50]

The PLASSF's strategic IO role revolves around the coordinated employment of space, cyber, electronic warfare (EW), and psychological warfare to "paralyze the enemy's operational system-of-systems" and sabotage adversarial mission command during the initial stages of conflict.[51] However, as the conflict progresses, cyber, EW, space, and PSYOPs each have a unique and synchronistic role to play.[52] PSYOPs and EW are viewed as crucial signaling assets, while cyber and space are valued predominantly for their communications-denial and disruption capabilities.[53] While PLASSF doctrine is scarce, likely due to the sensitive nature of strategic IO, several texts help illuminate leading Chinese thought on the employment of the PLASSF. For example, the *Science of Military Strategy* highlights that the PLASSF aims to converge assets to achieve "integrated reconnaissance, attack, and defense" as a joint force.[54] RAND has summarized available PLASSF texts to conclude they are seen as a "key component of strategic deterrence," critical to fighting "informatized local wars," countering U.S. military intervention in the region, maintaining domestic stability, and projecting China's emerging interests in more distant parts of the world.[55] Since 2015, the PLASSF has also executed multiple force-on-force drills and contingency training with other services, likely focused on spearheading the concept of a truly "joint force."[56]

As its mission, the PLASSF has been tasked with "securing information dominance by carrying out strategic, operational, and tactical [space, information, and] cyberspace operations, the aim of which is to seize access to information, maintain decision-making advantage during joint operations, and ensure national network security."[57] In wartime specifically, the PLASSF's core mission focuses on seizing and exploiting the "information domain to enable other PLA forces to achieve decision superiority" and coordinating information-related capabilities to capitalize on kinetic strikes," analogous to the U.S. Army's "information advantage."[58]

Moreover, as perhaps the most decisive force contributing to Chinese "information warfare," the PLASSF is subdivided into two Theatre Command (TC) deputy leader-grade departments: the Space Systems Department (SSD), and Network Systems Department (NSD). The Space Systems Department is directly involved with coordinating the PLA's space launch, satellite control,

navigation, space-based intelligence, surveillance, and reconnaissance (ISR), and counter-space operations, while the Network Systems Department is responsible for PLASSF network and electromagnetic spectrum management, and PSYOP.[59] Additionally, the PLASSF mission set is driven by organizational factors: the orders of the civilian Chinese Communist Party (CCP) that increasingly understands information to be a crucial determinant of victory in localized, informationized wars, and a large civilian science and technology industry that provides human capital, resourcing, and organizational capacity for information warfare.[60]

Since 2015, the PLASSF has increasingly integrated into training exercises, drills, and planning with not only the PLA at large but science and technology-focused civilian entities as well. While this has certainly strengthened civilian-military fusion, it has also created "amorphous command mechanisms between civilian and military authorities" which can prove detrimental to command, control, and effective employment.[61] Because the PLASSF is seen as a strategic *force* that parallels U.S. Strategic Command, overall decision-making authority for PLASSF asset employment resides at the highest levels through the Central Cybersecurity and Informatization Commission *and* the Central Military Commission.[62]

Paradoxically, the PLASSF's emerging identity as a leader in the PLA's "joint force" methodology could also impede its overall combat effectiveness through bureaucratic infighting and cumbersome approval processes.[63] With PLA emphasis on centralized decision-making, the PLASSF's ambiguous command authorities pose significant risk to kill chain management and agile executions of coordinated space, cyber, EW, and psychological operations.[64] While the existence and continued emphasis on the PLASSF underscores the PLA's increasing focus and prioritization of the space, cyber, and information domains to execute information warfare, the PRC's reliance and perhaps overconfidence in the data and strategic significance of the PLASSF leaves them vulnerable to deception activities that prompt strategic misallocation of resources, influence operations that exploit rifts to foster PLA infighting, and a blend of kinetic and non-kinetic strikes that destroy, disrupt, or degrade PLASSF capabilities. As much as the PLA want to "decapitate and blind"

their adversary while "crushing their bones and damaging their body,"[65] the PLASSF's organizational, technological, and psychological vulnerabilities leave significant room for the PLA to become blinded, as well as to suffer command and control (C2) decapitation, and experience strategic defeats themselves. Still, understanding the PLASSF is an important aspect of comprehending the totality and scope of Chinese information and influence operations, especially those directed against Taiwan.

More broadly, the PLASSF also enables the execution of the PLA's now ubiquitous "Three Warfares" – a PRC warfighting model that encourages the synchronization of psychological warfare, public opinion warfare, and legal warfare to gain an advantage over an adversary.[66] PRC Psychological Warfare "seeks to undermine an enemy's ability to conduct combat operations" by deterring, shocking, demoralizing, or eliciting specific behaviours from adversary military personnel and supporting target audiences. Public opinion warfare seeks to mold domestic and international public perceptions towards the PRC's military actions and dissuade adversaries from taking actions contrary to Beijing's interests. Legal warfare employs international and domestic law to assert legal superiority and backing behind the PRCs operations, activities, and interests, build international consensus, and restrict non-Chinese freedom of movement in multiple domains.[67]

Overarchingly, the PRC and PLA have employed these three warfare methodologies to pursue and reinforce several key narratives in Taiwan and across the Indo-Pacific:

- Chinese dominance is the historic norm and is inevitable;
- the CCP's objectives are permanent and unchanging;
- the CCP and PLA cannot be deterred and will pay any price to achieve Beijing's objectives; and
- the U.S. is an increasingly weak, unpredictable, and unreliable ally.[68]

In Singapore, the CCP has sought to influence many Singaporean elites to maintain open trade with China and at the very least remain "unopposed" towards China's efforts to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, ironically, an organization that exists to advance a liberal, rules-based economic order in the Indo-Pacific.[69] In Thailand, China has endeavoured to influence the public opinion of many decision-makers in order to gain opportunities to construct high-speed rail, proliferate Huawei's 5G network, and sell comparatively cheaper military equipment, such as submarines, to the Thai military.[70] China's state-media, diplomatic personnel, and business entities operating in the Solomon Islands and across the South Pacific, employed each of the aforementioned narratives to elicit Belt and Road Initiative participation and diplomatic recognition of China over Taiwan, and to encourage the denouncement of western ideals by political officials.[71]

China has also launched an international and domestic influence campaign to label human rights violations and Uyghur genocide as "counterterrorism operations" and continues to bombard Taiwan with disinformation and a blend of psychological and public opinion warfare to encourage peaceful reunification with the mainland. Both attempts have largely failed, but the PRC's deep-seated focus on eliminating internal threats and "Taiwanese separatists" continue to breathe life into these ineffective influence campaigns.[72] Ultimately however, the PRC's large-scale influence operations provide ample testing ground for continuous refinement of narratives, tactics, and approaches in the long game of seeking to influence Taiwan to reunify and actualize "national rejuvenation" through reunification.

PRC CYBER OPERATIONS AGAINST TAIWAN

In terms of operationalizing offensive cyber capabilities, China has "invested heavily" within them in order to be able to repel outside military interventions and routinely launches cyberattacks against Taiwan.[73] In the words of the PRC's 2019 Defense White Paper, "cyberspace is a key area for national security [and] China's armed forces accelerate the building of their cyberspace capabilities."[74] Taiwan remains vulnerable in the cyber domain, and the PRC has "trained its cyber-attack capabilities on Taiwan" to attack military logistics, command

and control systems, and counter-space systems than can exploit reliance on satellites for ISR, communications, and targeting purposes.[75] The U.S. Senate Select Committee on the CCP has also found that Taiwan currently "lacks the defense required to [fully] protect its infrastructure" and "will struggle to defeat an invasion without the continual operation of its ports, airports, and other transportation facilities, as well as its power supplies and other critical infrastructure," underscoring the volume and depth of PRC cyber capabilities aimed at Taiwan.

Moreover, since Taiwan has historically been used as a "test case for improving the effectiveness of Chinese cyberattack capability," there is a high chance that PRC cyber capabilities will "play a role" in any future cross-Strait conflict.[76] The PLASSF is believed to be responsible for the vast majority of election interference activities and the PRC launches roughly 20 to 40 million cyberattacks against Taiwan each day, which range from disinformation operations to espionage and offensive cyber operations targeting critical infrastructure.[77] China has also accomplished "serious" breaches against Taiwan, given that most critical infrastructure is digitized and vulnerable to the sheer volume of unrelenting Chinese cyberattacks. In 2021, China hacked Taiwan's Line messaging and disinformation awareness service to spy on politicians, military personnel, and city leaders, visibly reinforcing PLA cyber power.

PRC SPACE OPERATIONS AGAINST TAIWAN

A "Taiwan contingency" is also the "main strategic direction" driving PLA force modernization, and the PLASSF's capability to "complicate" foreign intervention will likely grow over the next ten to 15 years.[78] Chinese military writings such as *Space Information Support Operations* explain that space assets are crucial for a myriad of operations in Taiwan. Currently, PLASSF space asset missions include support to targeting through battlefield, electronic and oceanic ISR; communications support and denial; precision, navigation, and timing (PNT) services; and space-based jamming against adversary, communications, radar, electro-optical, and PNT systems.[79] In wartime, the PLASSF space forces are tasked with "providing vital support for raising up

an information umbrella" that would integrate with PLA land, sea, air, and rocket forces and become the "key force for victory in war."[80]

In a Taiwan contingency, ISR satellites in particular would be utilized to collect intelligence, develop targeting packages for ships and planes, and help produce battle damage assessment after the opening bombardment of strikes and during joint offensive operations.[81] In the event of a blockade, PLASSF space assets would be expected to disrupt U.S. and coalition communications, assist PLA commanders in understanding what time is best to launch a crossing of the strait for follow on offensive operations, and ultimately "blind and deafen [any] enemy" who seeks to disrupt reunification operations.[82]

China has also displayed its counter-space capabilities as tools of cost imposition and foreign policy. In 2007, China launched a ballistic missile with a kinetic kill vehicle (KKV) that collided with and destroyed a non-operational Chinese weather satellite, showcasing its anti-satellite (ASAT) attack capabilities on the world stage. Somewhat irresponsibly, the Chinese ASAT attack unleashed over three thousand pieces of space debris, causing significant obstacles in low earth orbit (LEO) for years to come.[83] This capability demonstration, while old, is still significant years later. The PRC's counter-space and ASAT capabilities continue to improve and now include kinetic kill missiles, ground-based lasers, orbiting space robots, surveillance satellites, satellite jammers, space-based cyber capabilities, and directed energy weapons.[84] In 2022, the PRC launched a "Shijian-21" satellite, equipped with a robotic arm, that propelled a non-operational BeiDou navigation satellite into a "high graveyard orbit" above Geostationary Orbit (GEO).[85] This counter-space grappling technology could easily be utilized in a future conflict to not only manoeuvre defunct Chinese satellites, but also to attack or pull adversarial satellites out of their orbital track – epitomizing PLASSF doctrine to "blind and deafen" their enemies in wartime.

Another recent example of the PRC flaunting its counter-space capabilities is how China threatened to close airspace north of Taiwan for three days in April 2023 due to a "falling object from a satellite launch vehicle."[86] Taiwan was later able to convince China to "rein in" its no fly zone plan to a thirty minute

window, but this interaction not only generated insights for Beijing regarding Taipei's decision calculus for similar future events, it effectively shut down Taiwanese airspace through counter-space capabilities. The PRC's counter-space capabilities even threaten Taiwanese contingency communication plans in the event of a crisis, especially as Taiwan moves toward adopting a fleet of Starlink-like LEO satellites to mitigate the effects of a Chinese undersea cable attack that would lead to an internet blackout crisis during a Chinese invasion.[87] These examples reflect not only a growing capacity of PRC space and counter-space capabilities, but also how these capabilities can be utilized in support of national rejuvenation, reunification, and promulgating a narrative of a "common destiny" for both the PRC and Taiwan.

CONCLUSION

To further its foreign policy goals of national rejuvenation, national reunification, and the cultivation of a community of common destiny, the PRC synchronizes and employs influence cyber, and space capabilities. Though many of the PRC's election interference and disinformation operations toward Taiwan have largely backfired due to poor execution and a growing Taiwanese identity that opposes national reunification and favours the status quo, China's long-term and individual-focused approach to influence operations in Taiwan is only just beginning. It will likely intensify and be refined with each subsequent election, especially as the PRC and PLASSF enhance influence techniques across the Indo-Pacific. The PRC's endless barrage of cyberattacks that target Taiwanese critical infrastructure, spread disinformation, and promote PRC espionage are another means by which the PRC is attempting to set conditions for winning local, informationitized wars and furthering its foreign policy objectives. Finally, increasingly robust space and counter-space activities not only showcase the PRC's power as a spacefaring nation on the world stage, they have also tangibly affected decision-making in Taiwan and offer a glimpse into how the PRC is seeking to control communications leading up to and during a potential conflict.

Collectively, PRC influence, cyber, and space capabilities, largely housed under the nascent PLASSF, represent means with which China is moving towards

national rejuvenation, national reunification, and the development of a community of common destiny. Because "rejuvenation" is not deemed possible by China without "reunification" and significant resources are invested into influence, cyber, and space operations every day, the PRC can be expected to further grow and modernize the PLASSF while refining associated OIE tactics. The PRC has already leveraged the fusion of influence, cyber, and space capabilities to support national strategy and foreign policy, and will likely continue to do as national rejuvenation, reunification, and the creation of a community of common destiny are pursued in the coming years of this decisive decade and beyond. Indeed, the PRC views the PLASSF as the "key force for victory in war" and decisive in competition. The future of Taiwan and global democracies depends on what we do in the present and near future. Any nation that seeks to preserve democratic ideals would be wise to study and develop strategic, operational, and tactical counters to the increasingly aggressive capabilities of the PLASSF.

CHAPTER

7

CHINESE MARITIME MILITIA

LIEUTENANT-COLONEL BEN GANS AND
MAJOR RUUD VAN DEN BOSCH

On April 8, 2012, a Philippine Long Range Patrol Aircraft (LRPA) was conducting a routine reconnaissance flight over the archipelagic country's Exclusive Economic Zone (EEZ). While approaching Scarborough Shoal, a triangle-shaped chain of reefs and rocks located approximately 220 kilometers northwest of Philippine's Zambales province, the aircraft's crew spotted eight Chinese fishing vessels which were anchored inside the shoal.[1] The Philippine authorities considered the presence of these vessels in their EEZ an act of illegal fishing and sent its largest naval vessel, the BRP *Gregorio del Pilar* (PF-15) to the shoal.[2]

Two days later, the *Gregorio* arrived at the shoal and launched a boarding team to search one of the Chinese vessels. During the inspection, the team found a substantial number of corals, giant clams and live sharks that were all collected illegally. It was not the first time that Chinese fishers violated the International Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), as the Philippine authorities had arrested several of them in the past for violating the Philippine's sovereignty and illegally fishing.[3]

During the boarding, however, the captain of fishing vessel *Qionghai* 02096 (which was anchored inside the shoal) sent several messages to the People's Armed Police (PAP) Border Defense Force Control Station situated in Hainan

province. Two civilian China Marine Surveillance (CMS) vessels, the *Zhonggou Haijian* 75 and *Zhonggou Haijian* 84, that were in the vicinity of the shoal responded to the distress call and set sail for the shoal.[4] Just when the boarding team of the *Gregorio* wanted to arrest the Chinese fishers, the two CMS vessels arrived at the shoal and took position between the Chinese fishing vessels and the *Gregorio*.[5] The captain of one of the CMS vessels then instructed the captain of the *Gregorio* to leave the shoal immediately because he had entered Chinese territorial waters illegally.[6]

The Philippine authorities initially responded to the incident by seeking a diplomatic solution. The administration further emphasized that they had not requested U.S. assistance in the matter at that time. To deescalate the situation, the Philippine navy withdrew the *Gregorio* from the scene on April 12th and replaced it with the *BRP Pampanga*, a search and rescue coast guard vessel. Rather than responding in a similar de-escalatory manner, the Chinese authorities deployed the *Yuzheng-310*, its latest fishery patrol vessel, to complement the two CMS vessels already at the shoal. Additionally, the Chinese Ministry of Foreign Affairs issued a press release in which they stated that "the attempt by the Philippines to carry out so-called law enforcement activities in the waters of Huangyan Island has infringed upon China's sovereignty and runs counter to the consensus reached by both sides on maintaining the peace and stability in the South China Sea and not to complicate and escalate the situation."[7]

The next morning, Philippine foreign secretary Alberto del Rosario met with the Chinese ambassador in Manilla to start negotiations over the on-going dispute. Shortly after the negotiations had begun, two Chinese cutters escorted the Chinese fishing vessels out of the shoal, leaving each country one vessel. When evening came, the negotiations stalled because the Philippine authorities had strongly objected against allowing the Chinese fishing vessels to leave the shoal with their catch untouched. The Chinese, on their part, insisted the Philippine coast guard withdraw its last vessel from the lagoon. According to del Rosario, this Chinese request was unacceptable, and he announced a stalemate. Shortly thereafter, a second Chinese vessel arrived at the shoal.

After five days without any diplomatic breakthroughs, the Philippine authorities changed their strategy by officially announcing that they were seeking international assistance to solve the dispute. In addition to this public call, the Philippine government also formally requested the Association of Southeast Asian Nations (ASEAN) to take a position on the matter. The Chinese responded by claiming that the Philippines' public outreach was a violation of the mutual agreement to resolve the dispute bilaterally. China responded by replacing the *Zhonggou Haijian* 84 with a Fisheries Law Enforcement Command (FLEC) vessel, equipped with several machine guns and light helicopters. Moreover, China informed the Philippines that Chinese warships were deployed to a holding area over the horizon.

On April 23rd the Chinese made a gesture of conciliation by announcing that they had withdrawn two of their vessels from the shoal and intended to seek a diplomatic solution. Although Philippine reporting confirmed the withdrawal of these Chinese vessels, the authorities did not comply but rather deployed a second fishing vessel to the shoal. In addition, the Philippine authorities announced on April 26th that it was seeking direct U.S. involvement. The Chinese reacted immediately by warning it would respond in conjunction with its civilian agencies if the situation would call for it. Two days later, a Chinese cutter harassed a Philippine vessel at the shoal and on May 2nd, four Chinese vessels were back in what became known as the Scarborough Shoal standoff.

By mid-June, Philippine President Benigno Aquino issued the order that all Philippine vessels had to leave the shoal due to an upcoming seasonal typhon. Once its coast guard vessel had departed, China began to consolidate its control over the shoal by constructing a chain barrier across its narrow mouth, thereby denying the Philippines' access to it. At the same time, China's Vice Minister of Foreign Affairs Fu Ying visited Manila and tried to compel the Philippine authorities to keep quiet on the issue and accept Beijing's de facto authority over Scarborough Shoal.

Today, the West considers the standoff to be the most tangible disruptive Chinese action in the South China Sea (SCS) since 2012. What stands out are the Chinese actions during the initial stages of the dispute, including the use of its civilian fishing vessels to occupy the shoal. These vessels and its crews

belong to the People's Armed Forces Maritime Militia (PAFMM). This militia is an example of one of China's ambiguous capabilities to expand its control of the SCS. In doing so, the PAFMM offers China the ability to apply coercion in an extremely unique way and presents an emerging 21st century security threat in an era of rising strategic competition.

This chapter is organized as follows: we first provide a brief overview of the PAFMM. What follows is the description of the three kinds of threats posed by this ambiguous capability: *seen* irregular, *known* regular, and *emerging* future threats. We conclude with a brief discussion of the main findings of this chapter.

THE PAFMM

China is home to the world's largest fishing fleet consisting of between 12,000 and 17,000 vessels and an even larger number of people that work either on the vessels themselves or in the related industries onshore.[8] A substantial number of these vessels and crews are members of the PAFMM. This maritime militia is trained to defend and advance China's national interests, including expanding its maritime territorial claims in the SCS. Furthermore, in times of war, the PAFMM may be deployed in support of the People's Liberation Army Navy (PLAN).[9]

From an organizational perspective, the PAFMM is part of China's militia, which is an element of the People's Liberation Army (PLA). A 2013 Defense White Paper describes the militia as "an assistant and backup force of the PLA."[10] Because the members of the militia retain their day-to-day civilian jobs and only participate in training, exercises, or operations on demand, the militia should be considered a reserve force that operates in parallel or in support of the PLA. To this end, the militia has two distinct tasks: assisting the PLA in the defense of China's homeland and assisting local authorities with maintaining order and stability as well as disaster relief.[11] Similar to the PLA's traditional military components, the militia is characterized by a military organizational structure. Due to their dual-responsibilities, however, civil-military leadership exercises so-called dual-track command-and-control over the militia.[12]

The PAFMM, together with the PLAN and Civilian Coast Guard (CCG), plays a substantial role in China's joint military, law enforcement, and civilian defense efforts at sea.[13] These joint efforts allow the effective coordination of the PAFMM with traditional PLA military components. To further enhance interoperability, the most advanced units of the PAFMM receive tactical military training from the uniformed PLA.[14] Furthermore, the maritime militia participates in joint exercises with the PLAN and CCG.[15]

The PAFMM thus enjoys a blurred status that allows it to operate discreetly, deceive potential opponents, and, importantly, lower the risk of escalation. This ambiguous status is particularly applicable to some of its most advanced units that collect intelligence and conduct reconnaissance far from China's mainland.[16] These advanced units comprise only a small portion of the PAFMM but are the ones that are involved in ambiguous activities such as the Scarborough Shoal standoff.

The PAFMM's most advanced units operate from China's southernmost province, Hainan, and include the Danzhou, Tanmen, Sanya, and Sansha militias. All four militias played a significant role in several key events that took place over the last five decades in the Near Seas. For example, the Danzhou militia emerged out of the militia that took part in a battle with Vietnam over the Paracel Islands in 1974.[17] Furthermore, the Tanmen militia played an active role in the 2012 Scarborough Shoal standoff. Importantly, President Xi Jinping conducted a high-profile visit to the militia a year after the standoff, indicating the militia's strategic significance.[18] The Sanya militia fulfilled a leading role in the disruption of U.S. Navy Ship (USNS) *Impeccable* survey operations in March 2009.[19] They were also cooperating with the Tanmen militia in 2014 while ramming and sinking several Vietnamese vessels during a standoff over an oil rig deployed by China National Offshore Oil Corporation (CNOOC) in disputed waters.[20] Finally, the Sansha militia increasingly functions as part of China's maritime forward presence in the SCS. From its home base in the Paracel's Woody Islands, this militia primarily serves as an advanced force equipped with powerful vessels capable of spraying and ramming. Moreover, the vessels are equipped with weapons and ammunition, thereby turning this militia into a more paramilitary force.[21]

In sum, the PAFMM illustrates an example of tactical units capable of achieving strategic effects, thereby expanding China's control of the Near Seas. The militia's ambiguous character allows China to effectively manipulate the traditional distinction between military and non-military forces. In doing so, the PAFMM is an effective instrument to be employed in strategic competition. Therefore, it is critical to better understand the threats posed by this emerging hostile capability, an overview of which is presented in the next sections.

THREATS

The PAFMM is designed to operate between the blurred lines of peace and war, and civil and military activities. The high level of ambiguity, such as type of unit, combatant status, civil or state activity, makes the PAFMM problematic to counter and contributes to the militia's success. This section examines the PAFMM through a different lens – not by type of force, but by type of threat. A closer examination of the PAFMM shows that the militia poses both an irregular and conventional threat, with the potential of integrating advanced technology. Seeing the PAFMM from this distinct perspective may contribute to a better understanding of this ambiguous maritime capability.

SEEN IRREGULAR THREAT

The first way to label the PAFMM is as a contemporary irregular threat. The Irregular Warfare Annex to the U.S. National Defense Strategy 2020 states that "IW [Irregular Warfare] favors indirect and asymmetric approaches."[22] This feature is clearly recognizable with the PAFMM. In the last decade, PAFMM activities occurred below the response threshold of armed violence and escalation. The most known tactic, which avoids military response or escalation, is the Chinese *cabbage strategy* of "surrounding a contested area with so many boats – fishermen, fishing administration ships, marine surveillance ships, navy warships."[23] This strategy is used to threaten other sailors at sea and thereby acts as a form of coercion. The targeted vessel is not only threatened by the PAFMM but also intimidated by the surrounding CCG and PLAN vessels. Despite the increased weaponization and training of the PAFMM, all reported incidents thus far were without the use of armed violence. This illustrates

the PAFMM's ability to stay below the threshold of armed response using an indirect and asymmetric approach.

Irregular PAFMM actions were seen in two distinctive forms: coercive manoeuvres and territorial seizure. Both bear the signature of ambiguity, and both remained below the threshold of escalation. In most events, China's maritime militia applied coercive manoeuvres to threaten foreign ships with harassment, collision, obstruction, or other intimidating manoeuvres.[24] China hereby structurally coerces foreign vessels out of disputed waters, creating *de facto* control of these areas.

The PAFMM's targets range from local fishing vessels to even U.S. Navy ships. A notorious PAFMM action was the harassment of the USNS *Impeccable*, conducting undersea reconnaissance in China's EEZ in the South China Sea in 2009.[25] Starting from 5 March, PLAN vessels challenged the *Impeccable* with crossing maneouvres and demands to leave the area. The *Impeccable* ignored the calls. Three days later on 8 March, in line with the cabbage strategy, the Chinese Navy, law enforcement, and fishing vessels surrounded the USNS *Impeccable*.[26] PAFMM vessels started a series of harassments. Chinese trawlers attempted to damage the *Impeccable's* sonar array, advanced within twenty-five feet, and forced the *Impeccable* to an emergency stop by dropping wooden blocks in its path. The *Impeccable* left the area on the same day. After days of Chinese and American diplomatic exchanges and statements, the situation was defused, and the U.S. *Arleigh Burke*-destroyer escorted the *Impeccable* back into the area.[27] The USNS *Impeccable* incident clearly shows how Beijing uses the PAFMM to harass and coerce foreign vessels. Considering the success of these tactics against a U.S. Navy reconnaissance vessel, it is not hard to imagine the effect on smaller foreign commercial vessels.

Besides the coercive manoeuvres, the PAFMM conducted several forms of territorial seizures. The Scarborough Shoal standoff in 2012 illustrates how this modern form of maritime territorial seizure unfolds. That instance led to a permanent Chinese presence on the shoal, and, thereby, a *de facto* annexation.[28] A more recent example is the Whitsun Reef occupation in 2021 – a sizeable shallow coral region within the Philippines' EEZ. From 7 March, around 220

Chinese fishing vessels *anchored* at the reef for several weeks. Manilla interpreted the presence as "threatening" to and "infringing" on Philippine territory. Beijing justified the fishing vessels as "simply escaping rough seas."[29] During the diplomatic disputes that followed, the U.S. National Security Advisor Jake Sullivan "underscored that the United States stands with our Philippine allies in upholding the rules-based international maritime order and reaffirmed the applicability of the U.S.-Philippines Mutual Defense Treaty in the South China Sea."[30] The statement shows the destabilizing risk of these PAFMM actions. The Chinese presence fluctuated after the initial move; however, concerns still exist about ensuing Chinese intentions of another "territorial grab."[31] Although the Whitsun Reef incident is not a classic seizure, it could be labeled as a more refined preliminary move toward land reclamation. Either way, it comes with the same effects and risks.

The PAFMM's irregular threat is a challenging problem for the international community. As mentioned, the PAFMM is difficult to counter due to its ambiguous character. The characteristics of the PAFMM thus form a complex issue to offset. However, the problem lays in the potential effect of the threat. China uses the PAFMM to slowly change the status quo via a salami-slicing strategy, forcing the international community to accept a *fait accompli*.

The first concern is that China's irregular strategy destabilizes the current international order.[32] China historically opposes hegemonic dominance and currently rejects the United Nations Convention on the Law of the Sea (UNCLOS, 1982).[33] PAFMM actions violate UNCLOS agreements by disregarding the globally accepted laws of the sea. Chinese reinterpretation of UNCLOS could lead to a maritime domino effect. A U.S. congressional report expressed that this concern "could serve as a precedent for challenging it in other parts of the world."[34] With the PAFMM, China manoeuvres at the forefront of a more prominent security theme between Beijing and the international community. The potential danger is that the maritime disputes will be the initial test or flashpoint within the changing world order. Within this highly volatile context, PAFMM irregular tactics play a vital role.

The changed physical landscape is a second destabilizing factor that results from China's increased assertiveness. The reclaimed landmasses strengthen

Beijing's position in the disputed areas.[35] Although viewed as illegal by the international community, China's perception of rightful ownership, including the associated maritime rights in the EEZ, could lead to new tensions.[36] Disputes over the economic values in the SCS are – historically – likely to occur. These risks could increase when perceived U.S. support emboldens Asian partners to provoke Chinese claims or when combined with a Chinese urge to show its resolve in defending its rights.[37]

The third concern contains the risk of escalation *above* the threshold of response. The PAFMM strategy, although intended to be below the threshold, does not come without risks. Renowned strategist David Kilcullen states that operations below the threshold may lead a state to "completely misunderstand" the other's actions and results in "lethal miscalculation."[38] The PAFMM's actions may unintentionally escalate. So, although China uses the PAFMM to achieve limited objectives below the response threshold, it could be considered potentially dangerous due to escalation risks.

KNOWN REGULAR THREATS

Although the PAFMM is most notorious for its irregular tactics below thresholds, the PAFMM must also be recognized for its regular or conventional capabilities. On a more conceptual level, it is incorrect to assume that an irregular force, like the PAFMM, only poses an irregular threat.[39] Just as regular forces can conduct irregular operations, irregular forces can conduct regular operations. This reality is also the case for the PAFMM. Although China rarely deployed the conventional capability until now, analysts have pointed out the regular threats the PAFMM poses. So, where the irregular threats have been *seen*, conventional threats are, to this point, predominately *known*, but equally important.

The current PAFMM activities do not represent the full spectrum of its capabilities. Erickson and Kennedy of the *Center for Naval Analyses Cooperation* examined the potential militia employment within the PLA. The authors identified a broad scale of peace and wartime tasks, such as "presence missions, obstruction, reef/island development, (…) mine warfare, ambush,

false landings, etc."[40] Their research concluded that the PAFMM will be a "key element of Beijing's overall vision of becoming a maritime power."[41] In a high-intensity conflict, the current PAFMM capabilities would support regular PLAN operations.[42] The PAFMM is, therefore, fully integrated into the PLAN organizational and command structure. Conventional taskings range from maintaining maritime security, e.g., control of waterways and vessel inspections, to directly supporting combat operations with resupplies, medical evacuations, and repairs. Furthermore, the PAFMM can establish a support network of depots, harbors, and maritime facilities.[43]

Conventional PAFMM capabilities are better known through operational analysis than operational events. A historical example from 1974 illustrates this type of threat. In 1974, after two days of fighting, Chinese forces seized the western part of the Paracel Island from South Vietnam. The PAFMM played a significant role in this classical seizure. The presence of two Chinese fishing trawlers caused discussion amongst South Vietnamese navy commanders about the combatant status. This confusion provided Beijing extra time to prepare for the assault, allowing two Chinese fishing vessels to transport five hundred Chinese troops to the islands, thereby delivering a decisive force.[44] In the following years, China constructed military barracks and an airstrip at Woody Island.

A second example occurred in 1995 when the PLAN seized Mischief Reef in the Spratly Islands, another island group in the SCS. China captured the reef after a short military confrontation with the Philippines and set up a permanent structure. During this operation, the Tanmen Maritime Militia provided essential logistical support to the PLAN by transporting construction materials to the sites.[45] This last example shows the supporting function of military operations, which are easily disregarded because of other, more thrilling operations. However, this example also highlights the PAFMM's contribution to China's Military-Civil Fusion (MCF), one of China's key "military and security developments."[46] The PAFMM's capability to enable China's conventional forces can therefore not be overlooked.

Countering the PAFMM as an irregular force in a conventional conflict comes with complex legal and practical problems. According to the international law of armed conflict, PAFMM vessels are not warships but auxiliary forces, which, in case of armed conflict, may be directly targeted, regardless of their activity at that moment.[47] In other words, the conventional supporting role of the PAFMM makes them a direct legal target in war. However, the problem is more practical than legal. Except for the modern challenge of distinguishing war and peace, the other, more practical problem is distinguishing the fishing vessels from PAFMM vessels in support of the PLAN.[48] The thousands of fishing vessels Beijing can deploy in the SCS, in combination with identical outer appearance, have the potential to cripple the strict Western targeting processes. The result is what Mao Zedong foresaw in the 1940s – the military hidden amongst the people – only this time at sea.

Moreover, Western navies are not operationally prepared to fight the sheer quantity and mass of the PAFMM. Throughout modern Western history, maritime irregular warfare has not occurred on the scale the PAFMM potentially can deploy. Modern navies are highly technological assets, designed to fight similar technological adversaries. Current maritime doctrine, capabilities, or training are not optimally suited to counter the sheer amount of low-tech PAFMM vessels. Most Western navies have operational experience countering piracy or narcotics, but the conventional PAFMM threat is of a different order. No significant recent operational experience can be utilized to counter thousands of ambiguous vessels trained, equipped, and organized by a rising superpower. In short, the PAFMM could potentially challenge conventional Western navies with a large-scale deployment. This threat could thus form a significant liability.

Taken together, the irregular and regular threat is a good example of what recent NATO doctrine defines as Comprehensive Defence: "an official Government strategy, which encompasses a whole-of-society approach."[49] NATO emphasizes the 98 per cent "untapped capability" of the private and civic sector's contribution to the public sector. Clearly, Beijing already established its own comprehensive defence with integrated regular and irregular components, before and in conflict. U.S. Navy (retired) Rear Admiral Michael McDevitt

described China's naval power as the sum of "comprehensive maritime power – navy, coast guard, militia, merchant marine, port infrastructure, shipbuilding, fishing."[50] In these perspectives, the PAFMM resembles a modern approach to force design utilizing all of society's maritime components.

EMERGING FUTURE THREATS

The development of advanced technology could potentially increase the PAFMM threat beyond the capabilities we have seen up to now. The described mix of state and non-state actors, with conventional and irregular tactics, is not new, and is widely known as hybrid threats.[51] However, a new element within these threats is emerging technology. Former U.S. Marine Corps officer and current national security analyst Frank Hoffman emphasized that, in the current era, "the fusion of advanced military capabilities with irregular forces and tactics is key."[52] Hoffman also warns not to ignore threats outside our preferred operations or strategies. Considering his advice, it is important to understand how the PAFMM threat could develop in the next era of disruptive technology.

A key question is *if* and *how* China can integrate the currently low-tech PAFMM in future high-tech warfare. Professor John Arquilla vividly describes the next face of battle as *Bitskrieg* with features such as networked systems, artificial intelligence, robots, and cyberwarfare.[53] Extremely accurate weapon systems combined with superior information and AI-supported coordination would force armies to disperse into smaller units operating in swarms "capable of coordination and of highly innovative tactics."[54] The risks of this new lethal type of warfare could be mitigated by "shifting from few-large to many-small" units to lower the costs when hit and to provide redundancy instead of relying on expensive large assets.[55] With little imagination, the PAFMM fits in this overall profile of many-small dispersed and low-cost units – as the following examples will illustrate.

The first worrisome development is the integration of the PAFMM with intelligence, surveillance, and reconnaissance (ISR) capabilities. China's homeland defence and regional dominance rely heavily on the so-called Anti-Access-Area-Denial (A2/AD) capability, an integrated system of sensors and

strike weapons.[56] Furthermore, Chinese doctrine emphasizes information flow between networks, sensors, and command and control nodes – the so-called "Shih."[57] Both A2/AD and Shih doctrine rely on accurate information. Professor Mark Stokes explains how PAFMM units can contribute to these "reconnaissance-strike operations."[58] In wartime, the PAFMM could act as unconventional ISR assets providing "technical reconnaissance, observation, communication, and electronic reconnaissance to theater component command."[59] In peacetime, the PAFMM already garrisons outposts along the Chinese coast with a "network of radar and electro-optical sensors."[60] Furthermore, China continues to reorganize its command and control structures, and PAFMM units have reportedly been trained and equipped to support the overall PLA ISR systems as early as 2014.[61] Thus far, the integration of PAFMM units as an ISR asset in the advanced Chinese kill-chain provides an indication of future capabilities.

Another disquieting development is the placement of containerized missile systems on merchant vessels. Placing a standard 40-foot missile container on board a merchant vessel creates so-called "Missile Merchants."[62] China has several YJ-18 containerized missile system variants, deployable from land, navy frigates, and submarines. The YJ-18C type is designed to deploy in commercial shipping containers.[63] These systems would be directed by navy vessels or aircraft operating in the area. Each container could carry 30 to 50 cruise missiles. The low-cost weapons systems, dispersed over many merchant vessels, will significantly increase China's maritime strike capacity.[64] And, as with the low-cost ISR assets, the large numbers provide redundancy when targeted – aligning with Arquilla's vision of the next face of war. Another reoccurring problem is how to distinguish these containers and, accordingly, how to distinguish potentially legal targets.

The two examples of networked sensors and containerized missiles illustrate how the PAFMM could potentially evolve with the emerging technology in naval warfare. While currently a fishing fleet, the PAFMM could expand with other merchant-type ships using the same characteristics of *many-small*, *low-cost*, *undistinguishable*, and *dispersed* vessels. China has already shown military ingenuity with other dual-use vessels, such as amphibious lift capacity,

allegedly intended for a cross-street Taiwanese invasion.[65] On the other hand, it remains doubtful whether the PAFMM possesses the organizational and technological capability to incorporate these modern technologies effectively. However, based on the characteristics of both future naval warfare and the PAFMM, Hoffman's advice to monitor these threats outside our strategic culture is still prudent.

CONCLUSION

With the PAFMM, China possesses an ambiguous capability that is difficult to counter. The PAFMM enabled China to hold a competitive advantage over the U.S. and its allies and partners in the Indo-Pacific. As *seen*, this advantage applies to situations that fall below the threshold of armed conflict. China has used the PAFMM to seize and reclaim territory in the SCS, as demonstrated at Scarborough Shoal and Spratly Islands. In both cases, China was capable of successfully implementing a *fait accompli* strategy, while denying the U.S. and its allies and partners the time to respond. These cases thus illustrate the challenges associated with deterring these ambiguous Chinese actions, as described by Professor Richard Betts: "ambivalent deterrence (…) amounts to a yellow light, a warning to slow down, short of a firm requirement to stop. Yellow lights, however, tempt some drivers to speed up."[66] Although concerns are growing about China's State-owned Enterprises and illegal, unreported, and unregulated fishing far outside China's region,[67] it remains to be seen if Beijing can extrapolate its coercive maritime campaign beyond its regional Near Seas into international Far Seas.

As *known*, China continues to develop the PAFMM's conventional capabilities. The U.S. Department of Defense (DoD) 2021 Annual Report to Congress highlighted the importance of China's MCF and explicitly mentioned the PAFMM.[68] The report warns that "the PRC's paramilitary forces continue to grow in scale and sophistication, including the coordination between the PLAN, the CCG, and the People's Armed Forces Maritime Militia (PAFMM)."[69] Other scholars question the benefits of further militarization of the PAFMM. They point out the challenges in coordination and the militia's limitation to prepare and acquire the necessary military skills to conduct or support

high-end missions in wartime.[70] Regarding these limitations, it would be useful to monitor *if* and *when* the further militarization of the PAFMM reaches a tipping point, when the PAFMM will lose the benefits of its militia character and experience some of the same constraints as regular forces.

As for the *emerging* future threats, this chapter has shown how the PAFMM's characteristics could potentially fuse with emerging naval warfare technology. Networked sensors and containerized missiles are just two examples that illustrate the utility of the PAFMM in this emerging field. Similar illustrations could be given in which the PAFMM integrates other technologies, such as unmanned systems or sea-based casings. The main point is that the PAFMM could continue to develop along similar lines in the future: avoiding (Western) conventional military power and exploiting its weaknesses. To this point, we must realize that China's MCF, in the maritime domain, is not limited to fishing vessels. It is a broad concept that can integrate several aspects of society and the private sector to strengthen China's instruments of national power.[71] Monitoring future developments should, therefore, also include other sectors in the maritime industry, such as transport, container shipping, offshore, research, or deep-sea mining.

In retrospect, the development of PAFMM's threat was evident. In 1999, two People's Liberation Army Colonels gave a unique insight into the Chinese way of thinking in their book *Unrestricted Warfare*.[72] The authors analyzed future warfare after the U.S. military victory in the Gulf War. Their key finding was that war would no longer be fought by an "armed force to compel the enemy" but by "all means, (…) military and non-military."[73] Future war would include all aspects of society, such as trade, financial, ecological, psychological, smuggling, media, drug, network, fabrications, resources, cultural, and international law warfare.[74] Unrestricted warfare proliferated in the first two decades of the 20th century in the Indo-Pacific, with the irregular threat as China's primary tool in the maritime domain. But it would be a grave mistake to overlook the other two threats. Both the conventional and the emerging technological threats have the potential to develop in a similar challenging way, thereby enabling China to confront its competitors with ambiguous maritime capabilities.

CHAPTER

8

OUTSIDE HIRES: THE WAGNER GROUP IN AFRICA

DR. MICHAEL J. SOULES

Between approximately the mid-1880s, to about the beginning of the First World War, multiple European powers, including Britain, France, Belgium, Germany, Italy, and Portugal, engaged in the "Scramble for Africa." Specifically, these countries divided up and colonized almost all of Africa so that they could profit by exploiting the continent's vast resources. The European-imposed borders were drawn with little knowledge of local cultures or the land itself. These arbitrarily drawn borders led to a variety of economic and social problems (e.g., ethnic discrimination and disputes) and the continent's natural resources were pillaged. European colonization had devastating consequences for Africa, as its subsequent development was significantly hindered, leading to economic underdevelopment, social turmoil, and political violence. This colonization, in part, was driven by competition among these European powers, and competition over Africa was an important factor in the outbreak of the First World War.[1]

In recent years, analysts have called for increased attention to a new "Scramble for Africa," in which Russia, China, and the United States and its Western allies are competing for influence. In the past decade, Russia has substantially increased its economic, military, and political investments in Africa to compete with its rivals.[2]

For the past several years, one of Russia's main tools for gaining influence in Africa has been the controversial and secretive private military company (PMC), the Wagner Group.[3] While perhaps best known for providing substantial military support for Russia's invasion of Ukraine, the Wagner Group, also known as PMC Wagner, has engaged in various military, political, and economic activities throughout Africa, including in Libya, Sudan, Mali, the Central African Republic, and Mozambique.

However, as of the writing of this chapter in early July of 2023, the future of Wagner in Africa hangs in the balance. Wagner's failed and short-lived mutiny in late June of 2023 has called into question what role it will continue to play around the world, including in Africa.[4] Indeed, as we will cover later in the chapter, there remains great speculation as to the future of the relationship between the Kremlin and Wagner, as well as how active, if at all, the PMC will remain in Africa.

Regardless of the specific trajectory Wagner takes, Russia's growing involvement in Africa, and its increasing reliance on PMCs, will likely threaten both African and U.S. interests in the future. Unfortunately, as it has previously, Africa is at significant risk of facing substantial political instability and human suffering because of this great power competition.[5] Due to its practices, Wagner has contributed to human suffering and political instability on the continent. As will be discussed, the consequences are likely to continue manifesting whether Wagner remains active on the continent or if Russia chooses to wield different tools of influence on the continent.

Indeed, PMC Wagner has been a significant threat and tool of Russian influence that the international community should take seriously. The international community has both normative and pragmatic reasons to respond to the threats posed by Wagner or threats that Russia will continue to pose to Africa in the future. To this point, the interests of the United States and its allies are threatened by Russia's involvement in Africa, including through Wagner's activities.

More specifically, American interests in Africa have been undermined for at least four reasons. First, Wagner has not only failed to curb terrorism in the

region, despite its promises to various African regimes to do so, but it has also contributed to the spread of political violence through causing increased instability and abuses of civilian populations. Russian and potential PMC involvement in Africa will likely continue to exacerbate the threat of terrorism. Second, there is a geopolitical threat posed by the potential of Russia gaining increased access to natural resources and the potential for seaports, an effort to which PMC Wagner has contributed.

Third, Wagner has become a vehicle for the Kremlin to gain substantial political and diplomatic influence throughout the continent. If unaddressed, these threats could worsen, inviting further instability and suffering to many African countries, as well as causing problems for the international community. Even if Wagner and the Kremlin completely sever all connections, the Russian government will likely continue its strategy of attempting to gain substantial political and economic influence in Africa. Fourth, as the fallout between Wagner and the Kremlin highlights, Russia's move towards greater reliance on PMCs in Africa, and the difficulties it could have in controlling these organizations, could lead to further instability on the continent.

In this chapter, I investigate the threats posed by Russia, and its reliance on PMCs, such as the Wagner Group, as well as the options that the international community has to respond to these threats. I examine the influence Wagner has had on Africa over the past several years to highlight the current threat and its potential trajectories.

I begin by outlining what the United States's interests are in Africa. I then discuss the origins of Wagner, the extent of its involvement in Africa, and Russia's more general increasing reliance on PMCs. Following this, I detail the main threats that Wagner has posed to the United States, including through its exacerbation of political violence, its contributions to Russian geopolitical power, and its promotion of Russian political influence throughout Africa. I also discuss the ways in which Russia could continue to threaten U.S. interests in Africa, even in the absence of an alliance with Wagner. I then pivot to exploring why Wagner has persisted for so long, despite the threats it poses. I also highlight the vulnerabilities that Wagner has created for Russian foreign

policy in Africa, as well as similar issues that might result from the use of other PMCs. I conclude by examining potential policy solutions to confront PMC Wagner.

U.S. INTERESTS IN AFRICA

The United States African Command (AFRICOM) has worked with dozens of African countries to help promote American interests in the region since 2008. In a 2023 statement to the Senate Armed Services Committee, General Michael Langley, the Commander of AFRICOM, laid out the mission of the command.[6] In particular, General Langley highlighted the threats of international terrorism and strategic competition with Russia in Africa. PMC Wagner featured prominently in the discussion of these threats.

General Langley made the case that terrorism is currently the greatest threat to both the United States and its African partners, as the Sahel has become a hotspot for international terrorism, with ISIS and al-Qaeda branches and affiliates operating throughout the region. The threat of terrorism in West Africa was also discussed by General Langley, including warnings of the Wagner Group's efforts to exploit the crisis, and how the mercenaries have increased human suffering and worsened the threat of terrorism in the region. As a further testament to the magnitude of this issue, the U.S. Special Operations Command Africa (SOCAFRICA), which is under operational control of AFRICOM, has a primary focus on countering violent extremist organizations on the continent.[7]

General Langley's statement to the Armed Services Committee also included significant discussion of how the Russian government has leveraged Wagner to help foster the dependence of weak and corrupt African regimes on the Kremlin. General Langley highlighted how Wagner's lack of normative and legal commitments means that it is a useful partner for corrupt regimes who are struggling to stay in power. Exacerbating this problem, as General Langley emphasizes, is that China is also substantially increasing its economic and military investment in Africa as part of strategic competition.

Furthermore, General Langley made the case that Wagner is threatening the long-term stability and prosperity of Africa through exploiting its resources and upholding its corrupt and repressive regimes. Even if the influence of Wagner wanes, Russia still has a vested interested in upholding corrupt regimes in Africa and exploiting the resources of these countries. The General also asked the committee for increased support for diplomacy, development, and defence, to counter a variety of threats on the continent, including Wagner.

Relatedly, the prosperity and stability of Africa will become increasingly threatened as it becomes a place of great power competition for the United States, China, and Russia.[8] As General Langley's statement highlights, U.S. security personnel have become extremely concerned with how the Russian government and Wagner threaten the interests of the United States and its African allies.

FORMATION OF PMC WAGNER

While its origins are somewhat ambiguous, PMC Wagner emerged as a network of private security companies during Russia's annexation of Crimea in 2014 and was involved in the conflict. Over the next several years, Wagner expanded its operations to other parts of Eastern Europe, Africa, and the Middle East. The Wagner Group has also played an active role in Russia's more recent invasion of Ukraine, which began in 2022.[9]

Two figures feature prominently in the history and formation of Wagner. The first, Dmitry Utkin, a retired lieutenant colonel in the Russian special forces, was Wagner's first commander and allegedly co-founded the organization. The name of the group, allegedly, is based on Utkin's callsign that is a reference to the composer, Richard Wagner. Utkin is a Nazi sympathizer and Wagner was one of Adolf Hitler's favorite composers. The other key figure is the Russian oligarch, Yevgeny Prigozhin, who owns and finances the Wagner Group. Prigozhin was a close ally of Vladimir Putin (until Prigozhin led the aforementioned failed mutiny), which facilitated Wagner becoming a prominent tool used by the Russian government. Prigozhin now publicly admits to founding and financing the Wagner Group.[10]

The Wagner Group, until very recently, had an extremely close relationship with the Kremlin. While PMCs are technically prohibited under Russian law, private companies and individuals are allowed to hire security contractors. Wagner, at least on the surface, is the "security" wing of Prigozhin's businesses. This legal designation allows Wagner to be significantly involved in Russian-led conflicts around the world. However, experts on Wagner believe that it did not previously take any major actions without the approval of the Kremlin. Indeed, the Wagner Group appeared to be a foreign policy tool of the Russian government for several years.[11]

However, the relationship between PMC Wagner and the Kremlin deteriorated over time. The tensions were particularly over the war in Ukraine. Prigozhin was in an ongoing and escalating dispute with Russian military leadership, accusing them of inadequately supplying Wagner forces, including in Bakhmut, where the PMC faced heavy troop loses. The tensions continued to rise in mid-2023, when Russian forces fired on Wagner forces, with the PMC claiming to have detained a Russian army commander in response.[12]

These tensions culminated on June 23rd when Prigozhin released a series of video and audio recordings, criticizing the Russian military leadership and Putin's justifications for the invasion of Ukraine, subsequently threatening to "march for justice" against the Russian military. On June 24th, Wagner forces crossed the border into Russia and soon captured the southern city of Rostov-on-Don. Wagner forces continued to rapidly advance towards Moscow for the next several hours.

The mutiny eventually ended with Alexander Lukashenko, the president of Belarus, helping to broker a peace agreement between Prigozhin and the Kremlin. Wagner forces withdrew from Russia and the criminal investigations into himself and Wagner forces were eventually dropped. More recently, Prigozhin, several other Wagner commanders, and Putin allegedly met in Moscow. A spokesperson for the Kremlin claimed that Wagner commanders were offered "further options for employment and further combat use."[13] However, the future and full extent of the relationship between PMC Wagner and the Kremlin remains largely unknown.

OVERVIEW OF WAGNER IN AFRICA

In line with Russia's goal to expand its influence in Africa, the Wagner Group has (at least until recently) a substantial presence across the continent. Over the past few years, Wagner is alleged to have thousands of operatives engaged in various combinations of military, political, and economic activities across Africa, including in the Central Africa Republic, Libya, Mali, Mozambique, and Sudan, among other countries. Wagner's military activities include counterterrorism operations and serving as personal protection for regime leaders. The group's political activities include pro-Russian and anti-Western disinformation campaigns, as well as biased election monitoring. Its economic activities include supporting companies it has ties to, especially for the mining of natural resources.[14]

Wagner Group has been an attractive option for many, particularly corrupt and weak, African regimes. This attraction is for a few different reasons. First, regimes can hire Wagner relatively cheaply in the short-term. Instead of paying them out of the coffers, many regimes have offered Wagner lucrative mining contracts in exchange for their services. However, these relationships will likely prove to have significant long-term costs to these countries, as corrupt regimes are giving away valuable resources that could benefit the countries in question, in exchange for short-term benefits. Russia and PMC Wagner have been very willing and eager to exploit this dynamic.

Second, while the support of some countries, such as the United States, is contingent on certain standards of democratic governance and respect for human rights, Wagner sets no such standards. Third, regional and international security forces, including French forces, were unsuccessful, in many ways, in curbing the spread of terrorism and insurgency. This failure provided Wagner with an opportunity to work with African regimes facing these problems. Thus, corrupt regimes do not have to reform and can maintain power through hiring Wagner to help them with their security, economic, and political needs.[15]

Wagner has been more successful in some countries than in others. One of Wagner's "successes" has been in the Central African Republic (CAR), where,

in exchange for political and economic influence, it has supported the regime against rebels since 2017. In exchange for gold mining concessions and other benefits, Wagner forces have become deeply entrenched in CAR, where they have successfully kept the ruling regime in power. However, Wagner has engaged extensively in human rights abuses in CAR and political violence persists in the country.[16]

Allegedly, the United States and some European countries have made offers to support CAR's government and to try to replace Wagner forces. However, because these offers would probably come with stipulations about protecting human rights, the government of CAR likely finds these offers less appealing than its current relationship with Wagner.[17] International efforts to promote peace and stability in CAR will likely be difficult.

However, Wagner has been less successful in other places. In Mozambique, for instance, Wagner struggled to successfully carry out its operations. Wagner operatives were very unfamiliar with the area in which they were operating; they had little to no experience engaging in bush warfare; they had tensions with the Mozambique Defence Armed Forces; they struggled to connect with the local population; and they were unfamiliar with the local culture.[18] These problems eventually culminated in the Wagner Group withdrawing from Mozambique.[19] While Wagner has successfully served Russian foreign policy interests in some countries, it has also struggled in others, revealing potential vulnerabilities of the organization.

FUTURE OF WAGNER IN AFRICA

As mentioned earlier, there is significant uncertainty surrounding the future of Wagner in Africa. Nosmot Gbadamosi discusses why a total withdrawal of Wagner forces from Africa might be unlikely. To start, the PMC has established an elaborate network of businesses in multiple countries on the continent. Furthermore, Wagner has allowed Russia to gain significant influence with multiple African regimes, something Putin will likely be hesitant to risk. Relatedly, the government of multiple countries, including Mali, have become increasingly dependent on Wagner support, and are unlikely to want to part with the PMC.[20]

Analysts have also noted that the Kremlin has tried to maintain a message of continuity with Wagner's partners in Africa, even as some of the PMC's operations have been on hold. The Kremlin has claimed that Russian involvement in CAR and Mali will not change. A few days after the aborted mutiny, a Russian envoy flew to Libya to assure Khalifa Haftar, the rebel leader supported by Wagner and the Kremlin, that Wagner forces would remain in the country.[21]

However, other analysts are more skeptical about the continuation of Wagner activities in Africa. For instance, evidence that Wagner troops have recently been leaving CAR has fueled speculation that the PMC is drawing down activities on the continent. However, the government of CAR claims that the movement is just a troop rotation and that Wagner will remain active in the country.[22]

Overall, at the time of writing this, it is difficult to predict Wagner's future in Africa. However, for the rest of the chapter, I will discuss the influence that the PMC has had on the continent and the implications this has for its African partners and the United States moving forward.

PMCS AND RUSSIAN FOREIGN POLICY

Given Wagner's insubordination and its somewhat mixed record of success in Africa, it is important to consider what Russia gets out of the relationship. While, as noted earlier, PMCs are not technically legally allowed to operate on Russian soil, the Putin administration has come to increasingly favor them as a foreign policy tool. Indeed, Wagner is not the first PMC that the Russian government has used to promote its foreign policy interests.[23]

Commentators have noted a few potential benefits that Russia can derive from using PMCs, including the Wagner Group. Previous analysis cited the plausible deniability associated with employing PMCs for delicate or controversial military operations instead of official armed forces.[24] However, given Prigozhin's aforementioned public acknowledgement of Wagner's links to the Russian government, as well as a more general growing body of evidence of the connection, the Kremlin cannot really credibly deny involvement in

Wagner's operations. Instead, because there is no longer really any credible deniability of a relationship, it is worth considering the other benefits that PMC Wagner provides to the Russian government.

First, there are domestic political benefits associated with using a group like Wagner. Specifically, using PMCs allows the Kremlin to conceal the true extent of Russian losses in Ukraine (and elsewhere), as losses of PMCs are not included in Russian Ministry of Defence (MoD) reports on Russian casualties.[25] Even when the public is aware of heavy Wagner losses, the Kremlin is unlikely to face the same domestic backlash that it would from losing conscripted and volunteer members of the regular Russian forces. As a result, employing PMCs, such as Wagner, can help reduce the domestic political costs associated with risky military operations.

Second, employing PMCs is a (materially) cost effective way for Russia to exert its influence across the world. The Wagner Group has helped the Russian government and other Russian elites gain substantial economic influence in Africa. This access has allowed the Russian government and elites to continue making money in the face of Western sanctions, reducing the effectiveness of Western efforts to punish Russia for its invasion of Ukraine.[26] Relatedly, as discussed earlier, the Wagner Group receives much of its payment through being granted mining contracts and other points of access to valuable resources. Therefore, without expending significant economic resources, the Russian government has been able to gain substantial political and economic influence in Africa through Wagner, an issue which we will return to later in this chapter. Given the benefits that Wagner provides to the Russian government, it is important to now consider how Wagner, and potentially future Russian PMCs, affect American interests in Africa.

TERRORIST AND INSURGENT THREATS

The Sahel has become the primary hotspot for jihadist terrorism in the world.[27] Data from the Global Terrorism Index for 2022 indicate that 48 per cent of all deaths that occurred from terrorism worldwide happened in sub-Saharan Africa. Mali, Niger, and Burkina Faso were among the top ten countries with the most deaths from terrorism in the same year.[28] This violence has

provided an opening for Russia and PMC Wagner, as governments in the region look for ways to combat this threat. A combination of anti-French and anti-Western sentiments stemming from both colonialism and Western military interventions; failed counterterrorism efforts by French and other Western forces in the region; and a desire by leaders of some countries to avoid international pressures for their human rights records; have led these regimes to push out Western forces and invite Wagner instead.[29]

However, Wagner, and any potential successors, threaten counterterrorism efforts in region for at least two reasons: (1) operational ineffectiveness and (2) engagement in actions that spur significant backlash, leading to an expansion of terrorist recruitment and activities.

OPERATIONAL INEFFECTIVENESS

Many of Wagner's counterterrorism measures in the Sahel (and elsewhere) have failed. While French forces in the Sahel had their share of problems with counterterrorism operations, PMC Wagner has proven even more ineffective at identifying and eliminating terrorist targets. This failure is due to Wagner's lack of familiarity with the area and inferior military capacity, relative to that of the French forces. For instance, in Mali, Wagner is completely logistically dependent on Malian military forces, which limits Wagner's effectiveness.[30] Furthermore, many of the African regimes that Wagner works with face both terrorist threats as well as threats from more traditional rebel groups that do not as extensively target civilians. As such, Wagner has to confront a variety of types of militant threats, and it is not necessarily well-equipped to do so. It is not clear that the other Russian PMCs, or the regular armed forces of Russia, could do better at implementing counterterrorism operations in the region.

SPURRING TERRORISM

A second problem is that Wagner has not done anything to address the issues that drive terrorism in the first place, such as poor governance. Furthermore, in many ways, Wagner exacerbates the issues that underpin terrorism in the region, particularly through its human rights abuses and its contribution to the perpetuation of corrupt and unstable governance.[31]

Specifically, the problem is that Wagner has engaged in brutal counterterrorism campaigns, intentionally killing hundreds of civilians and raping and torturing others. These actions have led to an increase in recruitment for jihadist groups in the region, enhancing their operational abilities, including their capacity to strike across international borders.[32] The instability brought on by Wagner has also allowed al-Qaeda and ISIS affiliates in the region to shore up their safe havens.[33]

Additionally, as a result of the instability, rebel groups, such as Jama'at Nusrat al-Islam wal-Muslimin (JNIM), have been able to step in and provide some alternative sources of governance, helping to further increase their popularity.[34] In essence, jihadist groups in the Sahel have been able to expand their recruitment, number of operations, geographic scope of operations, and governance activities, in part, because of the instability wrought by PMC Wagner.

However, as noted above, Wagner has been successful at keeping regimes in power in places like CAR, despite the persistence of terrorism and Wagner's exacerbation of political violence. Said differently, even though Wagner's counterterrorism efforts have been unsuccessful in many countries, certain regimes still favour the group because Wagner has helped them maintain power.

GEOPOLITICAL THREATS

PMC Wagner has presented geopolitical threats for the United States. Specifically, if its activities are continued, they could provide Russia with greater access to both natural resources as well as better seaport access, both of which raise issues for American interests in the region.

NATURAL RESOURCE EXPLOITATION

As discussed earlier in the chapter, various African governments have granted lucrative contracts to PMC Wagner for the mining of valuable natural resources. This arrangement is beneficial for regimes that are cash strapped, as they can offer mining contracts instead of cash payments to Wagner.[35]

Indeed, the Wagner Group now has mining, oil, and gas interests throughout the continent.[36] For instance, the group has access to resources such as gold and tropical timber in CAR.[37] There is also speculation that Wagner is being granted access to natural resources for its services in Mali.[38] Wagner has also become increasingly involved in the civil war in Sudan, which began in 2023. This involvement is likely motivated, at least in part, by the gold, silicon, and uranium that it could access in the country.[39]

As noted earlier, PMC Wagner helped Russia increase its economic influence in Russia.[40] Again, Wagner's vast business operations, particularly those related to natural resources, benefit many Russian actors targeted by sanctions, which lessens the overall impact of Western sanctions.[41] There is also significant concern that these operations will help finance Russia's war in Ukraine. In the short-term, this could undermine efforts by the United States and its allies to impose effective economic punishments on Russia for its actions in Ukraine and elsewhere. In the long-term, this could provide Russia with an advantage in its strategic competition with the United States and China. Wagner's extensive business operations across Africa are one of the primary reasons why the Kremlin might want the PMC to remain active on the continent.

PORT ACCESS

Over the past decade, Russia and China have heavily invested in port access and naval bases as part of their strategies for great power competition with the West. Russia has been providing a serious challenge to European maritime power, as it has important access to the Baltic and Black Seas, as well as some access to the Mediterranean Sea. This access has increased Russia's naval manoeuvrability and ability to project power. The annexation of Crimea played a particularly important role in helping Russia increase its ability to project naval power. Russia is continuing to pursue port and naval base access, including in Libya and Sudan.[42]

PMC Wagner has been heavily involved in the current conflict in Libya. Through Wagner, Russia has attempted to install the rebel leader Khalifa Haftar, though such efforts have thus far been unsuccessful. However, in installing a leader and garnering influence in Libya, Russia's hope is to gain unprecedented

naval access to the eastern Mediterranean.[43] Again, as discussed previously, the Kremlin has attempted to reassure Haftar that Wagner forces will remain active in Libya.

Russia has also made previous attempts to establish a naval base in Sudan. Under former President Omar al-Bashir, the Sudanese government made a deal with Russia to allow it to build a Red Sea naval base. However, the transitional government that came to power after al-Bashir was ousted in a coup, paused this deal and has appeared hesitant to revive it.

While the Wagner Group denies involvement in the current fighting in Sudan, the United States has accused the group of providing surface-to-air missiles to the Rapid Support Forces (RSF), one of the main sides in the conflict.[44] Furthermore, Wagner has previous ties to Sudan. Starting in late 2017, PMC Wagner deployed around 100 personnel to Sudan, where they assisted with military training and protection operations.[45]

However, there is intense speculation about the full extent of Wagner's involvement in the current conflict in Sudan. There is a concern that Wagner might be playing both sides to garner favour with the winner, so that Russia can benefit in multiple ways, including by potentially reviving its efforts to obtain a naval base on the Red Sea.[46] Of course, because of the failed mutiny, it remains unclear the extent to which Wagner will remain active in Sudan, if at all.

However, if Wagner continues to operate and is successful in places like Libya and Sudan, Russia could potentially substantially increase its naval capacity by gaining significant access to the Red and Mediterranean Seas. Such a possibility highlights the threat that Wagner poses to the United States' ability to engage in great power competition.

POLITICAL AND DIPLOMATIC INFLUENCE

The Kremlin has also used Wagner as a tool to increase its political influence throughout Africa. Indeed, some analysts consider Wagner to be Russia's most important tool in gaining political and diplomatic influence on the

continent.[47] As cited earlier, this is another reason why the Kremlin might continue supporting Wagner operations in Africa. This strategy is part of the greater competition between the United States and Russia to exert more political influence in Africa.[48] This approach has taken a number of different forms.

First, Wagner and the Kremlin have engaged in disinformation campaigns aimed at the populations of several African countries. These campaigns are intended to both increase anti-Western and pro-Russian sentiments and have been successful in some areas.[49] Such campaigns also build off the anti-Western sentiments, stemming from colonialism and military interventions, discussed earlier in the chapter.

Second, because some of these regimes depend on Wagner's protection for their survival, they are more likely to align themselves with Russia. The influence of pro-Russia regimes in Africa has already been felt on the international level. For instance, during a UN resolution against Russian aggression in Ukraine, 15 African countries abstained, and Mali and Eritrea voted against the resolution, siding with Russia.[50] Overall, Russia's increase in political influence in some African countries is driving these countries to conduct foreign policies that are favourable to Russia as they reject the liberal world order.[51] If more African countries continue to align with Russia, then the United States might have a more difficult time achieving some of its international political objectives.

INSTABILITY

A fourth potential issue arises over whether PMC Wagner will remain active in Africa. The withdrawal of Wagner from Africa threatens to create a power vacuum, as multiple regimes have become dependent on the group for protection and could collapse when challenged by armed non-state actors.[52] Thus, inhabitants of these countries find themselves in a precarious situation. If Wagner remains and continues operations as normal, these countries might continue to face increased terrorism and the consolidation of power by corrupt regimes. However, if the PMC ends its activities in Africa, then this might create a power vacuum that facilitates terrorism as well.

As Wagner's recent attempted revolt highlights, the Kremlin might have difficulty in the future in controlling Wagner or any other PMC it could work with. Thus, incongruent goals and infighting between Russia and its proxy forces could cause further problems for the countries that these actors operate in.

WHY WAGNER PERSISTS

Given the threat that PMC Wagner poses to the United States, and in many ways, the Putin regime, it is important to consider why the group persists. Indeed, CIA Director William J. Burns publicly stated that the United States was engaging in covert operations to undermine Wagner.[53] However, Wagner has managed to survive, and in many ways, prosper, because of the incentives authoritarian regimes have to employ its services and because of a lack of a coherent policy response from the West.

CORRUPT REGIMES

First, PMC Wagner is an attractive option for corrupt, autocratic regimes. Specifically, because these regimes engage in corrupt and ineffective governance, political instability and violent extremism are rampant. Western countries have offered to provide more assistance; however, this help typically comes with stipulations about democratic and human rights reforms that the recipient regimes must make.

Wagner can provide protection to these regimes to keep them in power, as was seen in CAR. Not only is hiring Wagner protection relatively cheap for regimes (at least in the short-term), but the group, of course, does not require any sort of human rights or good governance standards as a prerequisite. Corrupt leaders can continue to stay in power, without making any reforms that undermine the wealth and power they have accumulated, by contracting Wagner.[54] Again, even as Wagner becomes more alienated from the Kremlin, corrupt regimes will likely be reluctant to part ways with the PMC.

LACK OF COHERENT WESTERN RESPONSE

There has also been a lack of a coherent policy response to Wagner from the West. One issue is that there are significant internal divisions in the U.S. government, including in the Biden administration, over how Wagner should be dealt with.[55] While some piecemeal responses have been implemented, there has been no coherent plan by the United States or its allies to address the threats posed by the Wagner Group.

Some economic sanctions have been imposed on actors affiliated with Wagner. However, these sanctions have largely been unsuccessful at disrupting the group's operations, as they have not been robust and targeted enough.[56] Targeted actors have largely been able to avoid significant setbacks from these sanctions because Wagner has generated so much profit from its economic ventures in Africa.

Additionally, if regimes are sanctioned for working with Wagner, then this risks just pushing them closer to countries like Russia and China, who are willing to look past the abuses of these governments. Furthermore, evidence indicates that sanctions intended to reduce violence by non-state actors are substantially less effective than sanctions with other types of objectives.[57] For a variety of reasons, it has been difficult to effectively combat PMC Wagner with sanctions.

Another related issue is that much like Wagner, Western countries, including the United States, have often failed to address the underlying problems that drive regimes to ally with the Wagner Group in the first place. Relatedly, international counterterrorism efforts have not worked in places like Mali, in part, because they do not adequately address the problems that drive terrorism.[58]

As a result, there has been a dearth of coherent, international policy responses to PMC Wagner. Economic sanctions represent one of the few steps taken by the international community to confront Wagner, but these sanctions have largely been ineffective. More broadly, Western countries have also not taken adequate measures to address many of the political, social, and economic

problems that have allowed Wagner to flourish in many parts of Africa. Even if Wagner fades because of its strained relationship with the Kremlin, the same conditions will persist in these countries that incentivize the use of PMCs by corrupt regimes, and thus, we may continue to see an increased reliance on this type of non-state actor.

WAGNER'S WEAKNESSES

While its recent rift with the Putin regime is the most daunting problem facing Wagner, the Wagner Group also has some other major vulnerabilities that are worth considering. Even if the Kremlin comes to rely on other PMCs, these issues might be replicated.

First, Wagner's military capacity is lacking in many ways. The group is often unfamiliar with the territories it operates in and is often not well-prepared for many of the challenges associated with irregular warfare. For these reasons, many Wagner-led counterterrorism missions have not been successful.[59] Furthermore, as Wagner has increased in size, its standards for recruits have dropped to keep up with its demand for soldiers.[60] Many Wagner soldiers are also uncommitted and do not fight hard. They are accused of pursuing personal gain over the objectives of the group.[61] As noted earlier, Wagner withdrew from Mozambique following its military failures there.

Second, while Wagner and Russia remain popular in many parts of Africa, they have started to face some reputational backlash for their brutal and indiscriminate violence. For instance, in Mali, Wagner has both accidentally and intentionally killed many civilians. Indeed, Wagner and the Malian military have killed hundreds of civilians in joint operations. Wagner also engaged in a variety of human rights abuses against civilians, including summary executions, torture, and looting.[62] As such, Wagner is falling out of favour in some areas, making itself, and the regimes it supports, more vulnerable.

Third, while the Kremlin's use of Wagner is shrewd in many ways, some analysts have made the case that its reliance on Wagner is actually a sign of its weakness. Put differently, Russia is using Wanger, not because Russia has an extremely sophisticated foreign policy, but because it does not have

the capacity to project its power and influence across the globe otherwise.[63] In many ways, Russia might struggle to continue gaining power in Africa in the coming years. The recent Wagner mutiny further highlights the Russian government's weaknesses.

Relatedly, Russia is also not interested in long-term partnerships or state building in Africa.[64] Instead, Wagner, and by extension, Russia, benefit in the short-term from weak and corrupt regimes, as these governments are more dependent on Wagner and more likely to grant it access to significant natural resource wealth. This strategy is unlikely to be viable in the long-term, as it contributes to significant political instability and political violence, which could undermine Russia's strategy of using Africa as a tool for great power competition.

Thus, not only has the relationship between Wagner and the Kremlin been soured, but the PMC faces a variety of other challenges that make it vulnerable. It is not clear whether other PMCs could more effectively confront these problems than Wagner has.

WAYS FORWARD

Given both the dangers posed by the Wagner Group, and its vulnerabilities that can be exploited, it is important to consider how the international community can best confront this threat. What follows are a few commonly proposed policy solutions to deal with the Wagner Group, as well as the weaknesses of these possible actions. If Wagner, or any other Russian PMC, remains active on the continent, it is worth more carefully considering these commonly proposed policy solutions.

SANCTIONS

Current economic sanctions that are in place to undermine Wagner are criticized for not being strong and targeted enough. In response, analysts have recommended several sanctions to counter Wagner's influence. These suggestions include imposing sanctions which name and shame the partner states of Wagner; including third-party countries that are involved with

Wagner and its partner states; and to focus efforts on multilateral sanctions, as they tend to be more effective. Relatedly, analysts have suggested that relying on international organizations more heavily to implement these sanctions would be beneficial.[65]

However, again, there are risks associated with employing sanctions. Sanctions often lead targets to pursue alternative sources of revenue, and indeed, Russia has been able to mitigate the impact of Western sanctions, in part, because of the wealth that the Wagner Group brings in. If countries are targeted by sanctions for their cooperation with Wagner (or any future PMC), then this also incentivizes them to develop stronger economic ties to countries like Russia and China. This outcome could drive these regimes to embrace China and Russia more. Sanctions need to be implemented carefully to effectively undermine Wagner's operations.

COUNTERTERRORISM ASSISTANCE

Both Western (e.g., French) and Wagner forces have largely failed to successfully combat terrorism in various regions of Africa. Some analysts have advocated for the reframing and restructuring of counterterrorism efforts by Western countries in the region. They believe that if countries like the United States or France improve counterterrorism practices in the region, then they will come back into the favour of the regimes that are currently working with the Wagner Group.[66]

However, such efforts will not be straightforward. Western forces have themselves caused many civilian casualties in Africa, which has led to popular backlash against them. Furthermore, militant groups often respond to their loss of troops by ramping up their use of terrorism.[67] Another risk is that when counterterrorism efforts are effective in countries with corrupt regimes, then these regimes are more likely to stay in power, which can perpetuate the problems that contribute to terrorism in the first place. In essence, even when counterterrorism operations are successful at eliminating enemy combatants, there are significant risks associated with these missions.

HEARTS-AND-MINDS

Wagner and the Kremlin have engaged extensively in a misinformation campaign to both increase pro-Russian and anti-Western sentiments. Again, these narratives build off both the history of colonialism and unsuccessful military interventions launched by Western countries in Africa. While gaining the trust of the public will be important in dislodging the influence of Wagner (or any future Russian PMC), significant work must be done to offset past wrongs perpetrated by Western countries.

A MULTI-FACETED SOLUTION

Even though there are obstacles associated with these solutions, there is still merit to them. Indeed, there needs to be a way to punish actors who support Wagner (or future malevolent PMCs); ways to eliminate existing terrorist threats; and ways to gain the trust of the public in these countries so that efforts by the international community are effective. Having a multi-faceted strategy, which employs multiple solutions, will be crucial. Indeed, research that finds sanctions to be ineffective often does not adequately account for other policy measures that can be used in combination to make sanctions more effective.[68]

However, Western economic measures should focus more on addressing the issues that underpin terrorism. Perhaps one of the best ways to enhance the effectiveness of these aforementioned policies is to combine them with humanitarian aid. While military aid is often counterproductive at stopping the spread of terrorism,[69] humanitarian aid has been shown to reduce terrorism in recipient countries.[70]

Humanitarian aid can help reduce some of the problems that drive political instability and violence in the first place. This aid can also help build trust with local populations, especially compared to purely military-based solutions. Furthermore, humanitarian aid can help stabilize countries, making it more difficult for Wagner, or any future PMC, to exploit instability, as Wagner has consistently done. Combating the underlying factors that allowed Wagner to gain influence in the first place will be key to curbing any potential rise of similarly-behaved PMCs in the future.

CONCLUSION

As PMC Wagner continues to pose a significant threat, even with its recent difficulties, there is growing concern that Russia will gain even more power in Africa. However, even if Wagner fades because of its soured relationship with the Kremlin, or because of the heavy losses it has incurred in Ukraine, or both, the past decade has highlighted the damage that can be done with PMCs and the power that Russia can garner through them.

While this chapter focuses primarily on the Wagner Group, the problems highlighted here are likely to persist as Russia increasingly relies on PMCs. These problems will be particularly persistent if the international community does nothing in response and if it continues to inadequately address the factors that contributed to the influence of Wagner in the first place.

More generally, the influence of Wagner is indicative of larger problems of political instability, corruption, economic calamity, and political violence that are pervasive in the countries in which Wagner finds opportunities to exploit. While Wagner has captured the attention of many academics, policy analysts, journalists, and policy-makers, it is a symptom of larger problems. The international community needs to not only confront the growing threat of PMCs, but the underlying causes that have allowed these organizations to become so ubiquitous.

CHAPTER

9

BEACHHEAD WARFARE: ECONOMIC STATECRAFT DESIGNED TO INFLUENCE MILITARY POWER

COMMANDER SENIOR GRADE (NAVY) NIKOLAI FAUKSTAD

In a military context, creating a beachhead has generally been understood to mean establishing control over a span of ground at the water's edge in advance of an amphibious assault.[1] Gaining a beachhead, as in Operation Overlord (1944), can benefit the attacking force by creating a stronghold from which the attacking force can strengthen its advantage to advance further into enemy territory. The term "beachhead" is also used in economics, where a beachhead strategy involves concentrating resources on a small market area to establish a strong position before expanding to a larger market.[2] This chapter argues that the military and business senses of the term "beachhead" share a great deal conceptually when viewed through the lens of economic statecraft: the overall use of economic instruments to achieve foreign policy and/or strategic goals.[3]

To what extent is economic statecraft a threat to military power? This chapter introduces the concept of "beachhead warfare" as an unconventional strategy of economic statecraft in which the aim is to attain "relational dominance." It introduces a conceptual framework for understanding beachhead warfare, and then explores a specific example: the threat of Russian commercial acquisition of sensitive marine manufacturing capabilities in Norway. The renewed great power rivalry combined with increasingly intertwined economic

interdependencies creates greater potential for the use of economic statecraft to influence military power. While economic warfare focuses on the broader economy through the implementation of sanctions and economic pressure, the concept of beachhead warfare carries specific military implications as it aims directly at attaining military advantages. Beachhead warfare represents strategies and cross-sectoral threats that, over time, affect and challenge states' sovereignty, territorial integrity, the system of governance, and freedom of action.[4]

THE THEORY OF BEACHHEAD WARFARE

From an economic and military perspective, beachhead warfare can be be understood as an asymmetrical approach to overcome another more dominant actor. It involves building military forces that enhance the capacity to "fight and win" and aims to achieve a positional advantage by promoting national interests and weakening the adversary's military power before a conventional campaign begins.[5] The objective is to achieve relational dominance by advancing national interests and erode adversary military power in case it is needed in the future – in advance of a conventional campaign. The theory of beachhead warfare is defined and visualized in Figure 9.1.

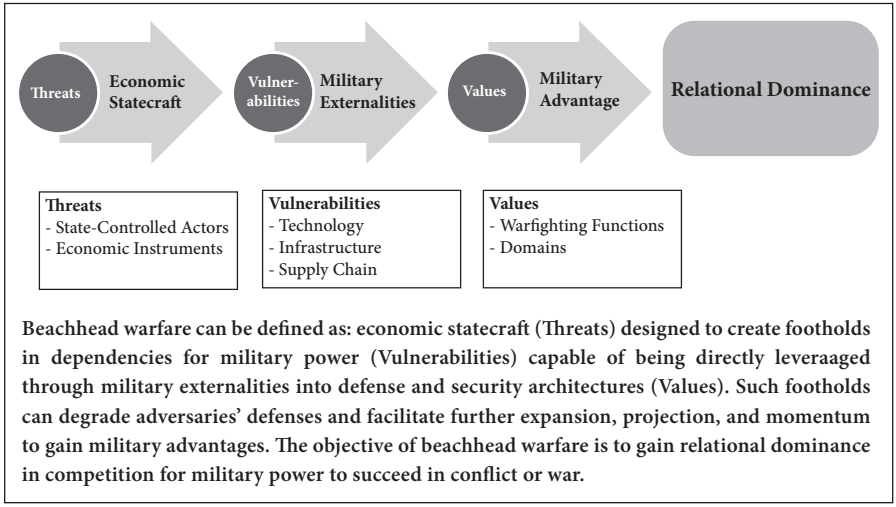


FIGURE 9.1 – The Theory of Beachhead Warfare

In the current era of strategic competition, a nation's capacity to achieve relational dominance can be crucial to accomplishing its strategic objectives such as deterring aggression, winning a military conflict or shaping the global balance of power. Figure 9.2 illustrates a relational dominance graph in beachhead warfare and how preparations in a competition phase can influence a state's ability to succeed in a military confrontation. The "relational dominance line" illustrates the *pivotal moment*: the point at which relational dominance is achieved, and the probability of success strongly outweighs the likelihood of failure.[6]

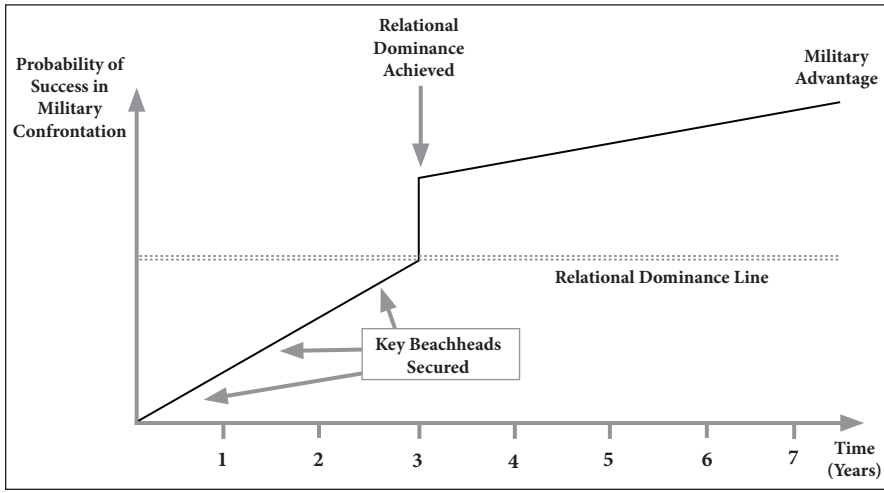


FIGURE 9.2 – Relational Dominance Graph in Beachhead Warfare

The importance of relational dominance in national security strategy is evident in many historical examples. For example, during the Cold War, the United States and the Soviet Union engaged in a global competition for relational dominance, with each seeking to establish influence over other nations through military alliances, economic aid, and propaganda.[7]

State-controlled actors are defined as *threats* in beachhead warfare. A relational advantage can be achieved by influencing military *values*, such as warfighting functions and military domains, indirectly with economic and financial instruments. If a company's values are exposed to unwanted influence, it can have negative consequences for the company's task. All values

have associated vulnerabilities which are conditions that an actor can exploit to affect a company's values. When a commercial activity entails a side effect or consequence for one or more of the parties involved without that effect being reflected in the economic transaction, this is described by the concept of externalities.[8] *Military externalities* refer to external factors that influence military values as a result of economic interactions. One way to influence a rival state's military power is to gain access to that state's technology, infrastructure, and supply chains, which are, for that reason, *vulnerabilities* in beachhead warfare. I examine the Bergen Engines case to illustrate how beachhead warfare works.[9]

THE BERGEN ENGINES CASE: AN ATTEMPT TO ACQUIRE MILITARY TECHNOLOGY?

The following case explores the practical application of beachhead warfare. It documents how Russian direct investment in Norway could have led to unwanted technology transfer to the Russian Navy. In 2021, Norwegian media revealed that companies within the Russian-owned rail and transport conglomerate Transmashholding group (TMH) were in the final phase of acquiring the Norwegian company Bergen Engines, a subsidiary of Rolls-Royce.[10] Bergen Engines has delivered engines to the Norwegian intelligence ship *Marjata*, several coastguard ships, as well as to allies.[11] By normal practice, Rolls-Royce notified Norwegian authorities about potential security challenges in the event of a sale. The Norwegian government eventually ordered Rolls-Royce to stop the sale of Bergen Engines. If Russian authorities were to obtain the technology of Bergen Engines, it could have potentially provided a military advantage to Russia that would have conflicted with the interests of Norway and its allies.[12]

BERGEN ENGINES

Bergen Engines' current engine factory was built in 1971 outside Bergen, Norway's second largest city. It is the only remaining Norwegian manufacturer of marine and large industrial engines. The shipyard Bergen Mekaniske Verksted (BMV), produced its first engine in 1855, quickly became one of the

leading shipyards in Norway, building iron and steel vessels, boilers, and steel engines. In 1942, BMV began building diesel engines and introduced its first gas engine in 1985. Since 1946, Bergen Engines has constructed over 7,000 engines, of which over 5,000 are still in operation. The factory is among the world's leading manufacturers of diesel and gas engines for ships and land-based installations.[13]

In 1999, the company became part of Rolls-Royce and, from 2013, a subsidiary of Rolls-Royce Power Systems AG. In 2018, Rolls-Royce Marine was sold to Kongsberg Gruppen, an international technology group headquartered in Norway.[14] Kongsberg Gruppen supplies high-technology systems to customers in the offshore oil and gas industries, defence, aerospace, and to the merchant marine.[15] Meanwhile, Rolls-Royce kept Bergen Engines in its portfolio.

In 2020, Rolls-Royce notified the Norwegian authorities that the company intended to sell Bergen Engines.[16] A letter addressed to the Ministry of Foreign Affairs indicated that TMH was among the potential buyers. Moreover, the letter specified that the purchase itself would be conducted by TMH International AG (TMHI), which is a Swiss-registered company, but owned by the TMH registered in Russia. In February the following year, Rolls-Royce announced it had entered into a deal with TMH for the proposed sale of Bergen Engines.[17] The proposed deal included the engine factory, the service workshop, the industrial property in Bergen, and a service network spanning seven countries. The sale was expected to be completed in the fourth quarter of 2021.[18]

Bergen Engines was Norway's only manufacturer of marine engines and a cornerstone company with 650 employees and a whole industry of sub-contractors. After Rolls-Royce had announced the previous year that it wanted to sell, local newspapers speculated on potential buyers. When Rolls-Royce announced the signing of an agreement with TMH, a local newspaper published a news article about TMH. According to the newspaper's research, two of the company's owners were among the world's richest individuals and some of Russia's most powerful men.[19] The Norwegian Ministry of Trade and Fisheries responded to further inquiries, noting: "The authorities do not monitor transactions carried out by commercial players. The ministry was

aware of the sale. We consider this to be an agreement on sales between two commercial actors, something the ministry should not interfere with."[20]

Despite this, the newspaper *Bergens Tidende,* continued to investigate TMH. Soon it became evident that such a sale would have significant security challenges for the Norwegian Armed Forces (NAF) and close allied countries, including the United States. The case led to a public debate about the consequences for national security interests of the potential sale.[21] The government received harsh criticism due to the serious revelations, and soon, the opposition's first threats of impeachment came.[22] Based on this, Norwegian authorities initiated work to evaluate all conditions related to the possible sale of Bergen Engines. The government decided to stop the deal based on the Security Act.

The decision came, among other things, because the technology at Bergen Engines would strengthen Russia's military capacity and give Russia access to essential military strategic knowledge and technology. The Parliament severely criticized the government's handling of the case and labeled it highly objectionable and serious. The Parliament´s Foreign Affairs and Defence Committee also underlined concerns over how the case had been revealed and how it would have been handled had it not been for external notices, pressure from the opposition, and investigative media.

EVALUATION OF THE CASE

ECONOMIC STATECRAFT

At the time, the two largest owners in TMH were the Russian oligarchs Iskander Makhmudov and Andrei Bokarev. The two oligarchs are considered to be among the world's richest men.[23] In addition, Bokarev was found on the so-called 'oligarch list' of the United States. The two have also been co-owners of the well-known Russian arms manufacturer Kalashnikov, which was included on the EU and U.S. sanctions lists. One of Bokarev's former partners, Alexei Krivoruchko, was appointed Deputy Minister of Defence for Russia in 2018.[24] Consequently, Iskander Makhmudov and Andrei Bokarev are among Russia's most powerful men, with close ties to the Kremlin.

The Bergen Engines case makes clear that Russian direct investments and acquisitions in Norway can create opportunities to transfer technology or expertise to a foreign-controlled entity that could use this to harm Norway's or another state's national interests.[25] In 2019, the total portfolio of foreign direct investments in Norway was about 210 billion USD, and it came from 66 different countries.[26] Of those, the Russian share of direct investments in Norway in 2019, including figures for ultimate ownership, was approximately 51 million USD, or less than 0.5 per cent of the total portfolio.[27] Despite the small share, it is worrisome given that Russia may previously have used direct investments to strengthen its military capabilities.[28]

Unfortunately, open sources do not specify in which sector or industry Russia's investments were made. Furthermore, those figures may not be entirely accurate. In some cases, Russia has manipulated trade information by investing in companies and by setting up a company in a third country to obscure their direct investment activities.[29] Nevertheless, as this case indicates, there is a potential to use direct investments to harm or acquire infrastructure, target services, value chains, or obtain sensitive technology.

MILITARY EXTERNALITIES

Further research into TMH's links to the Russian Navy uncovered an article in the Russian business newspaper *Kommersant.* The article mentioned the acquisition of Bergen Engines as attractive, considering acquisition of technologies that may be implemented in Russia.[30] The article also referred to an interview with the head of Russia's largest manufacturer of warships, United Shipbuilding Corporation (USC). USC was created by a decree from President Vladimir Putin to bring together the country's shipbuilders and is on the U.S. sanctions list. According to the USC manager, the company negotiated with TMH to establish a collaboration and a development program for diesel engines.[31] Several of Norway's coast guard vessels have engines from Bergen Engines, and at that time, several ships under construction were to get engines from Bergen. Additionally, the Norwegian intelligence ship *MS Marjata* had engines from Bergen as well as contracts with Bergen Engines for maintenance and service.[32] NAF officials stated that they had initiated a dialogue with

Rolls-Royce to clarify whether the sale of the engine factory would lead to the contracts having to be changed. Furthermore, the media revealed that Bergen Engines had signed military contracts with several NATO countries, including New Zealand, Australia, the Netherlands, and the United States.[33]

MILITARY ADVANTAGE

An edition of TMH's internal magazine from 2017 confirmed that TMH took an active part in the revival of the Russian fleet. The article "We conquer seas and ocean" stated that the "development and production of modern diesel engines for the Navy and river fleet is one of the strategic directions for the development of TM."[34] Director Evgeny Vozhakin was quoted as saying that "the enterprise takes an active part in the revival of the Russian fleet – it participates in several projects of the Russian Navy for the construction of surface ships and submarines."[35] According to open sources, TMH has close ties to Russian authorities and the Russian defence sector in general, which suggests that the company takes part in developing military warfighting functions.

It is worth noting that Russian ship construction proceeds at a slow pace, taking up to six years to produce one corvette warship, and the manoeuvre systems are often the bottleneck in this process.[36] According to defence analyst James Bosbotinis, who is associated with the magazine *Warships International Fleet Reviewer*, the sanctions from the West have severely disrupted Russian warship construction.[37] Further, Ukrainian manufacturers had previously supplied diesel engines for the Russian Navy. Deliveries of Ukrainian engines stopped due to the Crimea conflict in 2014, while the subsequent Western sanctions against Russia have restricted the country's access to marine propulsion systems of the desired quality from Western manufacturers. This has led to delays in delivering vessels to the Russian Navy, forcing a halt in the construction of three Admiral Grigorovich frigates intended for the Black Sea Fleet.

The three frigates were finally sold to India without engines.[38] Moreover, the lack of engines and those of acceptable quality almost forced the Russians to abandon plans for new corvettes entirely. At the time of the potential sale, Russian defence analysts had stated that the Russian Navy would benefit from

the acquisition of Bergen Engines and that it would enable faster construction and equipping of vessels.[39] The technology and expertise from Bergen Engines would consequently have been at odds with Norwegian and allied interests. Moreover, it could have been a potential game changer for Russia in developing adequate maritime manoeuvre systems for the Russian Navy.

The sale of Bergen Engines would have also impacted sustainment functions. The service organization of Bergen Engines manages some of the maintenance responsibilities for the engines, including spare parts. Essential customers in recent years include the Norwegian Navy. In addition to the intelligence ship *Marjata,* Norway's largest coast guard ship and the three new vessels in the *Jan Mayen* class also have engines from Bergen Engines.[40] Bergen Engines not only manufactures but installs the engines in the Norwegian Navy's vessels and is responsible for maintenance tasks related to the engines. In the event of a sale, the NAF would still have needed such essential services from Bergen Engines. To continue to carry out its mission and tasks, the Norwegian Navy would have had to secure solutions for maintenance and procurement of spare parts. In the hands of TMH, it would have been possible to disrupt or stop logistics and sustainment functions linked to central capacities in the Norwegian Navy and the Norwegian Intelligence Service (NIS).

Acquiring Bergen Engines could also have posed an increased intelligence threat through the company's deliveries and contracts with the defence sector. The role of Bergen Engines as a supplier and subcontractor to the defence sector means that the company represents a value for military power.[41] Access to goods, information, and technology can be exploited for intelligence purposes. Although Bergen Engines did not have direct access to classified information through its contracts with the Norwegian Navy, the overall knowledge and expertise the company has acquired would have been information with a clear intelligence value for the Russian authorities.[42] Sensitive knowledge and information transferred from TMH to the Russian authorities could have damaged Norway's defence sector and national security writ large.

A sale of Bergen Engines would also have included considerable real estate. The company's property is strategically located close to vital defence installations

in Bergen. Some of these installations have fundamental importance for Norwegian and allied military power, such as the Haakonsvern Naval Base, one of the largest naval bases in Northern Europe.[43] The waters at the naval base are a national secret. The same applies to details on the seabed along the Norwegian coast and is referred to as vital for national security, among other things, because it helps to make it more difficult for the enemy to hide submarines or lay mines effectively along the coast.[44] This way, Norway maintains a "home-court advantage" along the coastal zone. An enemy with equally good information about the Norwegian coastal zone is far more dangerous. Russian intelligence activity against such targets and defence interests may result in the property developing as an essential platform for Russian intelligence services. According to the Norwegian Ministry of Defence, the strategic location of Bergen Engines, among other things in the vicinity of defence installations, poses an increased risk of sabotage and intelligence activities toward force protection systems.[45]

The table below summarizes how the acquisition of Bergen Engines would affect warfighting functions.

TABLE 9.1 – Application of the Beachhead Warfare Theory to the Bergen Engines Case.

THREATS – ECONOMIC STATECRAFT				
	Yes	**Partial**	**No**	**Explanation (how/why)**
Economic Access				The acquisition of Bergen Engines by TMH would have been a so-called FDI where a financial transaction would have led to the company changing ownership.
State Controlled Actor				Evidence points to the fact that TMH had close ties to Russian central authorities, including the Russian Armed Forces. In addition, TMH is important in the renewal and development of Russian military capabilities.

VALUES – MILITARY ADVANTAGE					
	Domain	**Yes**	**Maybe**	**Unknown**	**Explanation (how/why)**
Manoeuvre	Maritime				Evidence shows that acquisition of Bergen Engines would have enabled faster construction and equippingof Russian vessels and capabilities connected to the maritime domain.
Fires					
C2					
Intelligence	Multi-Domain				Evidence shows that the overall knowledge and expertise Bergen Engines has acquired through its defence-related contracts is information that has a significant intelligence value for the Russian authorities with the potential to damage Norwegian security interests related to defence and preparedness across all domains.
Sustainment	Maritime				A sale of Bergen Engines would include the service organization that manages some of the maintenance responsibilities for the engines, including spare parts. Evidence shows that it is likely that access to goods, information, and service contracts through Bergen Engines would have made it possible for a new owner to carry out security-threatening activities or in other ways disrupt sustainment functions related to the maritime domain.
Force Prot.	Maritime				Bergen Engines owns a large property strategically located against the northern approach to Bergen and Haakonsvern Naval Base, a vital defence installation and main port for the Norway Navy. This property is consequently an ideal starting point for carrying out intelligence activities or sabotage in general and against Haakonsvern Naval Base in particular.

CONCLUSION AND WAYS FORWARD

Beachhead warfare represents a significant indirect threat to the military power of the target nation. In principle, it can potentially affect all warfighting functions across all domains, at the strategic, operational, and tactical levels. Furthermore, it can be employed as part of a long-term strategy to influence military power, with economic tactics used to gain access to critical military infrastructure, technology, and supply chains. This threat underscores the importance of identifying vulnerabilities in value chains, trade, and investment, as foreign interference in these areas can indirectly impact military power. The successful execution of a beachhead warfare strategy can lead to the establishment of relational dominance over other countries. This outcome is consistent with the beachhead warfare theory in which level zero and peacetime are viewed as critical phases in a conflict, as they enable the most significant preparations to be made.

While the specific case in this chapter focused on Russia, from a long-term perspective, the Chinese Communist Party (CCP) has the strongest hand to be successful with beachhead warfare. Technology transfer takes place through high levels of Chinese investment in and acquisitions of European and U.S. companies. One example is how the Chinese state firm, Mars Information Technology, took control of the Italian military drone maker Alpi Aviation in 2018.[46] The transaction was completed without the Italian authorities' knowledge, and the transfer of Alpi's intellectual and technical property to China began instantaneously.

China's integration into the global economy was predicated on the underlying notion that this regime would encourage greater economic and political openness.[47] Now that this assumption clearly has failed, the West must establish adequate mechanisms to prevent CCP from succeeding with beachhead warfare. The Chinese Counterintelligence Law from 2014 imposes obligations to relevant Chinese organizations and individuals to assist the People´s Republic of China's (PRC) security entities, and these organizations and individuals cannot refuse to cooperate.[48]

Most companies are at a disadvantage against competitors who do not need to make a profit. It can also be difficult for decision-makers, both public and private, to reject business offers that in isolation are very favourable. Consequently, Chinese companies can essentially be an instrument of beachhead warfare, creating backdoors designed specifically to advance China's military interests. Such actors will often take advantage of the fact that business decisions happen at the local level, while the consequences of these decisions impact the national level. This reality harmonizes with the characteristics of political warfare and economic warfare where the military instrument plays a less active role while the diplomatic, information, and economic instruments are at the frontline of competition in a permanent war.[49] Enhancing understanding of, and taking action against, this threat is imperative for the West to maintain relational dominance over both Russia and China.

CHAPTER

10

THE END OF SECRECY? THE IMPACT OF EMERGING TECHNOLOGIES ON COVERT SPECIAL OPERATIONS

LIEUTENANT-COLONEL MATTHIAS SCHWARZBAUER

On 4 November 2009, when an Italian judge convicted 22 agents from the U.S. Central Intelligence Agency (CIA) an historic legal process ended with a drum beat. These CIA operatives had abducted Hassan Mustafa Osama Nasr, called Abu Omar, the Imam of Milan, on 17 February 2003, supported by collaborators from the Italian Military Intelligence and Security Service (SISMI). They had snatched Abu Omar in daylight from a public street in a suburb of the Northern Italian city. The court ruling sentenced many of the Americans to several years in prison and put the United States' offensive intelligence operations in the public spotlight. The "Abu Omar case" was part of the U.S. extraordinary renditions program, designed to capture and interrogate suspected terrorists after the 11 September 2001 (9/11) terrorist attacks, often without any legal backing or knowledge from the resident's state.[1]

Yet, what makes this case so striking is the methods employed by the police investigation that quickly followed for tracking and finally identifying the CIA agents and their Italian companions.[2] The local Italian police meticulously reconstructed each of their movements from the moment they set foot in Italy until their departure nine days later, mostly based on cell phone data. The investigators precisely determined when, where and which mobile phone

was logged into the local telecommunications cell network, also identifying connections between the different devices. They could evidently pinpoint calls to the U.S. consulate in Milan and the U.S. embassy in Rome. Some American operatives had even maintained communication with their families back home.[3] The "Abu Omar case" is a stark reminder of the risks covert agents face when neglecting to effectively conceal their identities and movements. It also exposes the hubris of some Western operatives, which inevitably leads to sloppiness and vulnerability.

In the two decades since the kidnapping in Milan and the exposure of the covert CIA agents, technology in all fields has advanced in leaps and bounds. Networked cities, advanced biometrics, and near-instant information sharing have massively improved and spread, and this proliferation of technologies is not limited to Western nation-states. In the modern digital or data-driven age, terrorist organizations are tuning up their cyber capabilities, and private companies are outpacing governmental and military entities in the development of cutting-edge technology.[4] Until recently, the United States and its allies have maintained a decisive technical advantage over most other nations and organizations. But this edge is constantly shrinking. Modern tracking and surveillance software, equipment and processes – often enhanced by artificial intelligence (AI) and machine learning (ML) algorithms – are easily available for state adversaries and hostile non-state actors.[5] Compared to modern standards, the Italian investigators in 2003 were operating in the digital stone age – and yet the CIA agents were not prepared.

Special Operations Forces (SOF) emerged in the last two decades to unprecedented prominence as key assets in the global fight against extremist and terrorist organizations, offering a high probability of success with a low footprint. Yet, while carefully selected, highly trained, and extremely resilient, their *modus operandi* of working remotely in small teams makes SOF operators vulnerable in case of detection or loss of initiative. Beyond some prominent and "Hollywood-esque" helicopter-inserted raids, SOF regularly employ covert or clandestine methods for executing their missions, unseen by both the enemy and the public. They routinely move and communicate discreetly when traveling in, through, and out of their target areas. However, increasingly sophisticated technologies now add an extra layer of complexity and

vulnerability to SOF's high-risk missions. The proliferation of such disruptive technologies influences all aspects and means of modern intelligence and military operations, including special operations. While special operations and intelligence operations are legally clearly distinct, they broadly share applied techniques and procedures when conducted covertly. Hard-won lessons learned from intelligence operations can therefore be critical in reducing the risk to the SOF operators deployed in covert and clandestine operations.

This chapter discusses the role of emerging technologies and advancements in surveillance, tracking, and biometrics for the risk calculation in secret special operations. The central question is if secrecy in the execution of covert and clandestine operations is still possible – or even still desirable. In particular, the text focuses on the dangers to the deployed ground forces during and after an operation, especially when adequate technical, educational, and personal preparations are neglected. While there is a considerable risk of diplomatic or, at worst, violent blowback for invested nations, the discussion does not delve into the strategic implications for state-to-state relationships. Additionally, the employment of non-uniformed SOF, at least for parts of an operation, is a highly sensitive issue. Thus, the final responsibility for the legal specificities of any military operation rests with the respective nation.[6]

After clarifying the elementary terms "covert" and "clandestine," the chapter broadly follows the typical process of a secret special operation: first, the planning phase with information gathering, the selection of on-ground personnel, and the establishment of a robust communications plan; second, inserting and infiltrating into the target country and the covert movement to and from the desired objective avoiding hostile surveillance; and third, returning home after mission execution and the long-term impacts of data storage and traces left behind – a constant risk in a high-tech environment.

COVERT AND CLANDESTINE – SPECIAL OPERATIONS IN THE SHADOWS

Special operations aim to achieve strategic-level effects and often inherit significant political and diplomatic consequences in both success and failure. These "politico-military considerations may require clandestine operations

and the acceptance of a degree of political or military risk not associated" with missions by other military units.[7] The North Atlantic Treaty Organization's (NATO) SOF doctrine underscores the need for "clandestine capabilities/techniques" to execute special operations successfully while mitigating the risk of detection or attribution.[8] Though not every SOF mission requires clandestine or covert execution, secretive elements may be integrated into any of the SOF tasks, from direct action (DA) to military assistance (MA), but with particular relevance for special reconnaissance (SR) missions.

The terms "clandestine" and "covert" are regularly misinterpreted, interchangeably used, or not generally accepted, and therefore demand clarification.[9] NATO defines a "covert operation" as "an operation that is planned and conducted so as to conceal the identity or permit plausible deniability of the executor."[10] On the other hand, a "clandestine operation" is "an operation planned or conducted in such a way as to assure secrecy or concealment."[11] In other words, "covert" focuses on masking the identity of the executor and permitting plausible deniability of any governmental or national involvement, while the effects of the operation may still be visible and detectable. The concept of plausible deniability is central to covert operations. "Clandestine," however, goes a step further requiring secrecy not only in terms of who conducted the operation but also in the activities undertaken and the effects created, even in a non-attributable manner. The term "secret" is used in this chapter as a compound term for both covert and clandestine operations.

In the history of special operations, covert methods have frequently been employed. A noteworthy example is a British Special Air Service (SAS) operation in Gibraltar in March 1988, when the SAS soldiers killed three Irish Republican Army (IRA) terrorists.[12] Gibraltar is a British Overseas Territory and the political risk associated with extrajudicial killings of British citizens on de-facto national soil was significant. Covert techniques were thus used by the SOF operatives to infiltrate British territory. Another prominent example is the attempted assassination of former Russian spy and double-agent Sergei Skripal in Great Britain. Skripal and his daughter were poisoned by GRU agents, the Russian military intelligence service, with a toxic nerve agent in 2018 – which they luckily survived.[13] After a meticulous investigation utilizing various

technical surveillance systems, the British authorities were able to identify the individuals responsible as Russian agents.

However, while these former examples represent direct action or kinetic SOF tasks, secretive methods are even more regularly employed in reconnaissance missions. These covert, and more often clandestine, operations have significant operational overlaps with missions carried out by intelligence agencies in terms of tactics, techniques, and procedures (TTPs). An example is the deployment of Australia's Special Air Service Regiment (SASR) for civilian intelligence-gathering operations in Africa in 2011. Australian foreign intelligence agencies were officially not involved and the SASR operation therefore constituted a grave violation of national Australian laws.[14] Despite these few known negative examples, all eventually exposed through effective investigations or intelligence leaks, it is important to note that most successful covert and clandestine operations remain what they are intended to be: secret operations outside of any public perception.

MISSION PLANNING: INFORMATION GATHERING, PERSONNEL SELECTION, AND COMMUNICATIONS

A well-thought-out plan is the cornerstone of any military operation, but it must also leave enough room for creativity and adaptability when the mission unfolds. Special operations are no exception, and every SOF mission, even those requiring rapid responses to emergencies, begins with a planning phase. Sensitive operations in particular, aimed for maintaining the cozy cover of secrecy, demand meticulous preparation. The constant cycle of information-gathering, analysis, detailed planning, and rehearsals is vital in this initial stage to increase the chances for mission success and the safe return of all personnel. Typically, at the beginning of the operational and tactical planning phase, the designated unit or formation receives a package with intelligence products, coordination methods, and other pre-determined details. Still, this package is often just a pitch and the starting point for more in-depth examination. The following section highlights key planning considerations and explores the influence of modern technologies.

Open-Source Intelligence (OSINT) plays a substantial role in the planning of covert or clandestine operations, especially given the myriad of bits and pieces of information digitally shared on internet platforms and social media. Intelligence packages normally include a mix of analysis products from various intelligence collection disciplines (INTs), such as Human Intelligence (HUMINT) and Geospatial Intelligence (GEOINT). HUMINT builds on information from human sources, while GEOINT relies on the analysis of imagery and data related to specific locations.[15] Although these intelligence fields have had to adapt to technological advancements like AI-powered surveillance systems, data scraping, and the prevalence of disinformation, their core methods and processing sequences have largely remained consistent. In contrast, OSINT has seen a dramatic transformation in its prominence and impact on operational planning. The wealth of digitally available information, far beyond classic media like television or newspapers – from in-depth descriptions of urban areas and infrastructure to individual profiles, timelines, and economic and social patterns – is staggering. Even sensitive personal information is easily accessible with just a few clicks. ML and smart scraping tools also aid in sifting through this plethora of data, further enhancing the role of OSINT in the modern operational landscape.[16]

The rise of AI-generated fake information, such as altered images, fabricated narratives, and highly convincing deep fakes, poses a risk to the integrity of data used in operational and tactical planning.[17] This rapidly evolving technology provides new means for hostile deception, with, in the worst case, dramatic consequences for the invested SOF operators. Therefore, exercising caution in selecting and evaluating OSINT information is crucial. SOF units should prioritize continuous education for all operational personnel, not only intelligence and reconnaissance specialists, in the latest developments in AI and data verification techniques. Specifically for secret missions, where access is highly restricted, educating and sensitizing all involved personnel can mitigate risk-to-force from the earliest stages of the operation.

This issue of cover stories highlights a key difference between intelligence and SOF personnel. Whereas intelligence operatives often have a robust, artificial background in place, most SOF personnel have only a basic layer of

identity cover that may not withstand in-depth scrutiny.[18] Once the planning for a covert or clandestine special operation is approved at the strategic and operational level, the task is delegated to tactical formations. Yet, selecting the appropriate unit, and more critically, the right individuals for mission execution is challenging. Key considerations for designating a SOF unit are factors such as specialized training, level of preparedness, and resource availability. Beyond that, the SOF operators also have to regularly employ cover stories in these secret operations to disguise their origin and justify their presence in the target area. Individual factors like language proficiency, cultural and ethnic background, and operational history come into play. Since only a limited number of personnel are typically directly involved on the ground, individual operator selection requires a very careful assessment. The cover stories must cohesively tie various factors together to form a credible, unsuspicious, and sustainable narrative that can withstand skeptical questioning.[19]

The operators' social media presence is a critical factor in lending authenticity and realism and is directly linked to OSINT. Beyond the accessible data on the operational environment or targets, the openly available information on military units and individual SOF personnel can now also be consequential. Made-up personalized social media accounts offer a simple solution, but more modern ML tools can easily discern between genuine and fabricated profiles.[20] Moreover, a credible digital footprint extends a simple Facebook or Instagram profile, and encompasses elements like a variety of email addresses, online shopping histories, social network interactions, and even records of financial transactions. Fabricating such an amount of data and designing comprehensive, convincing, and "ML-proof" digital cover stories is incredibly demanding.[21] The option to use the operator's actual social media histories – modifying only the most sensitive information – offers a potent approach to mitigating the risk of early detection but undoubtedly jeopardizes individual identities and exposes potential venues for retribution.

The next crucial planning consideration after gathering the necessary information and selecting the SOF personnel is designing a robust communications plan. Effective coordination between individual operators, teams, and higher command centres relies heavily on advanced communication methods for

fluent mission execution. While SOF operators are regularly trained in low-tech information-sharing techniques, such as setting up dead drop locations, the dynamics of an operation often demand flexible responses and real-time communication. The selection of the fielded hardware like smartphones or laptops usually depends on the available models in the respective target country. Devices must blend in with those commonly found in the operational area to avoid drawing attention. Still, the decision has to be made whether the SOF operators bring their communication means with them, or if they are to organize the necessary hardware via the local market.[22] While specifically manufactured crypto phones offer secure communication, their often unique appearance and software functionalities can make them conspicuous.[23] Instead, software solutions embedded in open-source operating systems and working via trusted, or ideally governmental owned, networks and servers, often provide a more discreet alternative, but require a technologically adept organization with the required server infrastructure in place. Furthermore, these systems should employ additional security measures such as virtual private networks (VPN), frequent IP address changes, and deceptive counter-measures.[24] These features help to obfuscate the digital footprint, reducing the chance of tracing the SOF operators back to their originating units.

Planning for encrypted communications inevitably raises the question about the future impact of quantum computing. While quantum technology is still largely experimental, it is already foreseeable that today's cryptographic methods will be easily deciphered in the quantum era.[25] The dramatically increased processing power will render current algorithms useless and will likely also accelerate the development in AI, further impacting other surveillance means. Nevertheless, just as military and intelligence methods have historically evolved in a cat-and-mouse game of new measures and countermeasures, future SOF operators can expect to leverage new technologies or tactics themselves to counter the advancements in quantum computing.

However, more immediate and tangible concerns arise from the performance of modern electronic warfare (EW) capabilities that hostile states use to detect and disrupt electromagnetic communications, affecting everything from traditional military radios to advanced smartphones. Technologically savvy

actors like the People's Republic of China (PRC), the Russian Federation, or Iran not only have a capable EW defence industry but also proliferate their products worldwide.[26] For covert and clandestine special operations demanding complete non-detection of personnel on the ground, this imposes severe constraints on how, where, and when to communicate to avoid unwanted attention. Still, the amount of overlapping electromagnetic "noise" is globally exponentially rising – especially in urban centres – and offers new possibilities for hiding "in the noise." For hostile counterintelligence services, detecting and identifying suspicious signals without any additional hints remains taxing.

An effective approach for navigating these challenges in communication in a contested and high-risk environment might combine advanced technology with rigorous planning of means and patterns, including low-tech fallback methods like dead-drops or couriers. Ultimately and undoubtably, the key to success of any covert or clandestine special operation lies in the professionalism and realism in planning, the discipline in execution, and the flexibility and resiliency of the operators in the field.

IN THE TARGET AREA: MOVEMENT IN A HIGH-TECH ENVIRONMENT

Once the operational planning is completed and all details are refined, the final plan has to pass several layers of authorization respecting the high-risk nature of covert operations. Finally, after receiving the execution order, SOF start to deploy and move towards their target area. Up to this point, the risks associated with the mission lay largely in the political and strategic sphere but now extend to the tactical level, directly impacting the individual forces on the ground.

The movement of personnel and equipment poses increasing challenges over the multiple phases of covert or clandestine special operations, especially regarding the growing proliferation of advanced biometric data collection and AI-supported surveillance systems. While the initial part of the travel, until reaching the hostile-controlled areas, can sometimes be supported by the team's own national military forces, allies, or partners, operating inside the target area is usually highly remote. International travelers, even to developing regions, are most often welcomed by border officials equipped with a range of

identifying biometric capabilities, such as digital fingerprinting, retinal scans, and facial recognition.[27] The use of pseudonyms or various passports becomes impossible. While the collection of biometric data is not surprising, still, the storage of personal data of SOF personnel has long-term implications for future mission planning. Nevertheless, if a cover story can successfully integrate with this data collection, it may offer the chance for "de-sensitizing" hostile security measures and to "normalize" the movements and border crossings following an unsuspicious pattern.

Beyond the collection of biometrics, the boost of technical surveillance means by AI and self-learning and self-informing networks poses significant challenges for the movement and communication of covert SOF personnel. Already today, the density of surveillance systems with a growing number of closed-circuit television (CCTV) cameras can hamper sensitive missions. While authoritarian countries like the PRC are infamous for the mass surveillance of their population, even Western nations like the United Kingdom (UK) are intensively monitored.[28] As of 2020, an estimated 5.2 million CCTV cameras were in use in the UK.[29] These systems also notably played an important role in tracing and identifying the Russian agents involved in the Skripal poisoning case in 2016.[30]

Furthermore, the surveillance and monitoring of movements extends beyond the identification of individuals via cameras. Vehicles and public transportation are routinely monitored, as are electronic devices connecting to local telecommunications cells. AI added to these monitoring systems offers the potential to multiplying the speed of in-time information sharing and putting together a nearly perfect picture of past and current patterns. Connecting all these means in an AI-powered system also creates a nearly impenetrable web of 24/7 surveillance and data storage. In SOF operations, when completely avoiding these systems is impossible, the best chance to outsmart the AI is to fit into a reasonable narrative and hide in the flow of the population around.

Effective and efficient coordination among all SOF elements is pivotal for a successful mission, be it a pure reconnaissance operation or a more offensive activity. The central question is if, when, and where the SOF team meets

for synchronization. Physical meetings can bypass hostile EW and signals intelligence (SIGINT) interferences, but leave operators more exposed to local counterintelligence efforts and physical shadowing. Remote meetings, on the other hand, can make use of unsuspicious chatrooms and various digital platforms, often supported by disguising encryption technology. Institutions such as the United Nation's Office of Counter-Terrorism and the European Union's Radicalization Awareness Network have already warned about the misuse of digital platforms, including in-game chat functions in online games, by terrorist groups.[31] While the motivations of terrorists and SOF operators are diametrically different, both entities need to evade detection, and as such, may employ similar communication methods to maintain secrecy. Still, when using electronic means, especially radio-based devices like smartphones, the SOF operators must keep the possibility of enemy surveillance constantly in mind. Technical SIGINT instruments like IMSI-catchers[32] or deliberately disseminated spyware can infect or burn the respective hardware.[33] To identify such threats, the SOF personnel on the ground depends on robust technical training and expertise to recognize hostile countermeasures.

An additional vital factor when navigating through a sensitive environment is money: how to pay for transport, lodging, and food while constantly avoiding detection and maintaining cover. Cash seems to be a simple and easy possibility and offers anonymity, but carrying large amounts might raise suspicion, especially as many societies are trending towards cashless transactions. On the other hand, digital payments via credit cards or common internet platforms, although convenient, risk leaving an additional digital trail. Cryptocurrencies and respective exchange platforms are emerging alternatives for making payments without unintended leaks, particularly as their use gains traction in regions like Africa and South America.[34] The tracking of digital money flows based on blockchain technology is by design nearly impossible and offers a secret means for necessary payments.[35] Nevertheless, the feasibility of this method depends on the local conditions.

Finally, after the undetected and covert reach of the target area, the specific operational activities, the "action on target," depends on the task at hand. Thus, the discussion of the impact of emerging technologies on varying

SOF mission profiles is beyond the scope of this chapter. However, it is crucial to emphasize that the challenges for the SOF operators on the ground do not end with the mission execution at the target. The exfiltration phase can be as critical as the infiltration phase, if not more so. Especially when the operation results in immediately visible effects, the attention of the local security forces, counterintelligence agencies, or military or law enforcement organizations will be on high alert. The SOF operators have to face the same obstacles regarding coordination, communication, and movements, just with higher urgency. While a swift withdrawal to friendly territory might be a natural reflex, maintaining disciplined concealment is the best protection for small teams leaving a hostile area.

AFTER RETURNING HOME: RESIDUAL TRACES AND DATA STORAGE

The "success" of a covert or clandestine operation depends on several factors, and a definite assessment might only be possible in the long-term, if at all. The uncertainty about what traces may have been left behind, or may yet be found, demands reluctance to celebrate too quickly. Still, paramount for calling an operation a success is the safe and unharmed return of the deployed SOF operators, which should guide the political, strategic, and operational decisions throughout the planning and execution, at least in most liberal democracies.[36] Furthermore and not surprisingly, the success of the mission depends on whether it achieved the ordered objectives and if it met the desired intent. Still, the least tangible aspect of efficacy are the possible long-term implications for potential follow-up operations, depending on the residual breadcrumbs.

The measure of a successful operation also may vary depending on whether it is covert or clandestine. The defining principle of a clandestine SOF operation is complete secrecy: the mission must not only achieve its military objectives but also remain entirely undetected. This outcome is increasingly challenging given the advancement in surveillance technologies and proliferating EW, SIGINT, and data storage measures. On the other hand, the hallmark of a covert SOF operation is plausible deniability. For a successful covert mission, the strategic goals must be met while obscuring the operators' identities

and national affiliations. However, they can have tangible and visible consequences that serve as a means of signaling to show resolve, create uncertainty, and change an adversary's calculations. These outcomes can vary in visibility, from subtle effects known only to the intelligence community to more overt effects visible to the public.

The long-term effects of a covert or clandestine SOF operation largely depend on the traces left behind and the ability of the local agencies in the target country to detect these inevitable breadcrumbs. Political and strategic decision-makers must accept that all operations leave some traces in a contested high-tech environment. Furthermore, the sophistication of modern surveillance technologies and big data analytics increases the likelihood of detection, and some data will knowingly, and mostly unknowingly, be collected. On the one hand, the sheer volume of data is a new chance for cover, a "needle in the haystack" scenario. The larger this "haystack," the harder the data analysis. On the other hand, however, the growing processing power and advancements in ML and AI algorithms, paired potentially with future quantum computing, will improve the ability to identify anomalous behaviours and discern potential threats. Even if an operation goes entirely undetected, the long-term data storage capabilities of modern systems offer an avenue for post hoc pattern and actor recognition, potentially compromising operations that lie years apart. Therefore, understanding and recognizing the opportunities and threats posed by emerging technologies is a crucial starting point when envisioning the next secret special operation.

CONCLUSION: SECRECY NEWLY DEFINED

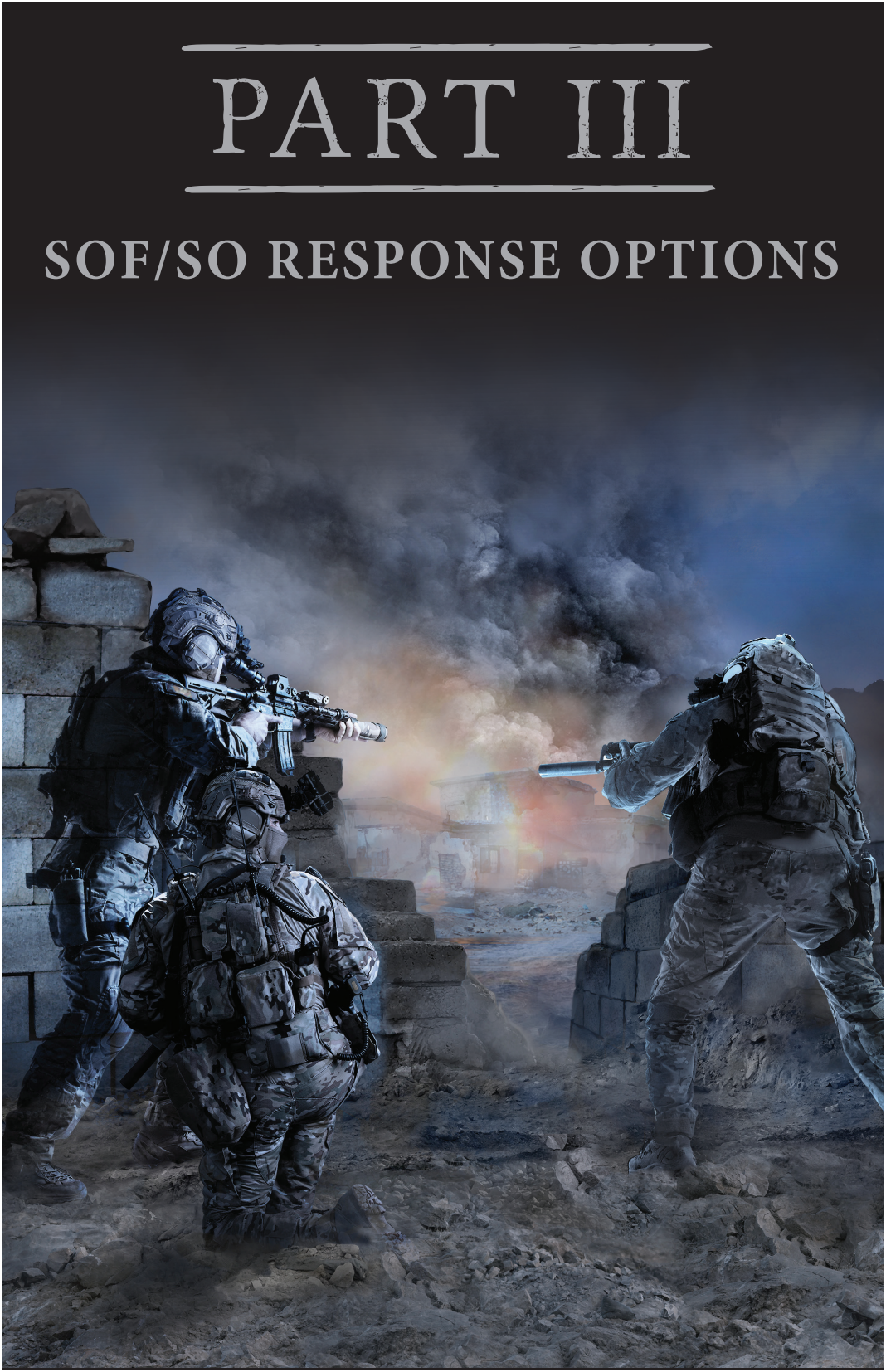
Emerging technologies have the potential to impact virtually every facet of a covert or clandestine special operation. Rather than discouraging future missions, these advancements merely shift the demands on SOF. When operating against technologically savvy adversaries, covert operatives must balance staying on the edge of technical advancements and honing their proficiency in analog skills.[37] While this chapter directs its lens largely at the risks to the SOF operatives on the ground, it also emphasizes that future secret missions are still feasible. Technical expertise combined with creativity, adaptability, and

mental resilience offer great potential for facing the global strategic challenges ahead, and will likely become core attributes for future SOF. Keeping the military and intelligence organizations abreast of the accelerating technological trends, and openly and boldly informing political decision-makers about the chances and risks, is the prerequisite for continuously safeguarding the SOF personnel on the ground, and for the future execution of successful secret special operations.

Secrecy is not dead; it just looks different. It has been redefined rather than eliminated. What once required total concealment has evolved into today's "hiding in the noise" amid the billions of everyday analog movements, and the countless bits and bytes of the exponentially growing digital world. In the coming years, trends like AI, quantum computing, and growing data storage capacities are likely to change this notion again, and demand constant adaptations in covert tactics and techniques. Today's decision-makers and SOF communities have the responsibility to plan ahead, prepare, and educate the future forces on the ground. Had the CIA agents in Italy two decades ago adequately prepared and adapted to the increasingly high-tech landscape, the "Abu Omar case" might have remained undisclosed. But due to their overconfidence and lack of technical understanding, they provide a great example of a covert operation done wrong.

PART III

SOF/SO RESPONSE OPTIONS



CHAPTER

11

EVOLUTION OF SOF IN CONFLICT

MAJOR CHRISTOPHER M. BOSS

When it comes to predicting the nature and location of our next military engagements, since Vietnam, our record has been perfect. We have never once gotten it right.

Secretary of Defense Robert Gates[1]

Special Operations Forces (SOF) are a military's paramount agents of innovation in the implementation of technological and procedural strategies and yet they are inadequate to rapidly adapt during conflict.[2] To remedy this shortcoming, the special operations communities must fully understand the aspects of organizational evolution that enable entities to grasp the changing environment and transform accordingly. Despite the provisions of Part II of this book, which outlines potential threats, and Part III, which offers insights on how SOF can tackle these threats, an excessive fixation on any single threat or approach is unwarranted. Moreover, technological advancements are highly unpredictable, and the unorthodox methods that adversaries will use to exploit these threats render any specific recommendation obsolete. Therefore, it is incumbent upon SOF units to systematize innovation internally in order to create the necessary conditions that normalize it, thereby facilitating rapid evolution. Without this ability to evolve, SOF units will remain highly vulnerable in high-intensity situations.

This chapter aims to present an overarching framework that elucidates the how and why SOF elements evolve during conflict, thereby enabling them to adapt and transform during periods of peace. To achieve this goal, the initial section focuses on distinguishing between organizational adaptation and organizational evolution, emphasizing that while adaptation is critical, evolution is essential. The triggers for organizational adaptation and, ultimately, evolution, arise from technological advancements and responses to an adversary's way of fighting. These triggers can lead to technological, organizational, or doctrinal adaptations, contingent upon various organizational mechanisms such as financial limitations, cultural aspects, leadership style, and political exigencies driving the need for adaptation. When an organization comprehends and simplifies the navigation of these mechanisms, the likelihood of successful organizational adaptation increases significantly.

To facilitate this process, the military unit must establish a systematic approach to innovation within its community. Among all military units, though, SOF units possess exceptional capabilities for institutionalizing innovation within their community owing to their smaller size, openness to unconventional thinking, and ability to research and develop novel ideas and practices in real-world contexts. By following this streamlined innovation process, SOF units may effectively evolve in anticipation of the evolving pre-conflict environment, but this first necessitates a comprehensive understanding of organizational evolution.

ORGANIZATIONAL EVOLUTION

Comprehension of evolution on military entities holds critical significance as it empowers such organizations the ability to unravel the intricacies of evolutionary mechanisms and, consequently, expedite the process of organizational evolution. Evolution, hence, refers to the adaptation of an organization's lineage in response to the environment. It distinguishes itself from simple adaptation, which encompasses any change to an organization's structure or function that makes it more suited to its environment.[3]

The difference between evolution and adaptation is vital. Instances of "Combat Darwinism" frequently yield adaptations in military units, terrorist organizations, and insurgent groups, yet their lineage – their identity, mission, and vision – remains unaltered even after the alteration.[4] Evolution, on the contrary, provokes a fundamental shift in how an organization perceives itself. An exemplary illustration of this can be observed in the transformation of the United States Navy SEALs.

In April 2022, Rear Admiral Hugh W. Howard III delivered a statement before the United States Senate Armed Services Committee, highlighting the ongoing process of "urgent transformation" within Naval Special Warfare (NSW).[5] The urgency of this transformation stems from the Navy SEALs' significant shift over the past two decades, transitioning from a maritime-focused commando force to a land-based one. Initially tracing their roots back to the Underwater Demolition Teams of World War II, the SEALs primarily served in a maritime support capacity for large-scale combat operations.[6] However, the landscape changed following the September 11th (9/11) attacks and the emergence of the Global War on Terror (GWOT) necessitating numerous simple adaptations for the Navy SEALs in order to remain pertinent in this new context. Ultimately, over time, these adaptations caused the SEALs to evolve their role and identity.

Presently, as the environment undergoes yet another transformation, the SEALs aim to rediscover their maritime heritage. But unlike during the GWOT, where the crucible of war propelled their evolutionary journey towards becoming a land-based force, the current shift back to a maritime force lacks similar immediate external catalysts. This predicament is not unfamiliar territory for the Navy SEALs, as evidenced by their experiences in the 1960s when the Vietnam War necessitated their evolution to a land-based force advising South Vietnamese units.[7] Subsequently, it took several decades of gradual adaptations for the SEALs to reestablish their roots as a maritime-oriented force once the war had concluded. Thus, it becomes imperative to comprehend the underlying mechanisms that drive evolution, enabling the desired transformations to take place swiftly and pre-emptively, even in the absence of war.

The biological connotations within this example indicate that organizational evolution is both a process and an outcome that are spawned through environmental causes. For this reason, the term "evolution" has been adopted in lieu of "military innovation" because it aligns more closely with this chapter's intended goals: how and why SOF units can adapt to changes in warfare. Moreover, the absence of consensus within the innovation community regarding the precise definition of military innovation suggests that attempts to establish an acceptable definition may serve only to obfuscate the issue, thereby diverting valuable resources away from more critical analysis of the processes required to expedite the evolution of SOF organizations.[8] Therefore, emphasis will be placed on both the process and outcome of organizational evolution, commencing with the environmental causes that instigate the evolutionary process of a military unit.

PROCESS OF ORGANIZATIONAL EVOLUTION

Organizational descendancy originates predominantly from technological revisions or in response to an adversary's way of fighting. The magnitude of technological progress or degree of radicalness of the enemy's approach to warfare is directly proportional to the probability of innovation adaptation, as illustrated in Figure 11.1. It should be noted, however, that these influences alone cannot ensure the evolution of an organization. There exist organizational mechanisms such as leadership style, financial constraints, organizational culture, and political pressures, which may accelerate or stagnate requisite changes needed to alter the military unit's lineage. Nonetheless, given the appropriate conditions, a unit can evolve via technological, organizational, or doctrinal innovation.

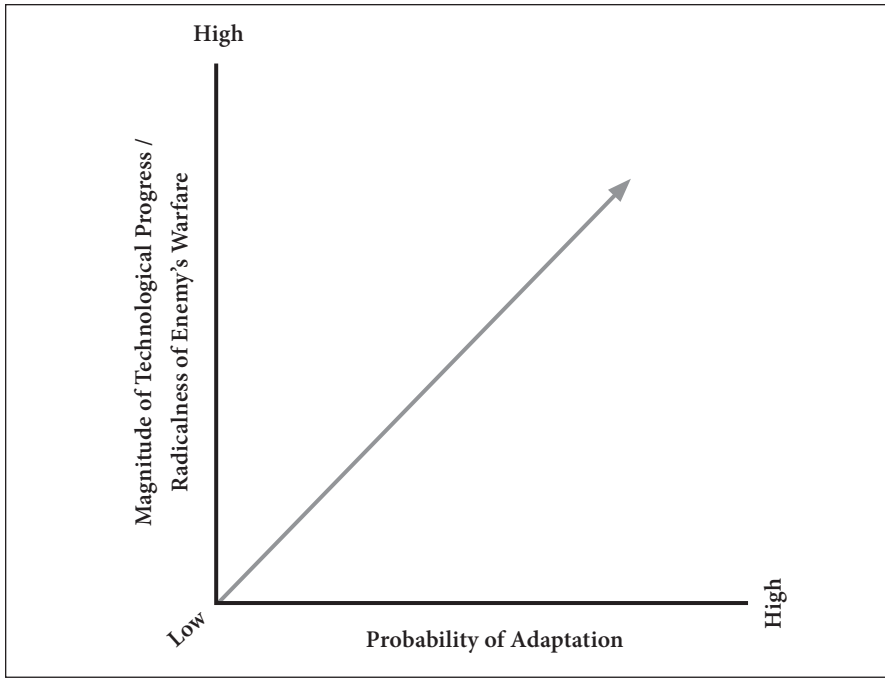


FIGURE 11.1 – The Greater the Technology Innovation or the More Radical the Enemy's Warfare, the Greater the Likelihood of Innovation Adaptation

Technological, organizational, or doctrinal adaptation emerge from the advent of technological or tactical invention, or from innovative uses of old technologies or tactics (i.e., exaptation).[9] The inception of technological, organizational, or doctrinal innovation is seeded by inventions and innovative applications, exemplified in Illustration 11.1. The profundity of technological advancement or the radicalness of warfare is reflected by the roots, while the growth of an innovation's adaptation is represented by the trunk of the tree. Sometimes, the emergence of only one type of adaptation occurs, as indicated in Tree A. However, unless such innovation is disruptive in nature, it may fail to catalyze sufficient change within an organization to generate evolution.[10]

Oftentimes, though, the adaptation of one type of innovation spurs the development of complementary forms of innovation, as illustrated in Tree B.[11] In such instances, the likelihood of organizational evolution is heightened,

but again, not guaranteed. Much like a plant relies on multiple factors such as the soil, the sun, climate, and water, organizational adaptations rely on several pivotal organizational mechanisms.

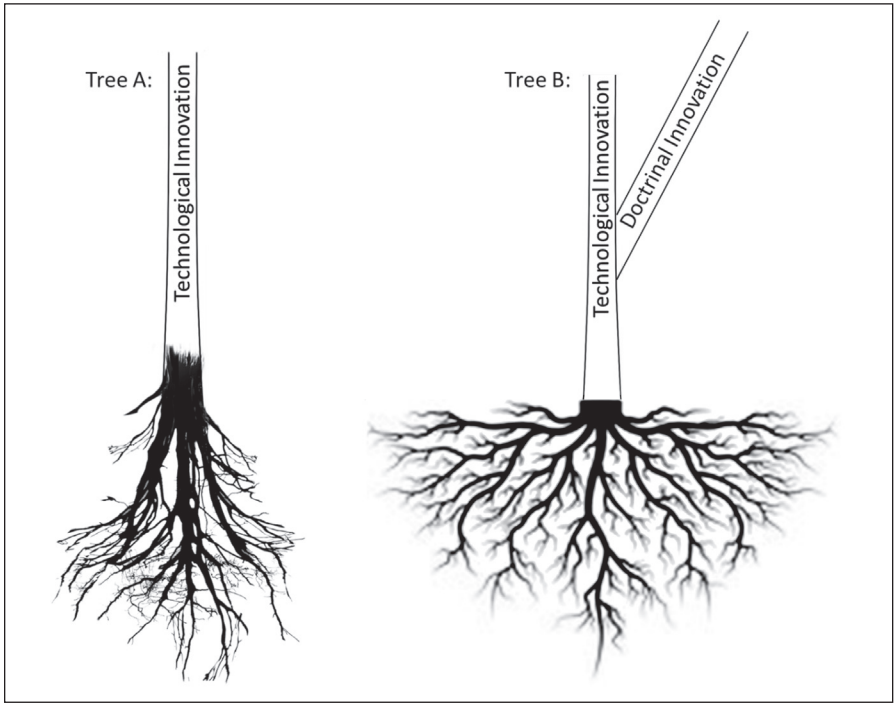


ILLUSTRATION 11.1 – *The Genesis of Adaptation*

MECHANISMS OF ORGANIZATIONAL EVOLUTION

Organizational adaptation within a military unit is determined by a confluence of factors, including but not limited to financial limitations, organizational culture, leadership style, and political exigencies. These mechanisms present within an organization can be likened to a labyrinthine structure that any innovation must navigate in order to permeate the entirety of the organization, as visually depicted in Figure 11.2. Though each of these factors' labyrinthine pathways may not be excessively intricate, the challenge for an innovation lies in the compounding effect that these mazes have on one another, resulting in a maze that is exponentially more complex. While prior research has tended to focus on one or two of these elements in isolation, it appears that a synthesis

of these factors is the key determinant of whether an organization will adapt successfully.[12] To apprehend the intersection of these mechanisms, a thorough investigation of the preeminent theories for each element is imperative. Only by such an approach can one achieve a comprehensive understanding of the complex interplay between these multifaceted factors and their collective impact on the organization's ultimate ability to evolve.

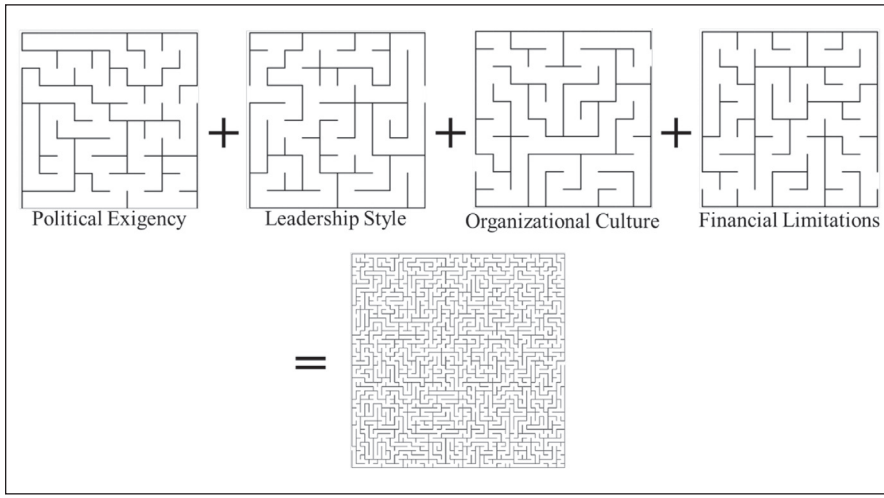


FIGURE 11.2 – Organizational Influence on Likelihood of Organizational Evolution[13]

Professor Michael Horowitz contends that there are two primary factors that determine successful implementation of innovative ideas: financial intensity and organizational capital.[14] *Financial intensity* refers to the cost per unit of hardware and the extent of military-oriented technologies involved in the innovation. Horowitz hypothesizes that the higher the financial intensity required for implementing the innovation, the slower its diffusion will be at the system level.[15] In other words, there is a lower probability that an organization will adapt to the innovation if it incurs significant financial costs.

The second crucial factor is organizational capital, which refers to the intangible assets that allow an organization to adapt and respond to presumed changes within the core ecosystem.[16] The level of bureaucracy, age of the organization, and its culture of experimentation all impact the unit's ability

to leverage its organizational capital. Horowitz hypothesizes that the "greater the organizational capital required to implement the innovation, the slower" its diffusion will be at the system level, and "the lower the probability that a state will attempt to adopt the innovation" in the first place.[17] In essence, organizations must determine whether they have the financial resources and the organizational agility for adaptation to occur. If the answer is negative or inadequate for either of these factors, the diffusion of a new innovation will be sluggish or non-existent. However, diffusion may never occur if an organization cannot grasp the significance of the changing environment.

The capacity to comprehend advancements in technology and warfare may be contingent upon the fundamental cultural and cognitive traits ingrained within the community. Dima Adamsky asserts that it is this aptitude to identify and comprehend a disjuncture in warfare – the swift transformation in techniques and modalities of combat – which constitutes perhaps the most pivotal facet of military evolution.[18] Consequently, a comprehensive awareness of the underlying cultural traits becomes imperative in ascertaining an organization's capacity to apprehend the ramifications of technological changes and paradigm shifts in warfare.

Political scientist Dima Adamsky has posited that variance among cultures stem from three cardinal features – social structure, time-orientation, and communication style – which exert a profound impact on a culture's cognitive style.[19] The cognitive style of an organization is a critical determinant of its ability to apprehend, arrange, and process information, with two predominant styles: holistic-dialectical thought and logical-analytical thought.[20] Organizations that have a natural inclination towards holistic-dialectical thought are better able to understand new shifts in the relationship between the focus point and its context than those who prefer logical-analytical thinking. Additionally, these organizations can explain occurrences by relating them to other concurrent events, even if they lack analytical coherence. Conversely, logical-analytical reasoning excels at decontextualizing entities into categories and perceiving the causal interconnections among their constituents. While both cognitive modalities offer advantages and drawbacks, it is vital to recognize the nature of the organization to avoid overlooking the advantages

of the alternative style. Since each cognitive style affects the methodology and, therefore, yields distinct outcomes, the type of leadership is essential for effective implementation.

The presence of effective leadership across all levels of an organization serve as linchpins to the successful diffusion of innovation adaptations and, consequently, the evolution of the unit. According to Professor Tai Ming Cheung and his fellow researchers, the organizational leader holds the key to allocating financial, technological, and human resources towards the innovation, and plays a critical role in its acceptance or rejection.[21] This concept is further expounded upon by military innovation expert Benjamin Jensen, who insightfully classifies these roles into two distinct categories, namely "incubators" and "advocacy networks."[22] Jansen views incubators as "informal subunits established outside the hierarchy," providing officers with the freedom to explore novel approaches to understanding the environment.[23] Meanwhile, advocacy networks comprise leaders from all echelons of the organization, who serve to promote and legitimize the innovations generated within the incubators. Of utmost significance for the diffusion of ideas is leadership advocacy, as it engenders political exigency.

Innovation adaptation within military organizations during peacetime is typically contingent upon political exigency, which is often instigated by the concurrence of military leadership. Agreement of a good idea can prove to be a delicate matter, as the acceptance of novel concepts within certain military units may be subject to the influence of the hierarchical structure of service members. For this reason, it normally takes substantial political urgency for military units to implement an innovation. While the routinization of procedures can enhance efficiency and ensure current safety standards, neglecting beneficial proposals in the midst of evolving warfare necessitates military organizational evolution. To achieve this, it is imperative for leaders to utilize collective agreement to sway senior military officials and policy-makers. The pivotal role of advocacy networks lies in facilitating this process.

The current section expounded upon the complexities of each influential organizational mechanism, which can either complicate or simplify the

organization's labyrinthine path towards adaptation. When each mechanism is understood, the overall maze becomes streamlined, thereby augmenting the probability of successful innovation diffusion, as depicted in Figure 11.3. But notice that even within the streamlined labyrinth, the route to successful adaptation remains unknown; an individual will still take wrong turns and may never locate the end point. Evidence that the labyrinth is becoming simplified is gauged by an increase in the number of adaptations an organization experiences. Therefore, a comprehensive understanding of the three aspects of organizational evolution – the catalyst that instigates innovation, the possible types of innovation, and the organizational mechanisms that affect the likelihood of innovation adaptation – enables organizations to rapidly identify the shifting environment and promptly adapt to it. This model of organizational evolution is applicable to both the military and civilian sectors. Hence, why is it essential for the military to prioritize the institutionalization of innovation, and what is the underlying reasoning for this emphasis?

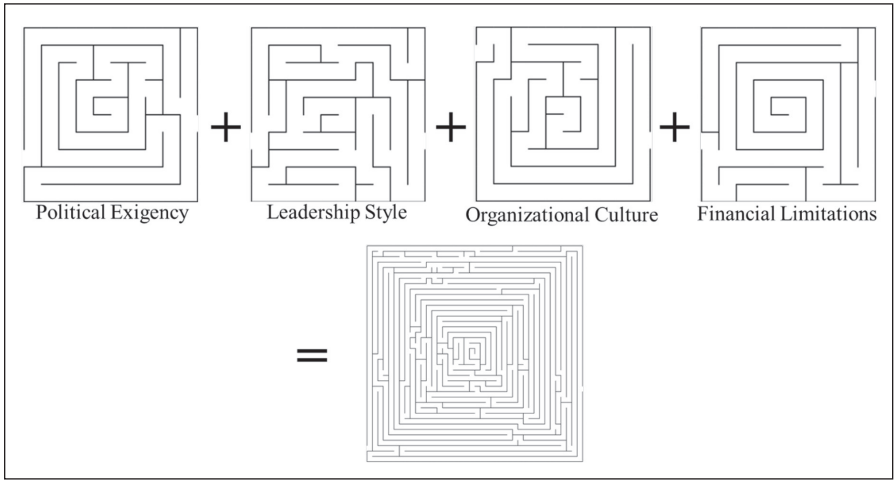


FIGURE 11.3 – Impact of Understanding Organizational Mechanisms on the Likelihood of Innovation Adaptation[24]

THE PROBLEM WITH MILITARY PROBLEMS

The problem with military problems lies in their inherent complexity (sticky information) and labeled significance (null problems).[25] Consequently, the vast sums of money allocated by governments to the civilian sector meant to

identify solutions to problems containing sticky information – experience-required knowledge – are futile since these corporations lack the necessary insight to fully grasp the problem.[26] Moreover, most military issues are categorized as null problems, which may seem trivial but possess tactical significance capable of impacting operational and, potentially, strategic levels. This limited presentation of designated "critical" issues to civilian entities means that a multitude of problems are being overlooked. Thus, a systematic approach to innovation within the military is imperative to address military issues effectively.

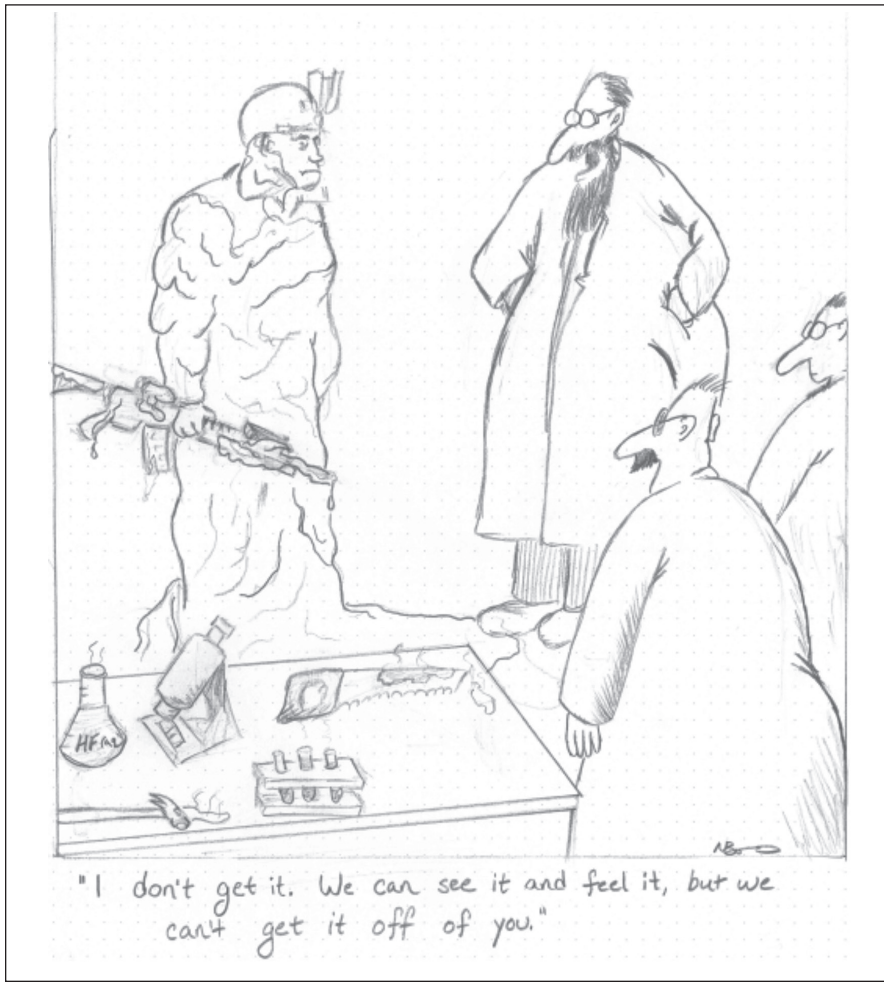


ILLUSTRATION 11.2 – *Sticky Information*[27]

Commercial entities persistently endeavour to uncover a solution to a proposed problem they do not fully understand and *cannot* fully understand. While the difficulty level of the problem itself may not be insurmountable, there are numerous factors and variables that evade effective articulation to someone who lacks the requisite experience. In accordance with Illustration 11.2, civilian Research and Development (R&D) personnel strive to comprehend a soldier's deployment experience via secondary means but are ultimately unsuccessful due to the inability that narratives, explanations, pictures, and videos provide of conveying all aspects of a military issue. Consequently, prototypes developed without actual experience led to purported solutions that often give rise to further problems, sometimes more detrimental than the original issue the company sought to remedy.

The scrutiny surrounding the adverse impact of civilian solutions is often attributed to a deficient demand-pull relationship, yet this overlooks the challenge of sticky information. According to Kendrick Kuo, when a military's security obligations increase at a faster pace than its resources, ingenuity may actually diminish the military's efficacy.[28] Consequently, the military may lose its expertise in conventional abilities and may fail to deliver novel capabilities, thereby exposing vulnerabilities that the enemy can exploit during times of war. While this argument is not wholly inaccurate, it fails to elucidate the shortcomings of futile innovations such as bat bombs or tank balls.

During World War II, the civilian sector endeavoured to tackle the obstacles encountered by military personnel on the battlefield through innovative means, but due to their lack of combat experience, these efforts proved ineffective. Among these initiatives was the proposition by Lytle Adams, a civilian surgeon, of attaching miniature explosive packs to Mexican free-tailed bats – bat bombs.[29] This concept, which gained traction because of President Franklin Delano Roosevelt's urgent backing (i.e., political exigency), proved disastrous when the bats inadvertently ignited an entire military facility. Another example is the invention of tank balls by civilian A.J. Richardson, which aimed to mitigate the challenges of navigating narrow terrain for tanks.[30] Regrettably, the design, resembling hamster balls with protruding guns, was poorly conceived, lacking any window ports and was prone to getting lodged in

the earth. Richardson failed to account for the criticality of a service member's situational awareness and lacked the requisite experience to understand the hostile terrain. These examples illustrate that sticky information can cause civilian R&D to expend substantial resources on frivolous undertakings that can lead to significant financial losses and the endangerment of military personnel. Nevertheless, the impact of these shortcomings is limited to issues that are deemed of operational and strategic significance, while null problems are left unaddressed.

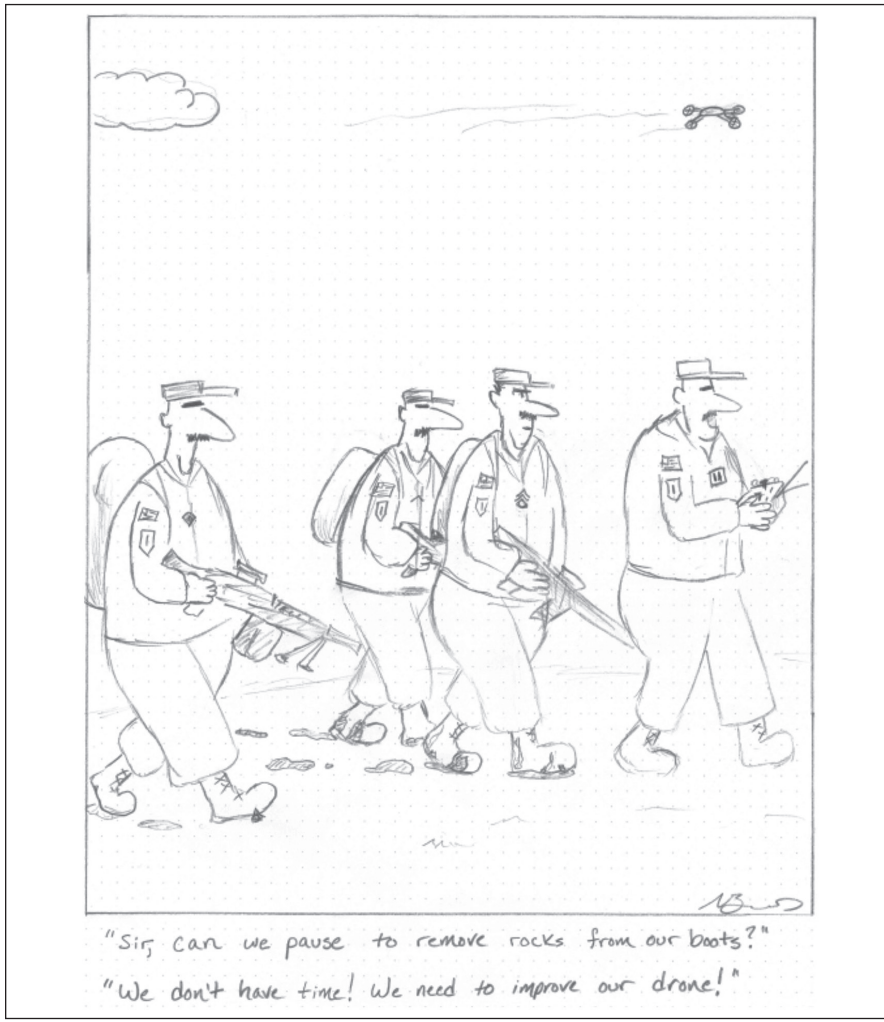


ILLUSTRATION 11.3 – *Null Problems*[31]

Most challenges faced by service members never rise to the attention of senior leaders due to a lack of perceived significance. As depicted in Illustration 11.3, a senior military leader may become overly fixated on enhancing their drone technology, that they fail to recognize the operational impact of not addressing their soldiers' injured feet. If such injuries are not remedied, it could result in their failure to arrive at their destination on time. And, if they do reach the battle in a timely manner, the soldiers will be combat ineffective which will ultimately lead to the Decisive Operation's failure. These issues at the tactical level often have cascading effects on operational and, in some cases, strategic outcomes. It is important to note that these issues are not just hypothetical, but are widespread throughout military units.

Service members at the tactical level frequently encounter impediments to their training, which can lead to injuries and even defeat in battle, yet these challenges are often ignored. For instance, cleaning up expended brass casings following firearms training at an outdoor range may appear to be a trivial matter that does not warrant investment of time and resources. This perspective is a mistake. The prevailing view is that the shooters themselves should pick up the brass because this is how it has always been done and it is, essentially, free. However, this issue has serious implications as it wastes valuable training time, requires significant manpower, exacerbates current injuries while causing new ones, and dampens morale. It is worth exploring how this seemingly innocuous activity can have such a significant impact.

The task of cleaning up expended brass casings reduces combat readiness, wastes millions of dollars in training time, exacerbates injuries that contribute to the non-deployable status of service members, and leads to increased medical costs incurred by the Department of Defense upon their transition out of the military. Within the military, the paramount resource for a service member is time. As such, despite the financial cost of deploying an entire unit to engage in the tedious task of cleaning a range for an hour, such activities seemingly hold little operational or strategic significance. The true operational costs of such cleanup activities manifest in the form of reduced training time and the hours spent in uncomfortable and ergonomically unsound positions, both of which ultimately undermine the combat effectiveness of service

members. In fact, noncombat musculoskeletal injuries (MSKIs) account for nearly sixty percent of soldiers' limited-duty status and sixty-five percent of soldiers who are non-deployable for medical reasons in the active component of the U.S. Army.[32]

Further, in a single year, these MSKIs resulted in over $434 million in direct patient care costs. Low back pain alone, which is enough to make a soldier combat ineffective, affects over thirty-four percent of U.S. Army service members.[33] The impact of these issues extends beyond immediate readiness concerns, as they can potentially affect long-term veteran disability and medical costs, as well as military recruitment, as over eighty percent of U.S. troops come from a military family.[34] Despite these pressing concerns, senior leaders often prioritize developing the next generation military platform or weapon system over addressing seemingly minor issues like brass cleanup. Thus, a demand-driven innovation development process that involves military members is necessary to drive solutions to such null problems.

The inclusion of service members in the innovation development process serves to alleviate the predicaments posed by the civilian supply-push market, while simultaneously elevating the advantages of an internal demand-pull innovation market. Inventions originating from civilian R&D are often of a supply-push process in which presented solutions contain but a mere conjecture regarding their appeal to defense contractors and consumers (i.e., military members) due to the sticky information.[35] Conversely, by engaging service members intimately in the development of an invention, the incubation process is strengthened, promoting a demand-pull process. The military's challenges provide an inchoate demand that establishes overarching objectives, which are then refined and made more specific and pertinent by service members.[36] Given their involvement, service members hold a critical role in the innovation process as they can sway the timing of implementation. Indeed, the psychological buy-in of the participants during the innovation process is particularly crucial.

The involvement of individuals in the process of innovation has a profound impact on their behavioural framework, leading to increased buy-in and

advocacy. One of the main reasons why a large percentage – forty to ninety percent – of new inventions fail is due to the differing biases held by consumers and producers.[37] These biases are in conflict, as consumers tend to evaluate new products based on the perceived value in comparison to products they already own, leading them to overvalue the losses associated with adopting the new invention by a factor of three.[38] Conversely, producers tend to overvalue the benefits of their new invention by a factor of three, since they view old products in relation to the new product they have created.[39] This discrepancy creates a significant mismatch, known as the "9x effect," where a producer's perceived benefits of an innovation are misaligned with a consumer's desires to maintain their current product at a ratio of nine to one.[40] However, this mismatch can be resolved by integrating consumers into the innovation process, since service members are the consumers of military innovations. By doing so, they also become the producers, mitigating the competing biases and eliminating the 9x effect. This increased buy-in and advocacy for the products produced enhances the likelihood of successful implementation and organizational evolution. Nonetheless, it is essential to note that such an institutionalized innovation hub cannot be established in the conventional force.

SOF AS THE MILITARY'S INNOVATORS

> *The modern military, like all bureaucracy, is an iron cage prone to crowding out innovation in an effort to promote efficiency and existing processes.*
>
> Benjamin Jensen, *Forging the Sword*[41]

The ethos of SOF fosters the essential organizational elements needed to disseminate novel ideas within their ranks, leading to their widespread adoption by conventional forces. Unlike their conventional counterparts, who prioritize predictability of lethality by adhering to the status quo, SOF benefits by constantly conceiving of novel ways to accomplish their missions due to their small size and clandestine nature of their operations. Thus, the SOF mindset of experimentation allows them to take risks without fear of jeopardizing their careers, a privilege not often afforded to conventional forces.

Additionally, SOF's consistent global deployment provides them with access to diverse terrain, enabling them to test new technologies and processes in environments that mirror potential future battlefields. These dynamics, along with a tolerance for unconventional thinking, engender a culture conducive to simplifying the organizational evolutionary mechanisms outlined above.

The significance of culture's role in organizational evolution cannot be overstated. As highlighted in the first section, the organizational culture not only helps in identifying problems, but also shapes the receptiveness towards innovative solutions aimed at addressing them.[42] SOF boast of a highly selective and rigorous assessment process that results in a community of resolute individuals with an experimental mindset, who are constantly striving for improvement.

This pursuit of excellence is a continuous process that extends throughout their careers, with special operators being afforded opportunities for education beyond the traditional military training programs. These diverse educational experiences provide a valuable platform for incubating fresh ideas and insights into the challenges that militaries face. Moreover, the relatively small size of special operations communities borne out of this selection process increases the chances of the effective dissemination of innovative ideas.

The comparatively diminutive size and autonomous nature of SOF communities facilitates the execution of creative ideas, given that they minimize the number of entities an innovation must navigate through. Innovative success is contingent upon the agreement of all stakeholders involved, and this "interdependence risk" intensifies as the number of parties increases.[43] This predicament becomes more complicated when there is a shift in leadership, loss of incentives, or fiscal constraints, all of which can put the project in jeopardy. For instance, consider an innovation adaptation that originates from a U.S. Army conventional infantry platoon, as depicted in Figure 11.4. Despite having a ninety percent probability of success at the inception of the ecosystem, the probability can plummet to below twenty percent by the time it reaches the Corps level. This variation in approval ratings can be influenced by such trivial factors as leadership attitudes, concerns about

career impacts, or even leadership turnover which results in a lack of buy-in for the project. These ratings can also be impacted by the need to safeguard the unit's budget or the inaccessibility to the additional requisite innovations it relies on. This may explain why an apparently sound investment of LED lights has yet to be implemented across the U.S. Navy.

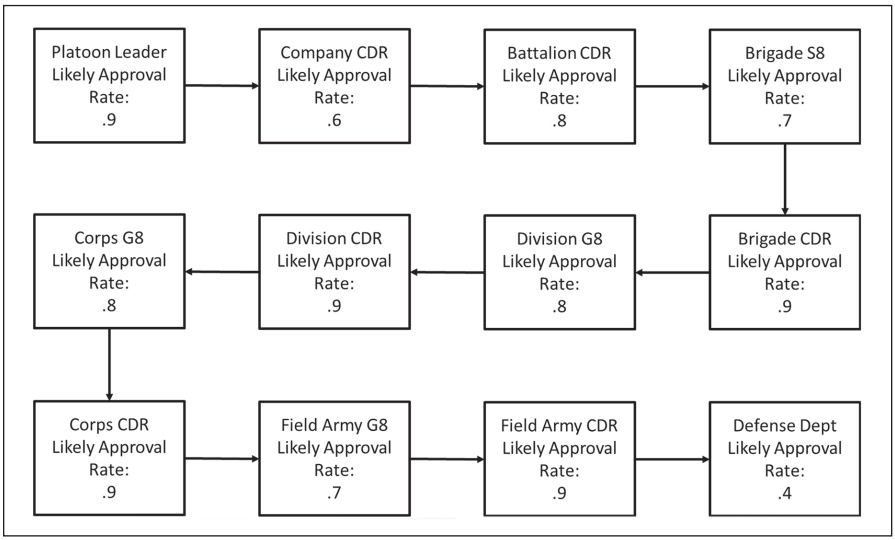


FIGURE 11.4 – Conventional Interdependence Risk[44]

The implementation of successful innovations by conventional forces is impeded by various factors, including attitudes, culture, ideology, and interdependence risks. In a case study entitled "How many Admirals does it take to change a light bulb? Organizational Innovation, Energy Efficiency, and the United States Navy's Battle Over LED lighting", Professor Nick Dew and his fellow researchers provide compelling evidence in support of the use of LED lights over conventional lighting systems, such as Compact Fluorescent Lighting (CFL) and incandescent bulbs.[45] Dew highlights the relative advantage associated with the longevity and significantly reduced energy usage of LED lights, as well as their potential to support the Navy's Great Green Fleet (GGF) initiative, enhance combat effectiveness, reduce maintenance burdens, and save lives within the Navy. Despite the considerable benefits of LED lighting, the U.S. Navy has been slow to adopt this technology, with less than ten percent of Navy ships transitioning to LED

lighting systems even after studying its advantages for over 15 years.[46] The researchers surmise that the principal impediment to the successful implementation of a well-conceived innovation lies in the insufficiency of endorsement garnered from the pertinent Navy stakeholders.[47] In light of these challenges, it is clear that attempts to systematize innovation within the conventional force are unlikely to succeed. Even if cultural barriers to diffusion were overcome and competing biases between consumers and producers eliminated, the complex and interdependent nature of the innovation ecosystem makes success unlikely. Therefore, it is more prudent to focus on smaller markets with lower interdependence risks, such as special operations forces.

SOF comprise several small markets that are capable of deploying novel ideas and solutions within their own ranks. This process produces the necessary proof-of-concept to introduce such innovations across the conventional force. Compared to their counterparts in the regular military, the chain of command within special operations is significantly streamlined, reducing the risk of excessive interdependence and stagnation. Once innovation adaptation occurs within the special operations community and consistently deployed, its relative advantage and effectiveness may become evident among all leadership levels in the conventional forces. Such exposure could generate a robust advocacy network within the regular military, facilitating diffusion. However, for innovation to flourish within SOF and diffuse into the regular army, the special operations community must fully comprehend and adjust the organizational evolutionary mechanisms detailed above and institute a formal incubation approach.

To facilitate the expeditious evolution of SOF entities prior to and during conflict, it is imperative to establish a formal organizational structure that emphasizes the entire innovation process. This approach necessitates the creation of an innovation doctrine by SOF to function as a strategic playbook that guides the organization from ideation to deployment.[48] Esteemed author Steve Blank stipulates that an innovation doctrine must emphasize the rapid deployment of new capabilities through an innovation pipeline.[49] Additionally, it must outline the processes that drive innovation efforts and define the role

of innovation leaders within the organization. Almost as a litmus test, the efficacy of an organization's design can be evaluated through the identification of individuals glorified as innovation heroes, which may signify a defective innovation doctrine.[50] Innovation should occur regularly and organically, and such celebrated heroism denotes an unusual occurrence that, conversely, a robust innovation doctrine would expect. In the absence of a unique SOF-specific innovation doctrine, the organization may not be able to adapt swiftly enough during conflict and consequently face defeat at the hands of their adversaries.

CONCLUSION

> *Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting.*
>
> 2018 U.S. National Defense Strategy[51]

When a special operations unit is asked about their role, the customary response is, "We are whatever our nation needs us to be." This response is commendable, yet its essence remains hollow unless the organization adheres to the comprehensive framework expounded in this chapter. Hence, understanding organizational evolution is of paramount importance for the purpose of adjusting to the ever-changing terrain, as well as for pioneering the transformation of the same, pre-conflict. In all likelihood, SOF are more likely to respond to variations in warfare rather than being the initiators of the said changes. However, the potential advantages of being the first mover in a disruptive innovation are monumental and strategically significant.

In the present landscape, disruptive innovations often hinge upon the widespread deployment of expendable materiel, such as swarm-capable drones for tactical operations. To effectively discern these developments and respond proactively necessitates the presence of an adaptive force that has successfully systematized innovation within its organizational framework. Notably, the civilian military-industrial complex exhibits limited interest for producing

cost-effective products on a large scale, amplifying the importance of possessing a streamlined innovation process within the military itself. Unlike their civilian counterparts, most military organizations inherently exhibit rigidity, characterized by bureaucratic structures that hinder adaptability. The capacity to dynamically adapt during conflicts, and ultimately undergo organizational evolution, equips specialized units with the ability to exploit their adversaries' inability to navigate the evolving environment, leading to their obsolescence. Consequently, fostering the mechanisms of organizational evolution that facilitate efficient adaptations to innovative advancements becomes an imperative pursuit in cultivating military units capable of agile adjustment both within and out of conflict scenarios.[52]

CHAPTER

12

BEYOND CONVENTIONAL WISDOM: SPECIAL OPERATIONS FORCES AND THE EVOLUTION OF RESISTANCE

MAJOR REUBEN MORRIS

The difficulty lies not so much in developing new ideas as in escaping from old ones.

John Maynard Keynes[1]

A chorus of voices have begun to call out the rising threat of violence in the modern day, both from within their borders and from amongst their threatening neighbours. The rise of domestic extremism, media disinformation, and acts of violence are a growing concern. While the end of the War on Terror appears to have passed with merely a whimper, states and their populations routinely hear that this has merely heralded a return to inter-state conflict and conventional large-scale combat operations. Liberal governments seek to build resilience in their populations but struggle amongst a cacophony of dissenting voices. While militaries seek to deter erstwhile threats, civilians are being prepared to resist if these options, and the defence that follows, fail. To succeed in this environment, Special Operations Force (SOF) professionals will need to be more than just adaptable, well-educated, and forward thinking. They must also be able to apply the lessons learned from a growing body of both military and academic writing to the challenges that they face in the future.

As a part of the "resistance profession," SOF must be prepared to both support and defeat resistance movements depending on the nature of the conflict and mission. This requirement has been transcribed in U.S. Army doctrine in the *Special Forces Unconventional Warfare* manual, *ATP 3-18.1*, which outlines the tactics of defeating these movements in detail.[2] In denied territory, unconventional warfare seeks to grow these movements to disrupt, coerce or enable regime change in opposing countries. In friendly or neutral countries, SOF may seek to suppress hostile movements through the use of Foreign Internal Defense (FID) or Counter-insurgency (COIN). This dichotomous relationship with resistance movements requires both a detailed understanding of how they come to exist, to grow, and either achieve their ends or are thwarted in the attempt. While military doctrine seeks to answer these questions from a practitioner's perspective, they are not the only ones to do so.

A growing body of research from scholars, activists, and researchers have sought to identify the conditions under which "weak" actors defeat their "stronger" adversaries. When viewed through an unconventional warfare or resistance lens, many authors highlight the advantages of employing indirect and opposing strategies from Arreguin-Toft's seminal work *How the Weak Win Wars*.[3] When these roles are reversed, however, these same insights apply to those adversaries who seek to overcome a conventional defence in an opposing country. Rather than directly targeting the strength of a well-prepared and determined military, they seek to take the indirect approach of targeting a vulnerable population. It is thus important to frame our conversation in terms of both offense and defence.

Initially it is important to clearly define some of the terms that will be explored throughout this chapter. The *NATO Comprehensive Defence Handbook* and the *Resistance Operating Concept* (ROC) will be cited throughout this work as foundational documents for our discussion. These documents define resilience as "the will and ability to withstand external pressures and influences and/or recover from the effects of those pressures or influences."[4] This capability can be developed both within an individual and in a society through civil preparedness and can be considered the first line of defence to an adversary. Resistance, then, is a "nation's organized, whole-of-society effort,

encompassing the full range of activities from nonviolent to violent, led by a legally established government (potentially exiled/displaced or shadow) to reestablish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power." Support to resistance (STR), adjusted from *ATP 3-18.1*, will be defined as support to foreign resistance actors that offers an alternative to a direct military intervention or formal political engagement in a conflict.[5]

Fundamentally, the challenge to SOF of building both resilience and resistance is one of growing a movement capable of opposing a hostile force and its overtures. While individual resilience is important, SOF's limited numbers suggest a greater focus on collective resilience and resistance, to achieve the greatest impact. Individual actors can be valuable to these objectives, but coordination and oversight will frequently be necessary to maximize their contribution to the national defence. Thus, by building more resilient organizations and societies, we lay the foundations for populations capable of resistance in the event of foreign interference, militarily or otherwise. With this mental framework in mind, we can begin to bridge the gap between the various military doctrines of our international SOF audience and the even more disparate fields of social movement theory (SMT), contentious politics, resource mobilization theory, and others.

National security experts Doowan Lee and Glenn Johnson contend that social movements, and by extension social movement theory, is a valuable contribution to SOF's understanding of the operational environment due to four trends in the contemporary operational environment.[6] First, states are increasingly working with or through non-state actors against other states, taking advantage of internal conflicts in other countries. Second, while fewer in number, internal contests are frequently becoming more protracted. Third, insurgent movements are increasingly more likely to win than before, as war becomes increasingly about controlling perceived legitimacy. Finally, non-military tactics such as civil resistance and unrest, are becoming more effective and pervasive. Therefore, they argue, SOF must "capitalize on, co-opt and incorporate existing opposition groups and networks" utilizing social movement theory as an approach.

While many explanations for movement success and failure have been proposed, they generally fall within three theoretical perspectives: political opportunity, cultural framing, and resource mobilization.[7] Cultural framing theories look at the beliefs and meanings of a social movement that enables them to inspire, legitimate, and mobilize their campaigns. This approach may be most valuable for determining the construction of information and influence operations, due to its ability to shape the perceived legitimacy of the movement and its opponents. Resource mobilization (RM) theory, conversely, looks at the materiel, human, organizational, cultural and moral resources that are necessary for a movement to succeed. For SOF professionals looking to build crisis response capabilities, joint capacity building, or network analysis, this approach has much to offer. Finally, political opportunity theories look at the variable opportunities afforded these challengers by the institutional structures, political systems, and individual actors.[8] Many SOF operators will find that these theories provide great insight into how and when their movements should execute the phasing of their operations for greatest success. Attempts will be made to incorporate each of these models in our discussion.

This chapter is structured in three parts. The first examines how SOF can contribute to enhancing resilience in friendly countries through the lens of recent research in the social sciences and especially social movement theory. The second section takes a similar approach to examining SOF's ability to enhance resistance, both within the context of friendly, neutral, and hostile countries. Finally, a quick examination of potential impacts of STR in the European theatre will be analyzed as a practical exercise in applying the previous theoretical discussion. While this discussion will only encompass a small portion of the valuable research being conducted in these fields, the hope is that it will expand the scope of study for SOF practitioners and thus better prepare them for a messy world.

ENHANCING RESILIENCE

To begin, we will explore how SOF can support resilience within a population against weaponized information and terrorist attacks. These malicious acts and actors are highlighted in the *Comprehensive Defence Handbook* as some

of the potential threats that a society must counter prior to open hostilities. While far from the full range of potential challenges, they can serve as a springboard for conversation and employment of the previously described theories. By executing a comprehensive risk assessment, SOF will be better placed to identify the most relevant and likely threats within their own area of operations.

Framing Theory shows how weaponized information, and more broadly disinformation, travels through a population farther, faster, and more broadly than the truth in nearly all categories of information, spreading fear, disgust, and surprise.[9] While governments will seek to build trust, cohesion, and motivation between themselves and their population, disinformation frequently seeks to tear this apart.[10] This negative framing of information attempts to shape an individual's understanding of their world and influence their behaviour to sow division, destabilize populations, and influence elections. Current research indicates that by simply altering the way they present a political issue or event, actors can substantially influence the support of individuals for individual policies.[11] Russian disinformation attempts in the 2014 Scottish referendum, the 2016 U.S. election, and the 2016 Brexit Referendum, show that these operations can shape political realities in even the most powerful countries.[12]

Russia and China have used this knowledge to their advantage in a myriad of ways. Drawing from its Soviet history of 'active measures,' Russia interweaves Tsarist, Soviet, and Russian narratives to belittle Ukraine and distract blame from Russia.[13] China, while slower to leverage this arena, has now taken to contrasting its anti-U.S. messaging with campaigns that seek to promote China as the responsible great power.[14] As authoritarian regimes and less scrupulous democracies look at the opportunities that this new strategy can provide, it will only become more appealing to interfere in the societies of those countries they compete with. Building upon societal divisions reduces the enemy's capacity and will to respond, especially in times of crisis. It takes advantage of perhaps implausible deniability to prevent escalation while "allowing space for myth and fear to take hold."[15] It can be used with great scope, canvassing vast swaths of an enemy's population, while costing comparatively little. Even

better, countries around the world frequently fail to respond in meaningful ways to these attacks, setting a frightening precedent.

Research indicates that the best way to combat this negative information is through the introduction of a competing narrative that minimize its effects.[16] Educating a population on the nature of misinformation, the narratives it employs, and its strategies through information literacy training has also been shown to effectively inoculate populations.[17] Currently, with the explosion of large language models (LLM) and narrow artificial intelligence (AI), the potential even exists to employ them as an early warning radar and alert human analysts of incoming disinformation.[18] Finally, the use of even small interagency organizations, like the Active Measures Working Group of the 1980s, can also be used to coordinate information sharing, expose disinformation and raise the costs of these hostile operations.[19] This particular group leveraged a wide range of expertise, obtained senior leader support, and scoped their purpose to establish small successes that grew over time.

SOF's historic strengths lend themselves well within this realm of influence and legitimacy. Christopher Maier, Acting Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), highlighted the importance of operators with detailed cultural knowledge and diverse backgrounds to address the broad range of modern threats in the information environment.[20] Military Information Support Operations (MISO) have made huge organizational strides to address many of these challenges. However, SOF needs to leverage and support other actors including Public Affairs, Information Operations (IO), State Department, and the Intelligence Community (IC) to maximize their effectiveness.

The Resource Mobilization model, conversely, can be an effective framework for the examination of terrorism, an arena where SOF admittedly has a well-established track record of success. Terrorism is a resource dependent activity that occurs under an externally constrained environment and is therefore inhibited by the ability to obtain men, money, and materiel.[21] Terrorists, therefore, frequently seek to use jujitsu politics to elicit an overreaction from the government which then mobilizes sympathy and support for their

movement.[22] While many analysts have concluded that these clandestine networks are fluid, adaptable and highly resilient to their opposing hierarchical states, this ignores the many vulnerabilities and inefficiencies of these threat networks.[23] The reality is that the average terrorist is inexperienced, relying on a dubious faith in their ultimate success to persist, but rarely do they survive the struggle.[24]

The decision to resort to terrorism, therefore, can also be viewed through grievances and perceived outcomes. Studies indicate that while higher levels of the rule of law can decrease domestic terrorism, democratization and any resulting political exclusion can drive these attacks up.[25] The openness of democracies provide these groups with the ability to operate freely, thereby lowering the costs of resorting to violence. Amongst democracies those with immature institutions, a deficient rule of law, and poor minority protections experience the highest levels of domestic terrorism.[26] A rational actor theory may thus view the question of whether to join these terrorist organizations from a more transactional perspective. Gordon McCormick, a professor at the Naval Postgraduate School, posits that the decision to join an insurgency is the sum of the perceived current and future rewards for joining after weighing and subtracting the costs.[27] Shifting this perceived calculus will correspondingly affect the ability of these organizations to attract and maintain members.

While this research may not advocate for a radical shift in policy for SOF, it does reinforce the decision to continue expanding their historical resilience building operations. MISO and IO can counter the narrative of perceived grievances and sway the mental calculus of potential recruits. The ongoing counter-violent extremist organizations (C-VEO) MISO operations against ISIS, Al-Shabaab and Boko Haram in Africa shows great promise in this regard.[28] Civil Affairs can serve to build government and institutional capacity, better integrating disenfranchised minorities and contributing to national protections. Special Forces can execute train, advise, and assist missions to increase partner capacity and reduce the freedom of manoeuvre for terrorist actors. By executing these tasks in coordination, SOF support to resilience is effective.

Political opportunity theory shows utility in explaining which networks are likely to exist in supported societies and when they are most likely to conduct operations. One study, for example, argued that countries with high levels of political freedom and civil liberties would see smaller revolutionary cells or lone wolf attacks, due to these societies' ability to limit large-scale mobilization.[29] These countries saw no noticeable coordination of terrorist attacks with elections, though disinformation during this period did escalate.[30] Countries characterized by middling levels of freedom, conversely, would see political partisans that employed violence and leveraged greater support networks, though without armed militias and/or concerted campaigns of violence. While disinformation around approaching elections remained high, terrorist attacks would also noticeably increase in frequency around elections. Terrorists, therefore, appear much more likely to strategically plan attacks during election periods in those democracies with less permissive electoral systems.[31]

ENHANCING RESISTANCE

If deterrence and defence should fail, SOF professionals must stand ready to assist a resistance movement within these newly occupied territories. Social movement theory can be a valuable tool to understand and shape how that resistance force is employed and to anticipate the ways that the incumbent force will seek to combat it. While STR covers a varied range of resistance scenarios, it will be used here as short-hand for both the application of SOF support to resistance in denied territory and prior to any incursion as envisioned by Comprehensive Defense and the ROC. Some of the most important decisions related to STR can draw from SMT to identify many factors, including: reasonable strategy outcomes for the campaign, type of tactics to employ, identification of the threshold of violence, and the means to maintain resistance support when confronted by hostile forces.

When deciding the objectives of the SOF STR, professionals should be aware of the most likely win-conditions for any potential operational objective. Studying U.S. STR from the 1940s to the present day, Army Special Forces Lieutenant Colonel (retired) Will Irwin found that those operations carried out under wartime conditions were nearly twice as likely to succeed as those

under peacetime conditions (63 per cent compared to 33 per cent).[32] Similarly, support to resistance was found to be most effective when conducted in direct support of a military campaign as opposed to an independent or main effort. He hypothesized that this was a result of the opposing regime's dilemma in simultaneously addressing both the internal and external threats to its power. Additionally, while most U.S. STR was conducted for the purpose of disruption, it was found to be most effective when conducted for coercive purposes. Sadly, although many movements will seek to overthrow their oppressive regime, this was only achieved in 29 per cent of the observed cases. While diverging interests between SOF and their supported resistance should be minimized, the research suggests that most movements' desired outcomes do not typically end in success.

The decision to employ a peaceful, violent, or mixed method approach to resistance is potentially the next most significant decision following desired effects. While many resistance movements will inherently preference one of these options based upon their unique cultural sensitivities, the circumstances leading to the resistance, and the resources available to them, careful consideration should be given. SOF professionals have been raised in the shadow of Mao's revolutionary warfare, advocating for a mix of mobile and guerrilla warfare, but this is far from the only approach.[33] While undoubtably successful in a number of cases, current research is looking to identify if it produces the best outcomes compared to the alternatives. While not specific to the expulsion of a foreign power, recent work by Erica Chenoweth, professor at the Harvard Kennedy School, suggests that nonviolent resistance in broader maximalist campaigns may be more successful in both their probability of success and the outcomes for long-term stability they produce.[34] These nonviolent campaigns lower the logistical and moral barrier to entry, increasing movement size, and enabling a more diverse and durable movement. This perspective, however, is actively debated, as new research looks at how a mixed-methods approach may increase government repression, but not effect success outcomes.[35]

Many scholars have attempted to document the range of strategies at a government's disposal for dealing with troublesome social movements. Governments generally seek to demobilize their opponents through violence

and intimidation, control of information, imprisonment or judicial action, and political division. In his 1987 book, *The State as Terrorist: The Policy of State Political Violence*, George A. Lopez discussed how violence is frequently the most overt form of repression.[36] Police brutality, political killings, disappearances, and torture are used to intimidate and silence opposition groups. Governments also shape the information space to change the public's perceptions of both dissidents and the government to increase support for these repressive measures.[37] Even the judicial arm of the government is weaponized, as courts frequently serve only to reinforce the supposed legitimacy of the state in relation to their rivals, ritualizing the punishment of dissidents to maintain loyalty.[38] To further spoil their opponents' cohesion, governments may also attempt to co-opt the movement by making concessions or by creating institutions that allow the movement to participate in the political process. However, these strategies can also backfire and lead to increased support for the movement, as well as international attention and condemnation.[39]

While SOF's ability to maintain support for the resistance movement will vary with the environment, their selected operational strategy, and a host of other factors, research suggests that some techniques lend themselves to success. As highlighted in the previous sections, backfire is the effect that turns a governments repression against itself in favour of both terrorists and resistance fighters. Study on Russian military operations in the North Caucasus from 2000 to 2008 identified Russian offensive operations in contested areas as being far less effective at containing violence than blocking operations, frequently leading to the amplification of violence in existing areas and the spillover of violence into new areas.[40] The use of strategic nonviolence has also been shown to benefit from this backfire effect and may even more effectively separate elites and state security forces who begin to pressure the regime to assume more conciliatory policies.[41] While violent campaigns appear more likely to receive external state support than their peaceful counterparts, care should be taken to ensure it does not alienate the resistance from the population.[42]

SOF STRENGTH TO RESISTANCE IN EUROPE

As a means to explore SOF's theoretical effects with the application of SMT it is essential to examine how social movements are already shaping perceptions in the European theatre. The intent is to show how the theories discussed in the previous sections could be applied in the current real-world environment. While argumentative, this section will seek to show that social movements are positively impacting their countries' respective leaders and their decisions not to escalate the war in Ukraine. SOF should read this section with a mind to applying the SMT already discussed and how this can positively contribute to similar coercive outcomes in the future.

BELARUS

Critical to understanding the Belarussian context is the deeply unfavourable position of its President Aleksandr Lukashenko, who has routinely called himself Europe's last dictator.[43] While President Vladimir Putin is largely still popular with many in his home country, Lukashenko does not enjoy the same domestic security following stolen elections in 2006, 2010, 2015 and 2020. Marked by electoral fraud, deemed unfair by the Organization for Security and Co-operation in Europe (OSCE), and rejected by the European Union (EU), the 2020 elections saw opposition movements mobilize a claimed half-million protestors following the disputed results.[44] Lukashenko's position, therefore, is far from stable, with the U.S. already supporting the Belarussian opposition there in their attempts at replacing Lukashenko through the ballot.[45]

These nonviolent opposition movements have the potential to hinder the basing and support of Russian military forces in Belarus. Recent Chatham House polling showed that 42 per cent of Belarussians are opposed to Russian forces stationed there, while 39 per cent believe they should be immediately withdrawn from the country.[46] Scholarly literature on Anti-Basing movements has historically focused on those opposing U.S. bases but highlights that even when foreign bases cannot be removed through protest, protestors can still be successful in hindering military operations there.[47] Journalist Amy Holmes discusses six means of successful obstruction including disrupting access, preventing expansion, forcing temporary shut-downs, and creating

supply shortages.[48] This action is separate from the widespread destruction of Belarussian railway which so deeply complicated the logistical challenges of Russian forces there at the start of the war.

Lukashenko's frequent and public attempts to mobilize domestic support for an active Belarussian military campaign in Ukraine have so far failed dismally as well.[49] Sviatlana Tsikhanouskaya, the leader of the opposition in the 2020 Presidential elections, has even used Lukashenko's support for the war to declare herself the national leader, publishing her Anti-War Manifest following the invasion.[50] As of June 2023, only 4 per cent of Belarussians surveyed would support Belarus taking an active part in the conflict on Russia's side.[51] Surprisingly, if Belarus did invade, only a fifth of respondents even believed that the Belarussian military would attempt to actively fight and only a quarter would oppose this refusal to fight. The active opposition of the Belarussian Anti-War Movement and Lukashenko's deeply unpopular leadership make the commitment of Belarus's 62,000 troops in Ukraine deeply unlikely.

RUSSIA

While President Putin is significantly more popular domestically than his erstwhile friend in Belarus, he is still forced to divert military resources, grapple with the limitations of a 'Special Military Operation' and seek to overcome strong anti-nuclear sentiment due to domestic considerations. These place very real constraints on the range of options that Putin views as available to him in Ukraine, helping to prevent escalation. While the extent of these impacts are challenging to measure, they will be highlighted here for clarity.

Following a spate of unsuccessful anti-war protests in Russia in which nearly 4,000 protestors were arrested, Putin was forced to return much of his premier pacification force, the Rosgvardiya, or Russian National Guard, to Russian territory.[52] With a fearful reputation for crushing internal dissent, Putin has deployed them heavily into the occupied areas of Ukraine to ensure the local populations are kept in line.[53] Hundreds of Rosgvardiya officers have already died in fighting there as they attempt to secure the notoriously overstretched

Russian logistical tails from Ukrainian partisans.[54] Regardless of whether Putin ultimately chooses accommodation or repression of his domestic dissent, the diversion of resources and attention from adventures abroad will serve to advance NATO and Ukrainian interests.

While several analysts feared that Russia would declare a formal war against Ukraine, enabling the mass mobilization of its population and the deployment of its conscripts into the warzone, Putin's fear of domestic repercussions oppose this. In late April 2023, when the Northern Front had collapsed and Russian advances largely stalled, many commentators assumed that Russia would use May 9th, Victory Day, to declare formal war to fill the crushing gaps in its military personnel.[55] While flush with tanks and missiles, the lack of dismounted infantry has frequently been viewed as the greatest factor in Russia's inability to effectively employ combined arms warfare, leading to the destruction of its unsupported armored forces. With so much to gain from a formal war declaration, the best theory as to why Putin refrains from this escalation is the increased domestic resistance that it would cause. As the U.S. has also learned from its past, the death of professional soldiers from a small segment of the population is easier to stomach without damaging support for the government's operations.

Perhaps most striking of all is the idea that Russian use of nuclear weapons is strongly opposed by its domestic population under nearly all circumstances and that this distaste can impact the decisions of Russia's elites. Published in July 2022, Professors Michal Smetana and Michal Onderco's ground-breaking research showed "a strong aversion to nuclear weapon use among Russian citizens, with an overwhelming majority preferring to face the prospect of military defeat than to agree with a nuclear 'de-escalatory' strike."[56] Over 70 per cent disapproved of a nuclear first use, even in the case of a limited use or demonstration scenario. While the Russian people and military may value the deterrence of their nuclear arsenal, they appear deeply opposed to its use. If Putin's successful shaping of domestic opinion on nuclear weapon use is a prerequisite for their employment, then he has much more work to do.

CONCLUSION

SOF professionals can meaningfully contribute to resilience and resistance across a wide range of operational scenarios. By understanding social movements and the wider social movement theory, academic research and findings on these topics can be applied that significantly enhance the likelihood of future success. Social movement theory can be used to help build societal resilience, prepare for a potential resistance, or even effectively coerce opposing governments and their leaders. Special Operations Forces and the wider JIIM force should therefore look to enhance their knowledge of the vibrant theoretical discussions occurring amongst academics, scholars and activists, which can greatly contribute to their existing doctrine and research. These ideas have significant potential to benefit SOF operations and deliverables in a world that increasingly looks to their leadership and expertise.

CHAPTER

13

PREPARING THE GRAY ZONE: EMERGING TECHNOLOGIES AND MARITIME IRREGULAR WARFARE THROUGH THE LENS OF THE UKRAINE WAR

CECILIA PANELLA AND
LIEUTENANT (NAVY) CHRISTOPHER MEARS

As Chief of Naval Operations Admiral (ADM) Michael Gilday stated in the *2021 Unmanned Campaign Framework,* "Unmanned Systems (UxS) have and will continue to play a key part in future Distributed Maritime Operations (DMO), and there is a clear need to field affordable, lethal, scalable, and connected capabilities.[1] This requirement is increasingly complicated by the proliferation of near-peer adversary "gray zone" operations, which require the U.S. Navy and our Allies and partners to deliver effects across the spectrum of conflict in all domains. Successful integration of UxS into the naval forces may allow the United States to successfully operate in a complex, denied, and amorphous environment. While totally seamless manned-unmanned teaming is a long-term strategic priority, the U.S. Navy must consider lowest barriers to entry within the Fleet and force for swift, low-cost, and agile integration in the short term. The enemy may not- and most likely will not- wait for the entire Fleet to be ready for conflict before testing the boundaries of the integrated deterrence concept.

Naval Special Warfare (NSW) has successfully utilized Unmanned Surface Vehicles (USVs) as well as Unmanned Aerial Vehicles (UAVs) in multiple mission sets. The increased development, experimentation, and operational agility that is ingrained in special warfare forces is a unique opportunity for the U.S. Navy to leverage in contested and denied environments. NSW may be the ideal test bed for successful, totally integrated man-machine teams in a hybrid fight. This chapter will begin with a review of available strategic guidance on unmanned and autonomous systems, focusing on the changing role for special operations forces (SOF) in a hybrid fight. To showcase how autonomous and unmanned systems might impact a high-end fight, this chapter will compare two types of autonomous systems: the unmanned surface vehicle (USV) and the unmanned aerial vehicle (UAV). These two platforms were selected due to their partial adoption into existing U.S. defense frameworks as well as their persistent presence in the Russo-Ukraine War.

Overall, the Russo-Ukraine War demonstrates the dangers that emerging technologies like unmanned and autonomous systems can pose on and off the battlefield. Based on examples of successful Ukrainian employment in the Black Sea, the Kerch Strait, and Russian sovereign territory, it is clear that unmanned and autonomous systems can easily erode the strategic advantage of larger, exquisite military capabilities and impose costs on otherwise dominant adversaries. More specifically, unmanned, and autonomous systems are easily integrated into an "irregular" or hybrid fight, thus suggesting that American SOF might be the optimal test bed for using such technologies in other conflicts. Furthermore, while the Russo-Ukraine War provides several compelling examples of effective tactical employment of unmanned systems, the true value proposition for NSW and the U.S. Department of Defense (DoD) writ large is the research, development, and acquisition of commercial off-the-shelf (COTS) technologies for hybrid problem sets. Simply put, *winning a hybrid fight means prioritizing hybrid preparation,* which this chapter defines as leveraging and integrating commercial industry best practices to build, test, and develop emerging technologies for use in all phases of competition.

STRATEGIC GUIDANCE FOR UNMANNED AND AUTONOMOUS SYSTEMS IN HYBRID ENVIRONMENTS

In order to understand how unmanned and autonomous systems might contribute to successfully waging and winning a hybrid fight, it is critical to explore existing available strategic guidance on the development and deployment of these emerging technologies. Overall, these documents suggest increasing priority on research, development, and integration of unmanned and autonomous systems into existing mission sets and conventional force designs. Furthermore, they all contextualize the role of emerging technologies as a tool that the United States can use to "re-center U.S. grand strategy in the 21st century around great power competition with Russia and China."[2] This is especially important for military planners who are seeking to use the strategic lessons of the Ukraine conflict for fights in other theatres. A review of accessible material on strategic development and employment of unmanned systems revealed that the similarities between the Ukraine invasion and a potential engagement in the Indo-Pacific region are similar but not truly analogous. If the DoD wants to leverage unmanned systems effectively, it must be willing to learn from the *process* and not the *prosecution* of the Ukraine conflict.

At the highest level, the priorities for development and deploying any emerging technologies for the purposes of national defense come from the National Security Strategy. In order for the United States to "modernize the joint force to be lethal, resilient, sustainable, survivable, agile, and responsive, prioritizing operational concepts and updated warfighting capabilities," the DoD must be willing to invest in emerging technologies like "applications in the cyber and space domains, missile defeat capabilities, trusted artificial intelligence, and quantum systems, while deploying new capabilities to the battlefield in a timely manner."[3] By prioritizing a modern joint force capable of developing and employing emerging technologies, the National Security Strategy is sending a key message not just to the DoD but also to the commercial sector. The Defense Industrial base is explicitly called out as "critical" towards "innovate[ing] and creatively design[ing] solutions" for the future fight.[4] The implication is that a separation between commercial and

public defense interests can no longer be tolerated when America is facing competition or conflict with a near-peer adversary. The U.S. must be willing to increase the size and scope of its innovative capacity and hybridize its research, development, and deployment methods to include commercial partners if it wants to be able to effectively field emerging technologies like unmanned and autonomous systems.

This requirement is more clearly articulated in the National Defense Strategy that links the proliferation of emerging technologies with increased gray zone activities that fall below the threshold of war. Specifically, "new applications of artificial intelligence, quantum science, autonomy, biotechnology, and space technologies have the potential not just to change kinetic conflict, but also to disrupt day-to-day U.S. supply chain and logistics operations."[5] This instability is exacerbated by the fact that legacy systems for "force development, design, and business management" are "too slow and too focused on acquiring systems not designed to address the most critical challenge we now face."[6] This assessment is significant for two reasons. First, it suggests that the United States is not currently organized to effect change or win a war with a near-peer competitor. Second, the implications of this antiquated organizational model for research, development, and deployment of emerging technologies are catastrophic not just for the DoD, but for the U.S. writ large. Despite these massive consequences, the responsibility for innovating has historically fallen upon operational units. These two strategic documents seek to centralize the innovation arm of the defense industrial complex to better compete in the gray zone, but they do not address this mismatch of responsibilities and ramifications.

When invention outpaces adoption, unclear normative boundaries are increasingly blurred, thus putting pressure on the services if not individual commands to identify, leverage, and employ new technologies without the strategic support of higher headquarters. This situation can be both a danger and an opportunity. If left unchecked, it is possible that the gap between innovation and adoption could broaden, making it harder for the DoD to effectively provide the services with the capabilities they need in order to preserve the safety and security of the nation. In contrast, informal delegation

of innovation to the smallest and most agile units may imply an inevitable comparative advantage for U.S. Special Operations, and Naval Special Warfare (NSW) in particular. As Dr. Leo Blanken, Justin Davis, and Phil Swintek state in their article "Special Operations as an Innovation Laboratory," "using special operations forces as (an innovation) laboratory could leverage the military community most comfortable with the rapidity, cognitive flexibility, and risk tolerance necessary for prototyping."[7]

This comfort with, and perhaps affinity for, change and adaptation make implementing emerging technologies in complex environments a natural fit for special operations. The *2021 Unmanned Campaign Plan* emphasizes this need for unmanned and autonomous systems to "increase lethality, capacity, survivability, operational tempo, deterrence, and operational readiness" and to "ability to adapt interactively to the dynamic maritime environment."[8] The *Framework* goes on to highlight the growing need for autonomous systems in unpredictable, complex, and denied or austere environments. This reality is another point of alignment with the historical functionality of special operations forces, as Dr. Eliot Cohen argues that these units can "try out new doctrines, test their validity, and then spread them to the rest of the force."[9] The flexibility of hybrid operations also encourages this friendship between operator and machine, as the *Unmanned Campaign Framework* demands that the U.S. Naval Forces "incentivize rapid incremental development and testing cycles for unmanned systems" since the Department "cannot continue with a traditional force structure in the face of new warfighting demands" like strategic competition and hybrid warfare.[10]

This call to action is echoed in the *National Defense Science and Technology Strategy,* which calls upon the DoD to "accelerate the process of turning ideas into capabilities by creating new pathways to rapidly experiment with asymmetric capabilities and deliver new technologies at scale."[11] In fact, the Strategy lists Trusted Artificial Intelligence (AI) and Autonomy as one of its critical technology areas where the U.S. should seek to achieve "an enduring advantage" despite "theft, diversion, and exploitation by our strategic competitors."[12] This threat is another example of the necessity of hybrid preparation, and the DoD must be willing to leverage legal, social,

and economic means to support national security objectives surrounding these critical technologies. U.S. Special Operations Command (SOCOM)'s SOFWERX is explicitly called out in this Strategy as paving the way for this hybrid preparation by "actively engaging [with] commercial companies to identify opportunities to leverage their dual-use technologies for military applications."[13] In fact, SOFWERX has increased the number of proposals from emerging technology companies going to SOCOM for review, decreasing the time it takes to award funding to those companies to bring their technology to a warfighter, and awarded approximately $61 million USD to Small Business Innovation Research (SBIR) designed to increase resiliency and adaptability in the defense acquisition process for special operations.[14]

The implications of this hybrid preparation are significant in three ways. First, each of these documents acknowledges the changing strategic landscape and the need for the U.S. to be ready and willing to leverage emerging technologies to maintain strategic advantage. Second, they also imply a leadership role for special operations forces in developing, testing, and employing these technologies due to their familiarity with complex environments and their higher risk tolerance. Finally, these documents acknowledge that hybrid warfare and gray zone operations are not new developments in and of themselves, but the consequences of operating in these environments may exponentially increase in magnitude and uncertainty given the proliferation of new and emerging technologies. What these documents gesticulate towards but do not outright say, though, is that hybrid warfare is not just conflict, but a competitive process. While traditional definitions of "hybrid" warfare use the term to "describe the increasing complexity of conflict that will require a highly adaptable and resilient response from U.S. forces," up to and including kinetic effects, the reality is that most of hybrid warfare as it pertains to emerging technologies takes place below the threshold of conflict in the research, development, testing, and evaluation arena.[15]

For Naval Special Warfare, this delineation is a critical warfighting enabler. The naturally agile force design and "powerful, flexible tools that can be integrated across the full range of conflict and operations, as part of whole-of-government efforts, and with partner nations and U.S. allies to deter

(…)" near-peer adversaries make NSW an ideal testbed and first adopter for emerging technologies like autonomy and unmanned systems that have an outsized role to play in gray zone operations.[16] In the maritime environment, hybrid preparation and warfare provide operators with increased optionality to accomplish their mission. A 2016 article by Admiral (retired) James Stavridis highlights four benefits of maritime hybrid warfare: limited attribution, increased speed and likelihood of surprise, more positive control of mission tempo, and comparatively low cost of execution.[17] For special operations, these tenets are baked into their force structure and already integral to their mission planning, thus making hybrid warfare a natural fit for these elite units. Stavridis clarifies that these benefits require the U.S. DoD to "develop tactical and technological counters," which he states can most effectively be accomplished by "linking international partners, the interagency and intelligence communities, and even private-sector elements."[18]

This approach is very much in line with the traditional "deliberate blurring and blending" of adversary means and methods that Dr. Frank Hoffman marks as integral to hybrid warfare.[19] While "blurring" is usually understood as creating a more expansive, strategically gray area where adversaries can engage in conflict, the rise of malign information operations and cyber tactics can sharpen and increase the consequences of successful hybrid warfare activities by an order of magnitude at extremely low cost. As U.S. Army Lieutenant General Karen H. Gibson, the Deputy Director of National Intelligence for National Security Partnerships points out, hybrid warfare is now marked by "the unprecedented ability to use information as an element of warfare with much greater volume, velocity, breadth and depth and precision than previously possible," thus possibly eroding trust between the defense sector, partners and allies, and the private sector.[20] This possible outcome implies that hybrid warfare can have an isolating or strategically chilling effect. Therefore, it is insufficient to say that the SOF's ability to employ hybrid warfare relies upon its operational capacity to deal with complex and complicated environments – rather, a successful employment of hybrid warfare for NSW also requires the ability to operate in austere and denied "zero trust" environments *and* the endogenous ability to build connective tissue between relevant stakeholders.

NAVAL SPECIAL WARFARE AND AUTONOMOUS SYSTEMS: EMERGING TECHNOLOGY AS A FORCE MULTIPLIER

Sufficiently preparing to operate in evolving hybrid environments will require U.S. special operations to fully embrace Admiral Stavridis' call to integrate the force with partners, allies, and key private industry stakeholders to achieve strategic advantage. Naval Special Warfare is uniquely positioned to accomplish this task, and even more strategically inclined to adopt emerging technologies like unmanned and autonomous systems. While SOF has always historically been the test bed for new doctrine, tactics, and equipment, unmanned and autonomous systems did not become battlefield ubiquitous until the Global War on Terror (GWOT). Partners, allies, and the U.S. leveraged unmanned and autonomous systems for kinetic strikes, intelligence, surveillance, and reconnaissance, and electronic collection against their adversaries while greatly reducing risk-to-force and exponentially increasing strategic effects. The world stood by and took notes.

Since then, autonomy has been transformational both on and off the battlefield, as the DoD set aside "about $7.5 billion in fiscal year 2021 for a variety of robotic platforms and related technologies" for both the services and for USSOCOM.[21] The naval services have been the largest proponent of research and development for autonomous and robotic systems, "with $1.76 billion USD" allocated towards the project.[22] The ability of autonomous systems to "reduce soldier burden, improve the efficiency of operations and increase situational awareness" make them all the more palatable for SOF, who rely on lean and agile teams who operate in complex and denied environments.[23] This expenditure is supported by a more recent push for attritable autonomous systems that operators can build, use, and lose without incurring risk-to-force – the sturdy paper plate and picnic silverware set of kinetic effects. As Christian Trotti, the Assistant Director of *Forward Defense* at the Atlantic Council's Scowcroft Center for Strategy and Security points out, these new technologies "can be the crux of a new US force posture" so long as operators apply "new applications and concepts for using those technologies" and do not rely on the tech itself as an ameliorator for all tactical woes.[24]

USSOCOM is particularly interested in avoiding the siren song of a single piece of technology. Culturally, the smaller, more insular, and agile SOF teams prioritize integration and operators over a single platform. Operationally, this means having "underlying autonomy software (working) the same on everything from a 3-D printer to a $10,000 drone."[25] It also means that autonomous systems and their underlying architectures must be baseline accessible to operators on the ground as opposed to more exquisite legacy systems with dedicated teams operating next to but not *truly with* the operational force. As a result, it may behoove the U.S. military to focus its development and integration of autonomous systems on USSOCOM, which already has a force geared towards distributed battlefield innovation. As Dr. Leo Blanken, Dr. Jason Lepore, and Cecilia Panella point out, organizations like USSOCOM that both incentivize innovation and scale and protect emerging solutions are more likely to be able to detect strategic gaps and have personnel who "empowered to engage in efforts to ideate, prototype, and collaborate around innovative solutions at the lowest level."[26] This is most evident in Naval Special Warfare, "given its unique mission set and smaller, more mature force, it is able to develop and field capabilities on significantly faster timelines than the services and traditional forces."[27]

Conceptualizing autonomous systems as accessible and flexible battlefield innovations not only speaks to NSW's operational strengths, it also more accurately reflects modern kinetic operations. This observation is most evident in the Russo-Ukraine war, where the Ukrainians have leveraged unmanned and autonomous systems to gain relative advantage against a perceivably superior opponent both on the battlefield and in research and development. The Deputy Prime Minister of Ukraine, Mykhailo Fedorov, points out the necessary link between operational and preparational agility, stating that "in order to win in this fast-paced technological war, the government needs to think and act as a technology company, to be agile, to make fast decisions and to move faster."[28] With this in mind, the Ukrainians have been using small expendable drones across multiple domains to gain advantage on the battlefield. Usually fashioned with zip ties, tape, and some homemade solders or welds, these small, cheap, and attritable drones allow small elements and Ukrainian SOF to conduct ISR, pre-assault fires, and harassing attacks on Russian elements.

In the air, these UAVs are usually fashioned with a control arm to release small munitions on Russian combatants. Moreover, they are exceptionally cost-effective for a small military taking on a global power. Unmanned systems are also expensive for the Russian Federation to shoot down, and the benefits of doing so are slim to none. As Philip Ross states in his article "Budget Drones in Ukraine Are Redefining Warfare," "For the most part, the price is right: China's DJI Mavic 3, used by both Russia and Ukraine for surveillance and for delivering bombs, goes for around U.S. $2,000. You can get 55,000 of them for the price of a single F-35 (Joint Strike Fighter). Also, they are much easier to maintain: When they break, you throw them out, and there's no pilot to be paraded through the streets of the enemy capital."[29]

The proliferation of robotics and autonomous systems on the battlefield is not limited to unmanned aerial vehicles. Ukrainians have also recently stood up the world's first specialized explosive naval drone unit.[30] This unit and its portfolio of USVs have held Russian vessels at risk and may have been able to conduct kinetic strikes on key Russian ground lines of communication. As of August 2023, Ukrainian sea drones were able to attack at least one major naval base in Russia, leaving a damaged Russian warship in the Black Sea.[31] Across both domains, these use cases speak to the evolving landscape of future warfare. The fact that the "Ukrainian Navy has a unit dedicated to a mode of warfare which essentially didn't exist 1.5 years ago" showcases how quickly and unpredictably emerging technologies can change an operational environment.[32] In the next two sections, the authors will explore two use cases of unmanned and autonomous systems within the context of the Russo-Ukraine War: USVs for mine warfare and sea denial and Unmanned Aerial Vehicles for ISR in Ukraine. Overall, these cases will show how these emerging technologies, and the hybrid environment they exist within, have both complicated and democratized the battlefield. The authors suggest that hybridizing preparation for warfare will allow naval special forces to harness the processes of rapid innovation and the employment of novel technologies that will be paramount in the new age of conflict.

UNMANNED SURFACE VEHICLES: TWO IF BY SEA

American NSW forces have been developing and evaluating unmanned surface vehicles for years. These low-profile, low-signature craft are designed to extend the operational reach of NSW while minimizing risk-to-force in complex and denied environments. Even as early as 2013, a RAND Report recognized the benefits of unmanned surface vehicles for defense purposes, stating that "USVs have greater potential payload capacity and endurance than comparably sized unmanned systems in other domains."[33] More importantly, the report notes the high level of interoperability that USVs can offer the U.S. Navy, highlighting them as "critical nodes for cross-domain networks" that can "overcome(e) adversaries' anti-access and area-denial measures."[34] By using unmanned surface vehicles in complex and denied environments, U.S. NSW can apply lessons from recent Ukrainian engagements in the Black Sea to assist in further integrating emerging technologies into existing operational constructs.

In 2007, the Department of the Navy released its first Unmanned Surface Vehicle Master Plan, as chartered by the Program Executive Officer for Littoral and Mine Warfare. Not only does this document prioritize aligning research, development, doctrinal and acquisition best practices to make these emergent platforms more available to warfighters, it also explicitly calls out special operations forces as one of the more prolific users of USVs. More specifically, the report lauds NSW's inherent training, doctrinal, and operational flexibility, as "U.S. SOF are legendarily innovative in adapting the systems and equipment at hand to fit emergent mission needs and environment. The modularity inherent in USVs can be a great asset in support mission innovation."[35]

While unmanned surface vehicles are now the purview of the Program Executive Office for Unmanned and Small Combatants, reliance on NSW's inherent agility for adopting these platforms remains at an all-time high. Moreover, the "Big Navy" has started to use NSW's innovation practices of quick, iterative technology testing and operational evaluation for unmanned systems integration across the fleet. As Chief of Naval Operations (CNO)

Admiral Gilday pointed out, "we are learning so fast and fielding these capabilities out to the fleet, or potentially fielding them quickly inside the [Future Years Defense Plan], we may be able to close capability gaps with small expendable unmanned [vehicles] off of any platform."[36] This broader application of SOF's "fast learning" concept has two key implications. First, it recements the concept of naval SOF as the service's preferred test bed for new and emerging technologies, especially when the service is considering using those technologies in the immediate future. In 2022, "the Navy (rethought) its planned portfolio of unmanned surface vehicles following testing of a variety of USVs in the Middle East," a feat that ADM Gilday says was only possible due to close alignment of research, testing, and fielding priorities.[37] In fact, "Task Force 59's success using small USVs to sense the battlespace and create a common operating picture for the U.S. Navy and its partners "has changed [ADM Gilday's] thinking on the direction of unmanned."[38]

Second, increasing agility in naval technology development, evaluation, and deployment is clearly connected to the ability of the services to integrate best practices from COTS products and as a result, these unmanned surface craft are explicitly designed to have an impact in a hybrid operating environment. Platforms like the *Mariner,* a recent deployment of the Navy's Ghost Fleet Overlord vessels, offer the Navy unparalleled abilities to test autonomous systems in the field. The *Mariner* features "wide array of commercial systems – like sensors, satellite links, radars and communications suites – that the Navy is experimenting with across its fleet of USVs," a capability that the U.S. Navy's Program Maritime Systems Unmanned Office states is a huge fleet force multiplier for deployed carrier strike groups.[39] Specifically, "we can take two of our USVs and go out and do multi-vessel [operations] and control and not necessarily have to take a [Destroyer] DDG off of actual fleet operations to go do that," thus expanding the operational control that U.S. and allied or partnered forces might have in a complex environment.[40] By diversifying the number, type, and scope of platforms employed for a particular mission, the U.S. Navy may be able to operate more effectively in competitive escalation scenarios with a near-peer competitor. This increases optionality for the fleet while reducing risk-to-force in a gray zone.

These hybrid options should not overshadow the very real kinetic implications of unmanned surface vehicles. Ukrainian forces have used small, unmanned craft to gain access to larger Russian naval fleet emplacements, in many cases inflicting disproportionate damage than their low profiles might otherwise indicate. These examples are significant for two reasons. First, they showcase how unmanned craft can level the battlefield, enabling smaller forces to have outsized operational impacts. Second, they emphasize how the emerging technologies like unmanned vehicles have become ubiquitous with modern warfare, implying that future combatants may need to integrate these platforms into their operational plans if they wish for any kind of success.

For the Ukrainian military, punching above their weight class is an operational imperative. Early reports after the Russian invasion clearly highlight Ukrainian ingenuity while also emphasizing the two previously mentioned maxims of economy of force and ease of COTS integration. Just seven months after the February invasion, a small, unmanned Ukrainian surface vessel washed up on the beach near Sevastopol, a Russian naval stronghold in Crimea. The craft is described as "small but purposeful," with a remarkably diverse sensor suite of "a mast mounted camera and forward looking infrared (FLIR) type device. This equipment is likely the main sensor for steering and situational awareness. There is a flat antenna behind the camera, possibly for navigation and/or communication. There is a smaller camera or sensor at the bow which appears to be fixed forward. There are two forward facing sensors in the bow."[41]

The USV is assumed to have been designed for ramming a target and exploding on impact, a feature that author H.I. Sutton describes as similar to remote-controlled USVs used by Iran-backed Houthis in the Middle East.[42] The comparison between this vehicle and those used near Iran speaks to the transient effect of hybrid warfare. Just as the Houthis sought to use USVs to expand their operational reach and put themselves on par with a larger, legitimate military, the Ukrainians are coopting techniques typically used by insurgencies to impose cost on the Russian military. This methodology implies that modern warfare can simultaneously be hybrid and conventional.

These small unmanned surface vehicles also have a deterrent effect. Ships not targeted by the exploding sea drones have huddled back in Sevastopol, reflecting "recent Russian Navy trends to keep their warships in port" after the discovery of these new platforms.[43] Furthermore, an analysis of the beached drone revealed that the parts were made by Sea-Doo, a maritime "company (that) sells its products worldwide, aimed mostly at the civilian market. This means that a Sea-Doo would be relatively easy to source."[44] Not only are these small boats deterring the tactically superior Russian fleet, but they are also able to shape Russian maritime behaviours for a fraction of the cost in terms of time, manpower, and money. To put this into perspective, the October 2022 USV strikes to Sevastopol "scored direct hits on *Admiral Makarov*, the fleet's flagship, and two other vessels, damaging all three. That was followed on November 18th by a big explosion at a Russian oil terminal in Novorossiysk, also reported to have been the work of the same type of naval drones."[45] The *Admiral Makarov* alone is estimated to cost approximately one billion U.S. dollars.[46] A brand new, 2024 Sea-Doo jet ski costs approximately seven thousand U.S. dollars, meaning that if the Ukrainians were purchasing name brand materials at full retail cost, they could purchase nearly 143,000 jet skis. The deterrent and kinetic benefits far outweigh the attritable costs of losing a single unmanned surface vehicle in this invasion.

Finally, unmanned surface vehicles are more dangerous and more widely applicable than their aerial or subsurface counterparts. As Dr. Scott Savitz states, USVs can conduct waterline strikes with larger payloads, longer ranges, and more diverse ability to re-task the boat once it has left positive control of the operator.[47] In Ukraine, this has dramatically increased the lethality of small, irregular maritime units like the new 385th Separate Brigade for "Special-Purpose Naval Unmanned Systems" and shaped Russian behaviour to prevent their exercise of larger, more tactically-destructive naval platforms.[48] When combined, these features strongly suggest that USVs will soon become synonymous with maritime irregular warfare. Lower signal profiles, higher payloads, increased operator standoff, and natural applications with existing U.S. NSW mission sets all demonstrate the utility, if not necessity, of maritime drones on the battlefield. While one robotic boat may not be decisive in a high-end fight, "USVs complement the other (options), contributing to attrition

of adversary forces and disruption of plans" and increasing allied abilities to manipulate risk and increase optionality when operating in complex and denied environments.[49]

When taken together, Ukrainian operational use cases and recent U.S. Navy testing for USVs demonstrate a clear value proposition for robotic and autonomous systems in the maritime domain in both competition and conflict. While it is important to note that the Ukraine War is not a perfect analogy for the operational constructs that most concern the United States and her partners and allies, this is the example that both friendly and adversary militaries are learning from in order to shape their forces for the next fight. It is possible that incorporating these platforms into special operations forces is an absolute necessity for operational superiority and integrating them with the larger conventional fleet forces may prove strategically decisive in both competition and conflict. Simply put, employing emerging technologies can affect not just the units in the gray zone, but also the enabling support commands, policies, doctrine, training, and military strategy that informs the global order.

UNMANNED AERIAL VEHICLES: EYES IN THE SKY

The U.S. Navy has been using unmanned aerial vehicles in some form since approximately 1917, where operators experimented with remote control aircraft. Later iterations surfaced during the Second World War, where the Curtiss N2C-2 "shadowed" other manned aircraft to expand naval force projection.[50] Even at this time, naval strategists were considering using UAVs as multidomain tools for kinetic strikes, ISR, and general force augmentation. "Project Option" focused on integrating these UAVs with the manned fleet, but had limited success due to technical constraints on drone span of control, flight times, and fuel capacity.[51] In fact, the major success of this early program was not a drone at all but rather, Project Option is said to have been the birthplace of the guided missile.[52] Despite these unintended consequences, unmanned aerial vehicles continued to sophisticate and proliferate and have since been used in every major conflict, particularly by special operations forces. In 2011, Director of Technical Special Reconnaissance and NSW Command

(WARCOM), Commander Robert Witzleb, highlighted the depth and scope of UAV integration with NSW forces, stating that "I can think of nowhere where SEALs are operating today where they are devoid of UAS support."[53]

While unmanned surface vehicles are more recent additions to the battlefield, the longstanding relationship between naval special operators and UAV technologies has cultivated a sense of trust in the technology as well as willingness to experiment. Exercises like Rim of The Pacific (RIMPAC) 2022 heavily featured unmanned systems across multiple domains, with UAVs key to "improving command and control within kill chains."[54] Central to this effort was the SeaGuardian, a UAV that Navy Captain Dan Brown, the head of experimentation at 3rd Fleet, says is designed with "multi-intelligence payloads for maritime domain awareness and for anti-submarine warfare operations. Its payload includes a synthetic-aperture radar/inverse synthetic-aperture radar, electro-optical/infrared sensors, communications intelligence and electronic intelligence tools, and sensors to look for submarines and then share that information via a Link 16 connection to the rest of the fleet."[55]

A payload this modular and this sophisticated is significant for two reasons. First, it speaks to the level of technical complexity that UAVs have already been able to integrate with major U.S. Navy fleet exercises and on the battlefield. Second, the proliferation of these systems and their payloads has the capacity to democratize the battlefield. Bryan Clark from the Hudson Institute substantiates this, suggesting that "unmanned systems provide a way for less-advanced militaries to remain more interoperable with U.S. forces because the unmanned systems can incorporate new technologies more quickly than manned platforms and be common between partners."[56]

This leveling of the battlefield and ease of integration with smaller, agile forces make UAVs the technological partner of choice not only for special operations forces, but also for traditionally "weaker" forces like the Ukrainian military. Since the beginning of the Russian invasion, Ukrainian forces have used UAVs as ways to augment friendly ground forces, conduct ISR, aid in tactical support to direct assaults, provide logistics and communications, and aid in psychological warfare. Recent use cases of these airborne drones

showcase the value proposition that smaller, commercially-available systems bring to hybrid and conventional battle spaces.

The primary function of UAVs in Ukraine in the conflict has been ISR missions. While the Russian Federation has its own satellite systems (GLONASS) to leverage for surveillance and reconnaissance, Ukraine has no such endogenous constellations. In contrast to the highly compartmentalized Russian approach to ISR, the Ukrainians have been able to leverage U.S. space assets, DoD small UAVs, and various commercial drones to scout troop movements, fortifications, and equipment (Figure 13.1).[57] These platforms are usually equipped with high-definition cameras and other sensors that provide real-time data back to command-and-control elements on the ground to "execute surprisingly effective tactical-range strikes and, even more lethally, to acquire targets for artillery fire of unprecedented precision and speed."[58]

ADDITIONAL REPORTED PRIVATE/COMMERCIAL UAV TRANSFERS TO UKRAINE JUNE-SEPTEMBER 2022				
COMPANY/DONOR	**TYPE**	**ROLE**	**VALUE***	**NUMBER COMMITTED**
AeroVironment (via Drone Aid Ukraine)	Quantix Mapper	Search & rescue support		2 for 'situational assessment'
AeroVironment	Switchblade-600	Heavy loitering munition	$2.2 million	Hundreds reportedly committed
Aeryeon Labs (via Veteran's Aid Ukraine)	SkyRanger R60	ISR quadcopter		3
AEVEX Aerospace	Phoenix Ghost	Light loitering munition		701
Anonymous Czech co. (crowdfunded)	Bivoj	Catapult-launch ISR drone		3 UAS donated (each w/3 drones)
Autel Robotics (via Eyes on Ukraine and XDynamics)	EVO II v2, EVO Llite+	ISR quadcopter, 30mm grenade	XDynamics donation worth $35,000	10 EVO 2 Pro, 27 EVO Lite (EoU), 10 EVO 2 v2 (Xydnamics)
Autel (via Come Back Alive Foundation)	EVO Lite +, EVO 2 640T Dual, EVO Nano	ISR, 264x with thermal	$2 million	300 Evo Lite+, 350 EVO 2 640T Dual, out of 4,000 quadcopters
Baykar (Turkey)	Mini-Bayraktar	ISR Mini UAV		24 donated
Baykar (Lithuanian, Ukrainian citizens)	TB2 Bayraktar	MALE UCAV	$20 million (UKR)	4 crowdfunded in Ukraine, Poland
Boeing-Insitu (U.S.)	ScanEagle	ISR	~$800,000 each	15 donated
DefendTex (Australia)	D40	Light loitering munition		300
Draganfly–Canada (via Drone Aid Ukraine)	Commander 2 UAV + 1x other	Mine detection		2 donated
Dronesvision (via Poland)	Revolver 860	Heavy attack quadcopter		Likely limited number
E-flite (via Drone Aid Ukraine)	Opterra	Flying wing FPV drone		11
Milrem (Estonia)	TheMIS	Casualty evacuation UGV		1 donated to Ukrainian charity
Parrot (via Japan, Quadra)	Anafi Thermal	Thermal ISR quadcopter		30 Japan + 6 Quadra + 54 humanitarian
Proxy Dynamics UAS (via UK, Norway)	Black Hornet Nano	ISR microdrone	$8.7 million	850 donated
QinetiQ	TALON	De-mining UGV		10 purchased
THREOD Systems (Lithuania)	EOS C VTOL "Magila"	Hybrid ISR minidrone		5 bought +2 crowdfunded
WB Electronics (Poland)	FlyEye	ISR Mini-UAV, artillery spotter		20
WB Electronics (crowdfunded in Lithuania, Ukraine)	Warmate	Catapult-launch loitering munition	$1 million / $1.73 million (crowdfunded)	37 from Lithuania, 40 Ukraine/ Monobank,
Additional unspecified unmanned donations: Australia (UAVs and UGVs), France (recon UAVs), Germany (43 ISR drones), Netherlands (UAVs), Portugal (UAVs), UK (200 surveillance drones), UK (estimated 1,000 anti-tank loitering munitions)				
*Value when converted to U.S. dollars on May 1, 2022 Purchase by private entity for donation to Ukraine; Corporate donation to Ukraine; Corporate sale to Ukraine; Government donation to Ukraine Donors specified in parentheses. Numbers indicate UAVs committed, not necessarily delivered.				

FIGURE 13.1 – Additional Reported Private/Commercial UAV Transfers to Ukraine June-September 2022[59]

These aerial drones have also provided crucial tactical support by designating targets for artillery and other long-range weapons systems. First, unmanned aerial vehicles serve as "spotters" to enable the Ukrainian forces to execute precision strikes. Second, UAVs have been used in ground element conducting direct assaults, which Senior Stimson Fellow Dr. Kelly Grieco highlights as "actually (…) one of the most effective uses of drones. So, they spot for artillery so that they're able to make the fire more accurate. The drone can fly over and identify targets and then send back coordinates so that artillery can be adjusted," a combination she describes as a "mix of old and new on the battlefield."[60] This usage speaks to the high impact that UAVs have had, and will continue to have, on modern warfare. As Dr. J. Phillip Craiger and Dr. Diane Maye Zorri suggest in their work on trends in unmanned systems for special operations, improvements in technology increase the likelihood that these drones will be force multipliers and force levelers on the battlefield, where this will be of "particular concern in gray zone conflicts."[61]

In many instances, the Ukrainians have augmented their drones with additional controls and different payloads. This additional layer of capability highlights the incremental nature of battlefield innovation. While larger countries might focus on bringing a large, exquisite weapon to bear against and enemy, the Ukrainians are either adding or subtracting material from COTS technology to innovate at the unit level. Not only does this capability allow Ukraine to hold the adversaries at risk, conduct pre-assault fires, and sow confusion in enemy ISR detection processes, it also forces the Russians to consider each drone at an individual level instead of as a "class," thus complicating and extending the targeting Observe-Orient-Decide-Act (OODA) Loop.[62] As Dr. Adam Lowther and Dr. Mahbube Siddiki point out, "For Russian soldiers already struggling to rationalize their experience in Ukraine with the justification they were initially given for the war, adding the fear of attack from unseen drones only makes the anxiety of war more challenging."[63]

The significance of this cannot be overstated. One of the primary functions of psychological warfare is to destabilize the adversary decision-making process or to sow distrust. Since some of these drones have been modified to nonstandard specifications to increase battlefield ambiguity, it is possible

that UAVs can exert psychological pressure on adversary forces.[64] This effect has a compounding consequence of slowing Russian troop movements and targeting cycles, thus eroding the tactical advantage of a larger fighting force while increasing Ukrainian fire mobility. For example, "small drones have changed the operational tempo of artillery, shortening time-critical targeting and firing cycles from about half-an-hour to three to five minutes," thus "help[ing to] increase precision and pace of artillery fires and keep soldiers safe."[65] More powerfully, video footage has been released that shows a Russian soldier actually surrendering himself to a Ukrainian UAV, and the clip has made its rounds on the internet with instructions for more Russian soldiers to follow suit.[66]

UAVs also have profound effects on a military's capability to supply its forces and sustain its operations. The Ukrainians have taken advantage of expansive UAV capabilities to augment their battlefield supply lines. This approach is neither unprecedented nor warfare unique. In 2019, scholars from Ukrainian Aviation University presented drones as a potential answer to civilian logistical failures, citing that "the degree of UAV involvement in freight traffic will continue to grow rapidly as the range of UAV flight and carrying capacity increases, and the air law is liberalized."[67]

While some skeptics have cautioned military planners against relying on UAVs for battlefield logistics, arguing that "drone technology is not ready for wartime" and "expressed concern about well-meaning outsiders with unproven technology creating risks borne by those on the ground," it is clear that drones have at least enabled existing Ukrainian supply efforts in the past year of the invasion.[68] As Marcin Frackiewicz notes, drones have had a revolutionary effect on the Ukrainian "ability to deliver supplies to troops on the front lines, often under heavy enemy fire, [proving] to be a vital asset in the ongoing conflict" by providing water and food as well as expanding mesh networks and extending lines of communication.[69] In all, the conflict between Ukraine and Russia has been a proving ground for the tactical use of UAVs in modern irregular warfare. Ukrainians have demonstrated that even a technologically outmatched military can effectively employ UAVs for a variety of roles, from ISR to psychological warfare. These "eyes in the sky" have been essential to

many of the tactical successes against Russia and will likely be instrumental in the outcome of the war.

WARFARE AS A CONSUMABLE: ATTRITABLE UNMANNED SYSTEMS AND THE GRAY ZONE

While autonomous systems have permeated the battlefield, the U.S. SOF enterprise is more used to exquisite and expensive systems than Ukrainian drones built en masse in the European theatre. As a result, unmanned systems in all domains are valuable assets that force commanders of accept a certain amount of risk when planning for their employment. The expectation is that expensive autonomous platforms, like the U.S. Navy's *Mariner,* will always come home. Operations are shaped accordingly. The Ukrainian conflict has added nuance to this perspective, offering that autonomous systems can, and in some case should, be disposable assets.

This realization is incredibly significant for gray zone warfare due to the emphasis that gray zone operations place on non-attribution and domain awareness, as disposable autonomous systems could enable the DoD to "to meet the needs that emerge in naval warfare areas such as mine countermeasures, anti-submarine warfare, or anti-surface warfare" at a lower risk to force and risk to mission in the maritime environment.[70] In other domains, these smaller, cheaper systems provide smaller units like SOF with the ability to punch above their weight – sometimes literally. Examples of cardboard UAVs and small "kamikaze" USVs allow Ukraine to inflict damage at exceptionally low costs. It is possible that attritable systems, which this chapter defines as autonomously-delivered, one-way payloads for military use, can both multiply and diversify operational effects in the gray zone, particularly for special operations.

In order to multiply the effects and utility of UAVs on the battlefield, the Ukrainian military has turned towards low cost, easily attainable materials that can get through embattled supply lines. While previous examples like the customized DJI Mavic drones have "have been so effective at combat that most of the drone rotors and airframes that filled the basement workshop would be gone by the end of the week," Paul Mozur and Valerie Hopkins point out that

for Ukrainian units, "Finding new supplies has become a full-time job."[71] The Russians are not the only ones who have degraded Ukrainian drone supplies. *The New York Times* also conducted an "analysis of trade data and interviews with more than a dozen Ukrainian drone makers, pilots and trainers," ultimately showing that "Chinese companies have cut back sales of drones and components to Ukrainians" while maintaining supplies to the Russian Federation.[72] [73] In response, the Ukrainians have necessarily diversified their unmanned systems repertoire to include units made of wooden dowels, rubber bands, and cardboard.[74]

Originally produced by Australian firm SYPAQ, these disposable drones called Corvo Precision Payload Delivery Systems (PPDs) are flat-packed and shipped off in the hundreds to the Ukrainians.[75] As *Insider* notes, these systems are confusing to radar, easy to build and launch, and easily augmented to meet the needs of the warfighter on the ground.[76] Allegedly, these units have already been used for swarming attacks on Russian airfields, but they also represent a strategic shift in the process and prosecution of conflict for two reasons. First, these drones are intended to be disposable, thus placing emphasis on supplying commercial off-the-shelf, low-cost replacement units rather than maintenance and supply lines for skilled repair of exquisite units. This practice suggests that the battlefields of the future might be more democratic and consequently, more complex than those of the past. Stakeholders interested in the outcome of a conflict could feasibly spend the money to send a drone like the Corvo PPD to a future battlefield, thus making war the purview of the individual as well as the purview of the state – essentially making the gray zone more "gray" than ever before.

This increased democratization may also increase the rate and efficacy of adopting battlefield innovations writ large. As Dr. Steven Biddle states, the war in Ukraine is "an interactive, two-sided competition" where adversaries modify, employ, and re-modify their technologies and force designs with deadly effects.[77] Michael Partridge, SYPAQ's general manager, supports this when he states that the inventive ways the Ukrainians have used their platform have led to "significant feedback that the company is using to improve the mission planning system, user interface and ground control station for the whole

family of Corvo drones."[78] Instead of developing an exquisite system, testing it, evaluating it, and then deploying it, this example showcases a strategic shift in risk acceptance and shorter decision-making times for operators. This method has dangerous implications for increased gray zone activity, including a lower barrier to entry for conflicts and "more deadly but less decisive" wars, will require forces to be able to adapt and innovate outside of traditional research, development, and procurement cycles to be able to survive let along thrive in a future fight.[79]

Overall, the concept of warfare as a consumable process may have far-reaching implications for hybrid warfare and special operations. As emerging technologies become more widely available at lower costs, fighting forces need not depend upon traditionally superior forces in order to achieve operational effects on the battlefield. Willingness to use and lose these systems represents a strong departure from previous dependencies on expensive systems to a more democratized, more competitive environment that will likely favour more adaptive and agile forces like special operations. While Russia's invasion of Ukraine demonstrates innovation for survival, it is possible that future consumable platforms, payloads, and tools may increase quality of life for forces on the ground and increase optionality for commanders while reducing risk-to-force.

CONCLUSION

Over the past five years, NSW has shifted back towards its maritime mission set instead of counterterror. Relevant guidance material from USSOCOM, INDOPACOM, WARCOM, and Pacific Fleet (PACFLT), as well as recently-released technology-oriented strategic documents from the headquarters level, suggest that emerging technologies like autonomous and unmanned systems can be force multipliers for special operations forces across the spectrum of conflict. In fact, these strategic documents are nearly unanimous in their position that special operations forces are uniquely selected, positioned, and trained to leverage autonomous systems in a hybrid environment. More specifically, Naval Special Warfare's contributions to developing, testing, and evaluating unmanned and autonomous systems for use in maritime irregular

warfare may provide a template for the SOF community and the military writ large to adopt promising innovations and make them more accessible to the United States Department of Defense and its allies and partners.

The Russian invasion of Ukraine provides a timely but bloody lesson on how emerging technologies can increase the scope, scale, and accessibility of the battlefield. In particular, employing UAVs and USVs has allowed the Ukrainian military to compete with the traditionally superior Russian Federation. These systems increase Ukrainian intelligence, surveillance, and reconnaissance capabilities, extend and support supply lines, and provide valuable overwatch for Ukrainian forces in the field. These systems can inflict outsized damage and casualties on opposing forces with lower risk to mission and force than their manned counterparts, but they are not without their flaws.

Unmanned systems have become more disposable, but they cannot replace good tactics and appropriate, informed training on the nuances of emerging technologies. Despite several compelling examples of effective tactical employment of unmanned systems, the true value proposition for NSW and the DoD writ large is the research, development, and acquisition of commercial off-the-shelf technologies for hybrid problem sets. Overall, it is clear that high-tech warfare is only as cutting edge as the operators that are required to employ these systems, which may often mean warfare is more accessible, but less advanced than one might presume given recent conflicts. Using autonomous systems in warfare may be faster and less expensive than an operator, but it is not a smarter choice if those systems are used as replacements for their human counterparts. Preservation of the culture, training, and willingness to innovate in Naval Special Warfare is necessary for the United States and her partners and allies to succeed in a future fight.

CHAPTER

14

THE SPECIAL OPERATIONS CYBER FORCE

LIEUTENANT-COLONEL MATHIEU COUILLARD[1]

On April 24, 1980, U.S. President Jimmy Carter authorized a bold rescue attempt of 52 American hostages from the chaos of the Iranian Revolution. Operation Eagle Claw should have been a confidence-building success for the U.S. Army's newly formed 1st Special Forces Operational Detachment – Delta, commonly known as Delta Force. Instead, the failure of the operation delivered a harsh lesson on the importance of joint planning and the integration of joint assets within special operations forces. Today, as we confront the emerging challenge of cyberwarfare, similar lessons can be drawn from the tragedy of Operation Eagle Claw. What joint effects do Special Operations Forces (SOF) require and how can they be optimally delivered? This chapter explores the broad categories of cyber operations which are most relevant to SOF and proposes the integration of cyber forces to SOF organizations. This recommendation is supported by a case study of Operation Eagle Claw and the subsequent birth of special operations aviation within the United States Special Operations Forces Command (USSOCOM).

BACKGROUND AND CONTEXT

Dr. John Arquilla and RAND researcher David Ronfeldt foresaw a revolution in military affairs that would result from the effective application of networked

technologies. In 1993, the authors predicted that the information technology revolution would give rise to *cyberwar*, the conduct of "military operations according to information-related principles."[2] Russia's coordination of land, air, naval, and cyber operations against Georgia in 2008 has been posited as first the instance of cyberwar.[3] However, the relative importance of cyber operations in this conflict has also been questioned.[4] In the context of the current Russian invasion of Ukraine, academics have once again debated the impact that cyber operations may have on a potential conflict.[5] Defence leaders are keenly aware of the challenges and opportunities presented by cyberwarfare, if expenditures are any indication: the Pentagon's cyber budget is expected to reach $13.5B in fiscal year 2024.[6] General Bryan P. Fenton, commander of USSOCOM, stated in 2023 that the command would "heavily invest" in cyber effects to support operations.[7]

General Fenton and other senior USSOCOM leaders have frequently spoken of the "SOF, Space, Cyber triad."[8] This discourse often suggests a partnership between organizations, rather than an integration of capabilities. For instance, General Fenton offered in testimony to Congress that special operations forces could provide "placement" and "access" to support the U.S. Cyber Command's operations.[9] Conversely, U.S. Cyber Command could provide intelligence and other strategic effects to support USSOCOM operations. While many benefits could result from this collaboration, the focus of this chapter is on the integration of cyber capabilities to SOF.

In the same way that SOF does not hold a monopoly over the conduct of special operations, the national cyber forces need not hold a monopoly over cyber operations. As an example of the former, a highly sophisticated cyber operation such as the Stuxnet attack can be conceived as a "special operation in cyberspace," even though it was not conducted by SOF.[10] The explosive growth of digital networks across the military simply renders it impossible for a single organization to execute on all cyber operations. Hence, many U.S. Armed Services have created service cyber components, such Army Cyber Command, Sixteenth Air Force (Air Forces Cyber), Marine Corps Forces Cyberspace Command, and Fleet Cyber Command (Tenth Fleet).[11] In many smaller nations, cyber operations are primarily centralized within

a single command and/or government agency, but these structures may be challenged as a result of the growing need for cyber effects across all warfighting domains.

CYBER EFFECTS IN SUPPORT OF SPECIAL OPERATIONS FORCES

Broad cyber effect requirements for SOF may be deduced from special operations theory. In 1993, William H. McRaven authored a graduate thesis at the U.S. Naval Postgraduate School that would lead to the publication of *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice*.[12] Supported by his analysis of eight 20th century case studies, he argued that the key to success was *relative superiority*, gained when SOF "have a simple plan, carefully concealed, realistically rehearsed and executed with surprise, speed, and purpose."[13] While McRaven's theory chiefly applies to direct action, the concept of *relative superiority* remains essential to other types of special operations (e.g., special reconnaissance, special warfare, etc.) as SOF typically operate with smaller forces to achieve an outsized effect.[14]

Today, digital networks are essential to the coordination of special operations and often critical to their execution. Therefore, their protection underpins the attainment of relative superiority and the success of special operations. Meanwhile, degradation of the enemy's information systems can act as a crucial force multiplier for SOF by disrupting the enemy's ability to execute a response, potentially extending the duration of *relative superiority*. While these effects may be desired by other forces, SOF's imperative to achieve *relative superiority* reinforce and specify the requirements.

This work proposes three categories of cyber effects which are required by SOF: *defensive*, *offensive*, and partner force *capacity-building*. Defensive effects include traditional cybersecurity, which aims to preserve the confidentiality, integrity, and availability of digital networks, but also more advanced capabilities that aid to conceal the force. Offensive effects are tactical in nature and once again aimed at preserving the element of surprise. Finally, SOF's partner forces may also require assistance to develop their cyber capabilities,

which protect both the partner force and SOF. The remainder of this section will further expand on each of these categories of cyber effects and their specificity to SOF.

While every network needs its defenders, stakes for SOF's information systems are higher given SOF's strategic employment and its vulnerability as a small force. Thus, defensive effects include cybersecurity and more exquisite capabilities such as deception and obfuscation. For instance, deceptive cyber defence can help prevent network breaches and alter the digital signature of a special operations team to help it blend in the noise of local internet traffic. The deception could consist of employing network protocols, devices, and encryption that are widely used in a target area. With obfuscation, deployed elements reach back to their higher commands through an intricate network path with multiple redirector nodes to prevent the detection of command-and-control traffic. Both capabilities represent powerful tools to preserve the element of surprise, often crucial to special operations. Yet, neither are particularly useful or even achievable for large conventional forces due to their scale and divergent operational demands.

SOF, as any modern tactical force, will benefit from offensive cyber support. In the planning phase of an operation, strategic effects may be required to gain intelligence. While conventional units may for instance seek information on the disposition of enemy manoeuvre elements, SOF could require much more precise information on individuals or infrastructure of singular importance. As an operation progresses to the execution phase, tactical cyber effects directly support *relative superiority* through the degradation of the enemy's information systems. In this context, SOF are typically employed as a precision force and will require equally precise offensive cyber effects. Thus, more stringent time and space considerations may be a key differentiation between offensive cyber effects that support SOF and other tactical cyber operations. In addition, the employment of exquisite capabilities, which are less likely to be detected by the adversary, may be required to increase the odds of success, and avoid detection.

SOF operate closely with foreign irregular forces, in which case developing the capabilities of that partner force may well be a key task for SOF. In such

scenarios, cyber training could represent a useful contribution to a broader capacity-building effort. Beyond the partner force's own need for defensive and offensive cyber effects, fortifying their abilities in this regard also protects the SOF force as a partner force network could contain information regarding the SOF force. Democratic governments often prefer to provide non-lethal aid to their partners, hence cyber assistance could be more politically palatable than typical forms of training (e.g., weapons handling). Conventional cyber forces will also conduct capacity-building missions but may be unable to do so with a partner nation's irregular forces due to political or cultural sensitivities.

Leveraging the concept of *relative superiority*, it's clear that secure and concealed digital networks and the ability to disrupt adversarial systems are key force multipliers for a small force seeking outsized effects. Further, SOF's partner forces in a capacity-building operation should require similar effects to succeed. As shown in Table 14.1, SOF's high-level cyber effect requirements align with those of other forces. However, these vary significantly on a more granular level based on unique operational characteristics of SOF. The question of how these effects should be delivered, and by whom, remains.

Cyber Effect	Description	SOF Requirement
Defensive	Cybersecurity and other measures to protect digital networks.	SOF require more sophisticated techniques like deception and obfuscation to preserve the element of surprise and protect a smaller force.
Offensive	Disruption or degradation of adversarial information systems.	SOF, being a precision force, require much more precise information and undetectable offensive cyber effects with stringent time and space considerations.
Capacity-Building	Developing the skills and cyber capabilities of a partner force.	SOF, due to their unique access and flexibility, can effectively engage and enhance the cyber capabilities of irregular forces.

TABLE 14.1 – Summary of SOF Requirements for Cyber Effects

OPERATION EAGLE CLAW

In November 1979, as the Iranian Revolution intensified, militants stormed the U.S. embassy in Tehran and took 66 Americans hostage.[15] Senior leaders in the Pentagon began to assess special operations assets that had the ability to conduct a rescue, including the U.S. Army's new counterterrorism unit: 1st Special First Operations Detachment – Delta. Colonel Charlie Beckwith, Delta's first commander, seized this opportunity to deploy the unit he had fought for decades to create. Beckwith had been profoundly influenced by his time embedded with the British Special Air Service (SAS) in 1962 and had relentlessly championed the need for an elite counterterrorism force in the U.S. military.[16] Yet, Delta was only created two years prior to the hostage crisis and had not been tested on the international stage.[17] In fact, Colonel Beckwith had just returned from a validation exercise when he was awakened by the news of the hostage crisis.[18] He immediately dispatched a planning team to Washington D.C., hoping to carve out a role for Delta in an eventual rescue.

The rescue plan rapidly took form and Delta was assigned a central role in the operation. Major General James Vaught took command of the Joint Task Force while Colonel Beckwith was responsible for the ground force in Iran.[19] The hostages were held in several buildings within the U.S. embassy's massive complex in Teheran. Delta was confident in its ability to overcome the occupiers and rescue the captives. However, from the early planning stages of Operation Eagle Claw, planners struggled with the challenge of inserting the ground force at the embassy. Having ruled out suggestions varying from a parachute insertion to the use of bicycles, planners selected a highly complex, if feasible, course of action.

Operation Eagle Claw brought all major service branches of the U.S. Armed Forces to contribution.[20] Three U.S. Air Force MC-130s transporting the ground force and three EC-130s transporting fuel bladders would depart from an island off the coast of Oman to land at an austere airfield some 200 miles southeast of Teheran, designated as Desert One. In parallel, eight U.S. Navy RH-53D helicopters would take off from an aircraft carrier in the Gulf

of Oman, *USS Nimitz*, to link up with the ground force at Desert One. A company of U.S. Army Rangers would secure the airfield while the helicopters refueled and boarded Delta operators. The RH-53Ds, selected by planners mainly due to their range and size, would transport Delta to a hide located closer to Teheran.[21] After the embassy had been cleared, the helicopters would pick the rescue team and the hostages up at the embassy. Meanwhile, the Rangers would clear an airfield just south of Teheran, designated as Desert Two, where U.S. Air Force C-141 strategic airlifters would transport all troops and the hostages back to safety.[22]

Throughout the winter and spring of 1980, units with a role in the operation conducted rehearsals and exercises to prepare. However, because these units were based in different locations and to preserve operational security, no full rehearsal with all elements was ever conducted.[23] C-130 crews from Europe and Japan familiarized themselves with night-vision goggles. Initially, U.S. Navy pilots were tasked with flying the RH-53Ds, normally used for minesweeping operations. These pilots were found unsuitable for the task and replaced by pilots from the U.S. Marine Corps.[24] Colonel James H. Kyle, the air component commander on Operation Eagle Claw, opined that U.S. Air Force pilots would be better qualified for the mission.[25] General Vaught brought this recommendation to the Chairman of the Joint Chiefs of Staff, but no change was made. Meanwhile, Delta continued to stage rehearsals in a mock-up of the embassy complex and perfected their component of the plan.[26] On 16 April 1980, U.S. President Jimmy Carter authorized the rescue operation, frustrated by months of failed negotiations with Iran.[27]

Late in the afternoon on April 24, 1980, Operation Eagle Claw kicked off with the departure of the ground force from Oman.[28] All was smooth from their perspective aboard EC-130s high above the desert storms. The RH-53Ds, however, were experiencing severe effects from the weather, such that two helicopters did not make it to Desert One and the remaining aircraft were delayed. Meanwhile, C-130s landed at Desert One but were rapidly met by incoming traffic. The U.S. Ground Force captured civilians that were traveling to a wedding by bus and destroyed a refueling truck. As troops began to board the RH-53Ds, a third helicopter was declared unfit to fly. Given the

limited lift capacity of the helicopters, the task force had previously determined that at least six of the eight helicopters needed to be in flying condition at Desert One to continue the operation. Consequently, Colonel Beckwith radioed to task force headquarters and ordered all aircraft back to base. In the ensuing chaos, eight American service members died when an RH-53D collided with a C-130. The remaining RH-53Ds were abandoned at Desert One, as flames consumed the wrecked aircraft and detonated the explosives on board.

APPLYING LESSONS FROM OPERATION EAGLE CLAW TO THE SOF CYBER FORCE

Operation Eagle Claw may have ended in failure, but it also led to the birth of modern SOF aviation.[29] In the aftermath of the operation, the Holloway Commission highlighted a series of deficiencies which ultimately led to the reorganization of SOF. The 160th Special Operations Aviation Regiment (160th SOAR) stood up in 1981, within the newly created Joint Special Operations Command (JSOC).[30] Working closely with other special operations units while maintaining a technical relationship with U.S. Army Aviation, the unit has been highly successful. As a potential consequence, the concept has been replicated in other SOF organizations. For example, in Canada, 427 Special Operations Aviation Squadron (427 SOAS) is generated by the Royal Canadian Air Force (RCAF) but embedded to the Canadian Special Operations Forces Command (CANSOFCOM) under an operational command (OPCOM) relationship.[31] The RCAF conducts personnel management and other aspects such as air worthiness and safety standards, and air procedures. Meanwhile, CANSOFCOM manages all operational tasks and provides SOF-specific training.

Cyber forces should be integrated to SOF organizations in a similar manner to optimize operational effectiveness. Just as the 160th SOAR was formed in response to identified gaps during Operation Eagle Claw, the absence of integral cyber units within SOF may constitute an important gap. Filling the void would enhance the coordination of cyber operations, foster the tailored development of capabilities, and ensure a cultural alignment. As with

427 SOAS, the integration of cyber forces within SOF can benefit from a joint management approach. The national cyber command could be responsible for personnel management and technical oversight while SOF would assume OPCOM, ensuring that cyber forces are aligned with their specific needs. Further, successful integration of 160th SOAR and 427 SOAS offers a blueprint for the process through which SOF organizations can effectively incorporate cyber forces within their operational context. Just as events at Desert One led to the creation of specialized SOF aviation units, the challenges and opportunities of today's cyber landscape should similarly drive the establishment of dedicated cyber units within SOF, ensuring a responsive, tailored, and coordinated approach to cyber operations.

The SOF cyber force is a necessary complement to a national cyber command. While the complete unification of cyber resources may offer certain efficiencies, effectiveness must be prioritized over efficiency in the context of special operations. The unique operational context and requirements of SOF require specialized cyber support that a dedicated cyber element can best provide. Nonetheless, national cyber forces would still provide essential support to special operations, in the same way that conventional aviation complements SOF aviation. For instance, through the routine monitoring of networks or the development of advanced capabilities beyond the scope of SOF cyber units. National cyber forces would also conduct technical oversight of the SOF cyber force and coordinate the delivery of effects in an area of operations. Considering the increasing reliance on digital resources within special operations, the cost of a SOF-specific cyber unit should be viewed as a strategic imperative to enhance operational effectiveness.

CONCLUSION

The closing pages of Colonel Beckwith's memoirs delve into the aftermath of Operation Eagle Claw. When asked in Congressional hearings how the military could avoid such a tragedy in the future, Beckwith responded:

> Sir, let me answer you this way (…) if Coach Bear Bryant at the University of Alabama put his quarterback in Virginia, his backfield

> in North Carolina, his offensive line in Georgia, and his defense in Texas, and then got Delta Airlines to pick them up and fly them to Birmingham on game day, he wouldn't have his winning record. Coach Bryant's teams, the best he can recruit, practice together, live together, eat together, and play together. He has a team.[32]

Beckwith concluded, "My recommendation is to put together an organization which contains everything it will ever need, an organization which would include Delta, the Rangers, Navy SEALS, Air Force pilots, its own staff, its own support people, its own aircraft and helicopters."[33] And so, the Joint Special Operations Command (JSOC) was formed before the end of 1980. With it, modern SOF aviation and other enabling units were created.

Today, SOF have a strong requirement for cyber effects which is distinct from that of conventional forces. This chapter described SOF-specific offensive, defensive and capacity-building cyber effects, which are crucial to the attainment of *relative superiority* in the current era. Thus, one can imagine that if Operation Eagle Claw and the ensuring upheaval had happened more recently, then a cyber unit may have been created alongside the other enablers that were integrated to JSOC. Cyber capabilities may already exist at various levels of maturity within SOF organizations across the globe and could ultimately take a multitude of different forms. However, lessons from Operation Eagle Claw indicate that the personnel and equipment required to provide SOF-specific cyber capabilities should be integrated within SOF organizations. Military leaders must not wait for a similar event to occur and impose this change.

CHAPTER

15

THE FIGHT FOR THE FUTURE: EVOLUTION OF SPACE AS A WARFIGHTING DOMAIN AND THREATS, ROLES, AND OPPORTUNITIES FOR NAVAL SPECIAL WARFARE

CECILIA PANELLA,
LIEUTENANT COMMANDER HANS LAUZEN,
LIEUTENANT (JAG) CHARLES BIBBS,
LIEUTENANT (NAVY) AUSTIN DUMAS AND
LIEUTENANT (NAVY) LLOYD (FORREST) HANSEN

After more than two decades of fighting the Global War on Terror (GWOT), Special Operations Forces (SOF) have finely tuned their staffing, technical, and operational capabilities to fight and win irregular, low-intensity conflicts in multiple theatres. With the introduction of information, cyber, and space as warfighting domains and the rise of near-peer adversaries, the parameters for ensuring the safety and security of the United States (U.S.) have changed. Threats to command and control, information superiority, and exploitable gaps between warfighting domains have forced the joint services to consider shifting the primary mission sets of their most flexible and adaptive forces – SOF. Despite changes in rhetoric, force structure, and resourcing, tightly

tailored GWOT mission requirements limited SOF's capability to adapt under austere conditions. In particular, Naval Special Warfare (NSW) was forced to rely upon a bare-bones operational structure that has negatively impacted their force resiliency and focused on traditional "black hat" adversaries. At the political level, general reliance on American military superiority has also bred complacency; winning against an operationally and tactically inferior adversary is a much more forgiving endeavour than fighting a peer. Simply put, SOF has been forced into brittleness.

Where some policy-makers have seized upon this opportunity to consider gutting the SOF community of its resources and bastardizing its mission set, we see the resurgence of near-peer competition and the increased importance of space as a warfighting domain as a critical opportunity for NSW. Recent developments in command, control, computing, communications, cyber, intelligence, surveillance, reconnaissance, and targeting (C5ISRT), complex mission sets, and increased emphasis on over-the-horizon capabilities have proven crucial for operating in a distributed maritime environment against a potential peer adversary threat. More specifically, NSW may be able to increase the likelihood of mission success for U.S. forces operating in complex, denied environments by exploiting their ability to both operate in and mitigate exogenous sensory "darkness," which this chapter defines as the deprivation or denial of traditional C5ISRT infrastructures.

The significance of NSW cultivating and enhancing these capabilities is twofold. First, SOF can innovate and adapt to emerging circumstances in space technology development and changing environments quickly, thus allowing the United States to maintain operational and strategic advantage. This proficiency is especially important as the prevalent view in strategic planning suggests that the U.S. Department of Defense (DoD) will lack space-based capabilities in a future conflict with a peer competitor. Although in a conventional sense, it is plausible or perhaps unavoidable that most space-based communications will be impaired if the U.S. engages in a major conflict in Indo-Pacific Command (INDOPACOM), it is dangerous to assume that the absence of 'space' will make it futile to pursue commercial off-the-shelf solutions or render naval SOF ineffective. Recent technological advancements and exercise implementations

show that numerous methods exist for augmenting infrastructure and communications resilience, which NSW could employ to preserve an operational edge. The NSW's key value proposition lies in its capacity to operate in a contested environment: conventional beliefs about the possession or lack of 'space' overlook the complexity of the full conflict spectrum.

Second, space-based capabilities may not constitute a conventional win-lose dynamic, but more of a lose-lose situation. If a peer competitor were to dismantle global space-based systems, it would consequently hamper its own operational effectiveness. Though an adversary might selectively target a specific U.S. asset, a widespread communication 'blackout' is a more probable outcome, necessitating U.S. forces to counter sensory deprivation or denial. NSW could leverage the value-neutral nature of space-based hardware to enhance force resilience, potentially facilitating strategic competition and integrated deterrence in a beneficial way. This perspective adds nuance to the standard assumption that 'space' will be completely unavailable, emphasizing that many space-based communications could face degradation, and rigid operational electromagnetic control (EMCON) may be enforced in certain areas of operation (AO).

This chapter will begin with a strategic and operational overview of NSW's current role in strategic competition, with emphasis on the initial rise of the Space-SOF-Cyber Triad and the necessity of developing and effectively employing space-based assets. The next two sections will compare and contrast space capabilities development during the Cold War with the more recent competition with the People's Republic of China (PRC), ultimately highlighting that both assets and operational forces must be designed, organized, and employed effectively together to achieve desired end states. This section will also emphasize the outsized role that NSW may play when engaging with China across the spectrum of conflict in terms of two specific capabilities designed to combat sensory darkness: Position, Navigation, and Timing (PNT) capabilities, and contributions to Combined Joint All-Domain Command and Control (CJADC2). Finally, this chapter will confront the assumption that space is not an attainable or manipulable asset for future engagements in the Indo-Pacific AO, ultimately arguing that in a

conflict with China, space will be the most important and most dangerous warfighting enabler.

STRATEGIC AND OPERATIONAL INFRASTRUCTURE

It is important to note that NSW's contributions to strategic competition and integrated deterrence do not happen in a vacuum. In fact, SOF are increasingly prioritizing integration across services as well as within specific warfighting domains. In 2022, the Senate Committee on Armed Services (SASC) Subcommittee on Emerging Threats and Capabilities received testimony on Special Operations Command (SOCOM)'s "efforts to sustain the readiness of special operations forces and transform the force for future security challenges."[1] One of the commonalities between service statements was a renewed commitment to integrating SOF for strategic competitive ends. Specifically, Lieutenant General Jonathan P. Braga highlighted Army Special Operations Forces (ARSOF)'s commitment to build the "SOF-Space-Cyber Triad," stating that "this is a convergence of trans-regional, multi-domain, and joint capabilities to exponentially increase the holistic strategic effects of each capability across the spectrum of conflict now and in the future."[2] Then NSW Command Commander Rear Admiral Wyman H. Howard echoed this sentiment saying, "our objective is to invest in capabilities that can provide all domain effects from maritime access vectors to solve the Joint Force's hardest problems" by "continuing to invest in exquisite, cross-domain capabilities to increase advantages in the gray zone where SOF's forward footprint provides effective access for holding adversaries' critical targets at risk."[3]

This alignment of people, processes, and capabilities across services and warfighting domains signals two things. First, NSW's promise to effectively resource integration across warfighting domains implies a necessary interoperability of technical and operational expertise that has traditionally been kept in service-specific silos. Simply put, NSW is putting its money – and personnel strength – where its mouth is. Second, it commits NSW and SOF writ large to a new value proposition: expanding irregular, integrated deterrence options to establish warfighting advantage across the conflict continuum.

Gone are the days of SOF as a hammer to achieve national, kinetic objectives. The service chiefs have created strategic and organizational room to manoeuvre and better compete against a near-peer adversary.

In creating this organizational room to manoeuvre, the creation of the Space-SOF-Cyber "Triad" may also expand the range and utilization of options that the United States has for implementing integrated deterrence. As Brigadier General Guillaume "Will" Beaurpere and Colonel Ned Marsh suggest in their article "Space, Cyber, and Special Operations: An Influence Triad for Global Campaigning," space, SOF, and cyber capabilities "…provide a much-needed menu of options for scenarios in which national security interests are potentially threatened but when hard power options that risk escalation are less preferable."[4] Their article goes on to articulate the utility of "less escalatory, more politically palatable, and more appropriate to competition and low-intensity conflict" capabilities that are "already significant in and of themselves" at the individual service level.[5]

The scope of this chapter focuses on two broad space-based capability categories that have demonstrated operational utility specifically for NSW: PNT capabilities, as well as Joint All-Domain Command and Control (JADC2). Given its distinctive and irregular capability set, NSW is uniquely positioned to identify, develop, and utilize specific technologies in these categories to increase mission success in "dark" environments. In doing so, NSW will be able to increase the plasticity of its force and mission set, thus contributing to a more resilient DoD and increasing optionality across the spectrum of conflict in integrated deterrence.

HISTORICAL CONTEXT

In order to understand the importance of space for special operations, it is crucial to contextualize the historical, technological, and strategic significance of space capabilities for both the United States and prominent near-peer competitors like the Russian Federation (RF) and the PRC. This section breaks space capability development into two main periods, with the first focusing on the Cold War and U.S.-Soviet great power competition. For the Americans,

space was a symbol of Cold War technological superiority over an amorphous Communist threat. The most common goal for American research and development expenditures over this period focused on intelligence collection through increasingly accurate imagery, with the goal of understanding Soviet capabilities throughout multiple proxy wars in the late 20th century. Similar to American sentiments at the time, the Soviet Union's space capabilities development during the early Cold War era reflected its desire to establish technological dominance over its peer adversary. Despite these motivations and large commitments in resourcing and personnel from Moscow that led to initial successes, the Soviet space program lost both momentum and funding during the second half of the Cold War, possibly due to domestic political destabilization issues.

The second section focuses on post-Cold War technological development and increasing American military advantage in the space domain. Comparisons to the Russian space program Roscosmos and the Chinese space program managed by the China National Space Administration (CNSA), particularly in areas like commercial industry, highlight the primacy of cultivating and maintaining space-based capabilities for employment across the competitive spectrum. When combined with the recent strategic pivot to INDOPACOM, a push for increased capabilities to plan and execute distributed maritime operations, and the articulation of the Space-SOF-Cyber Triad, new advances in command and control, targeting, and reconnaissance space-based technologies can be easily leveraged by NSW.

When comparing these two eras of space capability development, two key lessons arise: First, political commitment to technological advancement must be equitably matched with consistent resourcing for testing and experimentation down to the component level for a program to be successful, especially for special operations. Second, employment of space as a war-fighting domain specifically for special operations is not new. Rather, space intelligence, surveillance, reconnaissance, and targeting capabilities have been integral for SOF since states could maintain orbit. Both lessons suggest that there is ample foundation for developing SOF-familiar, if not SOF-peculiar, space-based capabilities for utilization across the spectrum of conflict.

AMERICAN COLD WAR SPACE HISTORY

For the Americans, the history of military space capabilities began in 1958 with the first satellite reconnaissance program developed by the U.S. Air Force – Weapon System 117L (WS117 ARPA).[6] This technology was groundbreaking for the time because it provided new concepts of intelligence collection with a wide range of applications and was difficult to detect and impede. The WS program, funded with $163.9M (adjusted to $1.02B today), involved the launch of SAMOS reconnaissance satellites into low-earth orbit. The SAMOS satellites could provide optical reconnaissance products (photographs and video), and electronic intelligence (ELINT) and transmit these products back to Earth.

From a more bureaucratic perspective, some of the success of these early Cold War missions can be attributed to the consistent executive attentionand resourcing for space research and development. This was partially a consequence of the Second World War – as former Director of Policy Development for the National Aeronautics and Space Administration (NASA), Dr. Sylvia Katharine Kraemer, points out in her paper "NASA, Monopolies, and the Cold War: The Origins and Consequences of NASA Patent Policy, 1958-1996," continued military equipment requirements resulted in "federal dollars becoming the fuel that powered a vast enterprise of post-War industrial research and development."[7] This investment institutionalized and routinized the relationship of industry and defense after the cessation of World War II hostilities, essentially allowing the United States to continue to shape civilian research and reap the benefits of substantive technological developments during this time frame. NASA's portion of the federal budget skyrocketed to a peak 4.5 percent of the annual budget in 1966, and the United States also continued to provide for the establishment of private companies developing space-based capabilities throughout the 1960s and 1970s.[8]

Despite the success of the Apollo 11 mission in 1969, federal investments in space-based research and development dwindled into the 1970s. It is important to note that this reduction in federal spending did not indicate a lack of interest in space capabilities; rather, it demonstrated a shift in the strategic and economic value proposition of space. As Dr. Trevor Brown highlights in his

article "The American and Soviet Cold War Space Programs," the transition to a focus on "practical economic and security space applications" gave the United States a substantive lead in depth and breadth of program development over the Soviets.[9] American willingness to focus on less sexy commercial programs like communications satellites and space imagery resulted in around "$38B (saved) for its economy by the achievements of applications satellites by the end of the 1970s."[10] Dr. William Schauer's book *The Politics of Space: A Comparison of the Soviet and American Space Programs* substantiates this, pointing out that while Communications Satellite Corporation (COMSAT) was founded by federal act in 1962, the company was privately owned and eventually privately paid for a large portion of NASA's satellite launches by the mid-1970s.[11]

The traction of the American space program was not limited to its hybridized, consistent funding model. Early satellites were quickly superseded by a joint Central Intelligence Agency (CIA)-Air Force program called CORONA (codename DISCOVERER), providing improved satellite image clarity and increasing the proliferation and quality of American surveillance of the Soviet Union.[12] The CORONA program put large cameras into orbit to illuminate U.S. understanding of Soviet strategic bombers and nuclear capability. Once high-quality images were captured, a capsule of the exposed film was parachuted to Earth and caught in midair over the Pacific Ocean by the Air Force's C-119 Flying Boxcar.[13] The first 13 CORONA missions were unsuccessful due to camera malfunctions, spacecraft errors, and missed recoveries. Mission 14 was an incredible success for space-based intelligence collection, providing more photographic coverage of the Soviet Union than all previous U-2 missions combined.[14] The U.S. Air Force conducted an additional 30 CORONA missions until 1972.

While CORONA was not a SOF-specific mission, the strategic implications of the program's success were massive. As Drs. Dwayne Day, John Logsdon, and Brian Latell point out in their book *Eye in the Sky : The Story of the Corona Spy Satellites*, CORONA set the new standard for intelligence, surveillance, and reconnaissance for DoD.[15] By providing high quantity and quality satellite imagery, CORONA provided defense leaders with the ability to refine intelligence estimates and pass that information to components for action,

as is made evident by American reliance on satellite programs during the Vietnam and Korean Wars.

The DoD was also increasingly willing to leverage smaller, more proliferated space-based capabilities significantly affecting how American SOF prepared for and conducted operations. Meteorological satellites equipped with day and night vision capabilities presented invaluable intelligence data that informed SOF mission planners of flooded rice fields used to conceal booby traps or burning rice paddies that would obscure helicopter pilot vision. Contributions such as these enabled the 1970 So'n Tây Prisoner of War Raid, a daring special operations attempt to free prisoners of war outside Hanoi, North Vietnam's capital city. When planning the mission, the Defense Intelligence Agency (DIA) used "a dedicated team of experts to analyze photos of So'n Tây being produced by satellite reconnaissance, SR-71 reconnaissance aircraft, "Buffalo Hunter" low-altitude drones, and RF-4 aircraft missions" since the dense and inhospitable jungle environment and a savvy adversary made traditional human intelligence (HUMINT) and signals intelligence (SIGINT) methods of collection impossible.[16]

Commanders also used satellite imagery provided by weather satellites to forecast ideal weather conditions for the rescue, allowing a substantial air package of 25 aircraft to enable the operation.[17] While Benjamin Schemmer, a retired Army paratrooper and owner, editor, and publisher of *Armed Forces Journal International* magazine in Washington, D.C. for 24 years, highlighted that the team was "almost totally dependent on photographic reconnaissance for the intelligence so vital to the success of the raid." He continued, the mission is still regarded "as arguably the preeminent model of all special operations missions conducted by the U.S. military."[18]

Military satellite communications (SATCOM) have also been critical to special operations for many decades.[19] Like remote sensing, SATCOM originated in the Cold War era when the U.S. and Soviet Union sought to secure communications between their respective military forces. During the Korean War, U.S. Army Satellite Communications Agency (SATCOMA) deployed the first ever satellite communications terminal in Korea, the AN/TSC-54.

According to SATCOMA recorded history, AN/TSC terminals "w(ere) also the last voice out of Saigon at the end of the (Vietnam) War."[20]

Since the Defense Satellite Communications System (DSCS), one of the earliest operationalized systems, communications satellites have significantly evolved to provide two-way tactical communications, global coverage, increased security, increased resilience to interference and jamming, and increased bandwidth and data transmission rates. The customization and bandwidth characteristics associated with current SATCOM systems, such as the Wideband Global SATCOM (WGS), are essential for SOF to support unique mission requirements.

The development of global positioning system (GPS) technology in the 1970s and 1980s further enhanced the American military's use of space-based capabilities. The predecessor to GPS originated out of necessity to provide nuclear submarines an accurate fix on their location – a requirement to launch ballistic missiles.[21] A collaboration between the Defense Advanced Research Projects Agency (DARPA) and Johns Hopkins' Applied Physics Laboratory produced the first satellite positioning systems to provide this capability (the Transit Program) to submarines. While this system would later be superseded by what we now refer to as GPS, the original Transit system proved the longevity and utility of integrating civilian and defense research institutions to directly enable operations.

From this early era in American space exploration, we can clearly see the importance of tying resources to clear research and development priorities and programs. President John F. Kennedy's address to U.S. Congress in 1961, exemplified this call to action, stating that "before the decade is out" the United States should "land a man on the moon and return him safely to Earth."[22] From that moment on, the United States mobilized its newly integrated defense, research and development, acquisition, and industry team towards achieving this end. Despite this mobilization for scientific purposes, it was not the landing of the man on the moon that changed the strategic and operational context for the U.S. DoD. As is evident throughout the Cold War, specifically in Korea and Vietnam, U.S. special operations relied heavily on space-based

capabilities to be able to land on, fly over, and navigate through degraded and denied environments in service of the nation.

SOVIET SPACE HISTORY

In contrast to the American willingness to diversify their space portfolio into smaller, more achievable projects, the Soviet Union focused on the grander aspects of manned space flight. Moreover, the Soviet space program was more obviously dual use in terms of research, funding, and development when compared to the United States. While this might seem like a natural consequence of a centralized, Communist economy, the reality was that early American estimates of Soviet expenditures only marked a five-percentage point difference in space spending between the two countries. Early reports from the CIA's Directorate of Intelligence substantiate this, pointing out that Soviet space programs were also largely derivative of one another when compared to more diverse American options.[23] This report also highlights the fact that "Soviet applied satellite programs – communications, meteorology, and navigation – appear to be considerably behind similar U.S. efforts."[24] When taken overall, the Soviet space program had lower funding points and a comparative lack of diversification of projects and infrastructure to American efforts. It is important to note that these shortcomings did not stop either side from investing heavily in space capabilities throughout the Cold War – the margin of error was small enough that both nations committed the brunt of their research and development dollars to space development and exploration.

Russia's history of space activities dates back to the Soviet era, when it launched the first artificial satellite, Sputnik 1, in 1957. For some Americans, "the success of Sputnik seemed to herald a kind of technological Pearl Harbor" and a clear sign of burgeoning Soviet national prestige.[25] For others, American delay was strategic: a memorandum of a meeting between then-President Eisenhower and his advisors on 8 October 1957 explicitly stated that while "Redstone (an early American Intercontinental Ballistic Missile (ICBM)) could have been used and could have orbited a satellite a year or more ago (…) it was better to have the earth satellite proceed separately from military development."[26]

But by the time the U.S. published its first National Intelligence Estimate on the Soviet space program in 1962, "the Soviet approach has contributed to an impressive record of pioneering achievement in the past five years," citing the heaviest satellites in orbit, successful manned orbit, and the reliability of the first-generation Soviet ICBM boosters as indicators of a "well-planned, long-term program."[27]

Soviet commitments to space superiority are further demonstrated by plans in the late 1960s and early 1970s to develop and launch a secret military space station. This expansion came swiftly at the heels of the successful launch of Salyut, the first space station. Despite these early successes and lofty plans, the Soviet space program of this decade was largely seen as a "failure of hasty, scattered, and underfunded Soviet attempts to catch up with the Apollo lunar program," where Massachusetts Institute of Technology's Dr. Slava Gerovitch notes "numerous failures of automatic systems and unsuccessful manual dockings in the absence of onboard guidance computers" plagued Soviet efforts.[28] These failures combined with increasing internal political pressures, ultimately indicating to American intelligence officials that future space endeavours would need "demonstrable economic or military benefits to be derived for any sort of budgetary support" when they issued their official National Intelligence Estimate on the Soviet program in 1971.[29] By further entangling space exploration with military ends, Soviet leadership's attempts to regain earlier international prestige via grand projects were somewhat rewarded – they were able to successfully launch six space stations, Salyut 1 through Salyut 6, before the end of the 1970s.[30]

It is important to note that this entanglement of civilian and military space endeavours was not without issue. In 1975, the CIA released an Interagency Intelligence Memorandum that stated "three out of four" Soviet satellites were associated with explicit military or intelligence activities that "support the operations of military forces either directly or through the national level decision making apparatus."[31] This memorandum assesses Soviet dependence on space-based capabilities as "very high," specifically citing the use of space-based assets in space reconnaissance. While integrating military space capabilities with national strategic ends was a salve to the USSR's wounded

political legitimacy, that same report notes that this dependence might in fact pressure the Soviet Union to cooperate with the United States rather than out-compete it. This prediction is consistent with then-Soviet Premier Leonid Brezhnev's declaration in 1973 that "peaceful coexistence was the normal, permanent, and irreversible state of relations between imperialist and Communist countries."[32]

History tells us that this air of positivity was not to last. The Soviet-Afghan War began in 1979 after Premier Brezhnev ordered the invasion of Afghanistan to support a struggling pro-Soviet government, spawning a conflict that eviscerated the political and military will of the Soviet Union for a decade.[33] During the entirety of the conflict, the Soviet Union had over 100 satellites in orbit, performing collection of communications, photo-imagery, and meteorological patterns to contribute to the war effort. Despite repeated National Intelligence Estimates in 1983 and 1986 that heralded the quality and quantity of space-based assets available to the Soviets, these tools were largely insignificant during the conflict.[34] Preeminent scholar of Russian history Dr. Lester Grau highlights this point, stating that "impact of high-technology weapons (…) can be negated by camouflage, heat shields, decoys and dispersion."[35]

The importance of this relegation of "high-technology weapons" to the operational and tactical periphery cannot be overstated. Soviet failure to successfully and reliably employ space-based capabilities during the Afghan invasion and occupation showcases that space assets – and emerging technologies writ large – are not a panacea for operational failures and tactical mistakes. As casualties in Afghanistan rose, Dr. Grau emphasizes that Soviet forces were often mismatched to tactical needs. More specifically, Soviet SOF (Spetsnaz) were relegated to "convoy interdiction," essentially zeroing out their combat efficacy.[36] This outcome implies two key lessons. First, SOF must appropriately employ emerging technological assets like space-based tools as well as *be appropriately employed themselves.* Second, the willingness to subordinate scientific exploration to military ends that transcended borders and adversaries was not necessarily a bad thing. In fact, some strategic planners might simply call that alignment.

Overall, when compared to Soviet efforts during the Cold War, the Americans focused on smaller, iterative projects that were immediately accessible downrange for SOF. By moving from prestige towards practicality in the face of conflict, the U.S. was able to maintain a more consistent budget for space development and link operators with the technologies that they would need to successfully wage the nation's wars. While neither the Soviet foray into Afghanistan or American entanglement in Vietnam could ever be mistaken for long term strategic success, both conflicts set a powerful precedent for developing and utilizing space-based assets for explicit military purposes – one used with increasing regularity and sophistication in the post-Cold War era and current competition between the West and China.

POST-COLD WAR STRATEGIC REALITY: THE WORLD ORDER IN CONFLICT AND AMERICAN SPACE PRIMACY

Despite the proliferation of space-based capabilities during the Cold War, NATO only declared space a warfighting domain in December of 2019. More recent publications from NATO declare space to be "essential to the Alliance's deterrence and defence," highlighting emerging technologies as having the most potential for "new risks, vulnerabilities and potential threats" in this domain.[37] The *2022 NATO Strategic Concept* states that the Alliance must "maintain secure use of and fettered access to space" and that they "will enhance our ability to operate effectively" in order to meet those goals.[38] The formal articulation of space as a warfighting domain and NATO's commitment to maintaining its freedom and security is significant for two reasons. First, it acknowledges the dependency that many NATO allies already have on space and provides strategic infrastructure for continued support, thus matching space policy and strategy to the ground truth of military operations in the 21st century. Second, this commitment to enhancing space-based capabilities as a cornerstone of deterrence sends a clear signal to peer adversary nations that NATO will not let them operate with impunity. In fact, "hostile actions to, from, or within space (…) could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty."[39]

To be clear, NATO is not advocating for unchecked escalation in space. Rather, these cumulative policies indicate that NATO is now cognizant of the importance of space and acknowledges the danger of neglecting it or abandoning it to a near-peer adversary. This realization is widely agreed to be a step in the right direction, but the simple reality is that peer adversaries like China and Russia have sought to leverage the space domain and space operations to achieve their own strategic ends, often by, with, and through accepted international security processes. For example, "Russia and China attempted to define a space weapon in their proposed treaty, "Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects" at the UN Disarmament Conference in 2008, as referenced in a more recent Congressional Research Service Report.[40] While on the surface this may seem to be a collaborative attempt to organize space for the good of the international order, this proposal was critiqued because it "lacked language that would prevent the development, testing, or deployment of ground-based anti-satellite (ASAT) weapons, which China currently has in its counter-space arsenal."[41] The United States went a step further, stating that the proposal was "a diplomatic ploy by the two nations to gain a military advantage."[42]

These condemnations should be taken with a grain of salt. To this date, the United States has refused to ban space-based weapons altogether. In 2020, "the First Committee (Disarmament and International Security) (...) approved 14 drafts, among them several aimed at stemming the spread of illicit weapons on Earth and at preventing a celestial arms race, and also defeated a motion questioning its competence to approve a text on reducing threats in outer space."[43] This action came at the heels of months of Russian direct-assent missile system testing, with multiple American signals that these activities "represent an ever-increasing threat to U.S. interests," and further describing an April ASAT Test as "potentially threatening and similar to those conducted by Russian satellites with characteristics of space weapons."[44] This international bickering suggests that while the world's major governing bodies have attempted to legislate space to prevent an arms race or future kinetic conflict, these methods rely on compliance by all parties and are largely ineffective against revisionist adversaries. Furthermore, such legislation might also limit the strategic optionality for the U.S. to develop a space-based weapons

of its own. For this reason, the Alliance, and the U.S. in particular, must be knowledgeable of emerging threats in the space domain and be prepared to combat them.

POST-COLD WAR OPERATIONAL REALITY: THE CHANGING VALUE PROPOSITION FOR NSW AND NEAR-PEER ADVERSARIES

For the U.S., the technological advantages provided by space-based capabilities provided a unique augmentation to SOF mission sets, ultimately contributing to special operations successes in the Iraq and Afghanistan campaigns.[45] This increased efficacy came with increased responsibility, as SOF units became the hallmark of the Global War on Terror, exploding in size, increasing operational tempo, and ballooning the SOCOM budget.[46] Specifically, increases in satellite-provided capabilities due to improvements in situational awareness, dynamic command and control (C2), encryption techniques, intelligence gathering and sharing, and data transmission rates that could even enable video teleconference ensured American forces had reliable lines of communication in an austere operating environment. It is important to remember that not all of these capabilities were endogenously developed by DoD. The Iraq and Afghanistan conflicts highlighted the extent to which American forces worked with and relied upon commercial industry to meet their operational needs.

This requirement for fast, reliable, resilient, and secure communications has only been amplified in competition with near-peer adversaries. As of the end of GWOT, the U.S. special operations community is now larger than the entire German army, with a larger wallet than all of Poland's defence budget.[47] Investments in space-based capabilities and architecture have also been on the rise over the past decade. According to the *Journal of the U.S. Bureau for Economic Analysis,* "national defense (space gross output) has been growing much faster than nondefense (space gross output) in recent years, increasing 11.4 per cent for 2019–2021, compared with 2.4 per cent for nondefense."[48] These parallel increases are significant because, as discussed previously, budgetary commitments that mirror national priorities have the

highest chance of maintaining strategic relevance. When taken in combination with SOF's decrease in operational tempo and the rise in importance of demonstrating SOF contributions to the "Space-SOF-Cyber Triad," the U.S. is uniquely positioned to attain and maintain space military advantage in ways our adversaries are not.

This unique positioning is not without tradeoffs. At the operational level, every American SOF commander will have to make their own decision whether to fight with or without the use of space. This decision is especially acute for NSW, which is the tip of the spear for maritime domain awareness and distributed maritime operations in INDOPACOM. On one hand, by using space, a naval special warfare operator can achieve a clearer picture of the mission, through clear communication systems, relevant and timely operations intelligence, or even pertinent weather information. Yet, on the other hand, by utilizing space, a commander accepts the risk of geolocation and counter-targeting, putting operators at risk. Overall, in order to compete in the 21st century battlespace complete with an ever-changing scenario, those same commanders must determine and accept at least some space assets to compete against an adversary. As good practice regardless of the amount of risk, a well-rehearsed and well-tested Primary, Alternate, Contingency, and Emergency (PACE) plan will prove valuable in the face of threats to the joint space domain. This action is not a suggestion; it is a necessity. As Assistant Secretary of Defense for Space Policy John Plumb points out, "space-based missions are essential to the U.S. way of war."[49]

POST-COLD WAR OPERATIONAL REALITY: AMERICAN ADVERSARIES

When the U.S. and her allies and partners consider future operations in the space domain, they must take into account the motivations and actions of an adversary. While the U.S.' most recent experiences with GWOT have hardened SOF to operations in urban, denied, and austere environments, competing in space is much different than fighting a terrorist insurgency. The most dangerous and most capable competitors in space are the Russian Federation (RF) and the People's Republic of China (PRC), both of which can

be considered near-peer adversaries. While the previous section highlighted space positioning and opportunities for American SOF, this next section emphasizes that the U.S. faces challenges both in *type* and *scale* of the threats posed by Russia and China in very different ways.

The 2022 invasion of Ukraine follows a decades-long pattern of Russian aggression, marking President Vladimir Putin's autocratic regime with instability and a declining reputation on the world's stage. This decline has also had disastrous consequences for the Russian space program, which has faced decreasing investments and fading attention. Despite these shortcomings, Russia has demonstrated the ability and willingness to use space-based intelligence, surveillance, and reconnaissance (ISR), organic navigation, and signals intelligence (SIGINT) capability-enabled systems to disrupt communications and degrade foreign militaries' ability to leverage satellite-based capabilities.[50] This seemingly low technological and normative barrier to entry for employing space-based assets in a competitive or conflict scenario makes the Russian Federation a dangerous adversary.

In contrast, the PRC's space program is young, well-funded, and unencumbered by a grueling land war in Europe. In fact, China has developed a strong civil space program, producing the Tiangong Space Station and deploying its own global navigation satellite system (GNSS), the BeiDou Navigation Satellite System. China is also an increasingly capable launch provider with a host of space launch vehicles, including the Long March 5 rocket. When combined with Chinese aggression in INDOPACOM and the Chinese Communist Party (CCP)'s increasing willingness to publicly challenge the global order, it is clear that enhanced Chinese ISR capabilities are anything but benign. In fact, there are many aspects of the PRC's space program that should concern military planners, particularly special operations.

While thoroughly exploring every space-based threat would be a dissertation in itself, there are two technological capabilities that highlight the type and method of common space-based threats currently utilized by near-peer adversaries. The first technology capability to consider is Position, Navigation, and Timing, or PNT. This capability is significant in that militaries have not

always relied upon space-based assets to meet mission requirement. The evolution of small, proliferated satellites reflects a subtle shift in intelligence, surveillance, and reconnaissance that is indicative of the increasingly dual-use nature of these technologies. The second technological capability is less concrete. CJADC2 is the optimistic instantiation of author Christian Brose's warning that militaries should seek to increase the "efficacy, speed, flexibility, adaptability, and overall dynamism of its kill-chains" by integrating space-based assets, autonomous systems, and more agile acquisition practices into battle networks.[51] While space-based assets are insufficient for CJADC2 on their own, no discussion of closing the kill-chain is complete without considering this cluster of technologies and their implications for special operations.

The Ukraine War is an example of the successful use of both these referenced technologies, and nowhere else in recent memory have military technologies and the men and women who employ them evolved so quickly to meet the needs of an autonomous, space-enabled, and robotics-heavy battlefield. It is important to note that the Ukraine War is not a glass ball for NSW when planning future engagements in INDPACOM. Spectating and learning from the European theatre is key to understanding how, where, and why near-peer adversaries might employ space-based assets against the U.S. and its allies and partners, however, this observation is not a Band-Aid for good military planning. More dangerously, the U.S. must assume that the PRC is learning from the Russo-Ukrainian War as well and could be willing to apply those lessons closer to home in a conflict over Taiwan.[52] Overall, the PRC poses a substantively different threat than the Russian Federation, and naval special operators must be prepared to adapt should their services be required in the Pacific.

Specifically, China's space investments and accomplishments have seen exponential growth in recent years. Perhaps the most strategic investment in the eyes of Chinese policy-makers is the ambitious China-Pakistan Economic Corridor (CPEC) and Belt and Road Initiative (BRI) economic connectivity projects that aim to strengthen its political influence in its immediate neighbourhood and around the world. China sees CPEC and BRI

as opportunities to expand its space program. Today, China manufactures, launches, and provides communication, PNT, and remote sensing satellite application services to several participating partner states. Chinese intent is to enter the global satellite manufacturing, launching, and servicing industry market dominated by the U.S. and its European allies. BRI and CPEC provide the impetus, connectivity, and markets for the Chinese space industry to break the International Traffic in Arms embargos on its satellite-related industries, enlarge Chinese economic activity at the regional level and expand Chinese soft power and political influence globally.[53]

Overall, China's commitment to becoming a world-class space power is systemic and methodical, backed by substantive commercial industry involvement, increasing government investment, and military pursuit of high-level prestige projects that the Russians could not dream of considering as they hemorrhage resources into Ukraine. These commitments can be a threat to American access and placement in INDOPACOM. When considering future force design and acquisition structure for special operations, the U.S. should monitor near-peer adversary space activity, particularly as it applies to PNT and CJADC2.

POSITION, NAVIGATION, AND TIMING FOR SOF

Naval Special Operations Forces require the ability to infiltrate and exfiltrate without compromise. To achieve this mission essential task, American SOF and their supporting assets rely on the Global Positioning System (GPS). A part of the broader PNT space mission, GPS uses a constellation of satellites to deliver metre-level position accuracy around the globe and provides USSOF with precision PNT data for operations, including geolocation of targets, ISR imagery, and data collection for targeting and precision fires. When operating in remote and hostile environments, this precision PNT data can be the difference between mission success or failure.

Using GPS for PNT has not always been standard operating procedure for special operations. Operators relied on more primitive navigation methods such as map and compass navigation before space-based systems were made

available to SOF in the 1990s.[54] However, map and compass navigation has many disadvantages especially in low light and low visibility terrain, a common feature of many special operations. Map and compass navigation relies on either terrain association or using lines of bearing to navigate from point-to-point. Many special operations, in the maritime domain for example, do not have the necessary conditions for this method of navigation because of limited visibility or terrain.[55] These limitations made GPS an appealing PNT solution for U.S. SOF adoption.

It is important to note that GPS is not the only tool for satellite-informed PNT. Broadly, these constellations of satellites are called Global Navigation Satellite Systems, or GNSS. They are identified by two main characteristics. First, they provide PNT to an entire region or perhaps the globe. Second, they tend to be associated with one particular nation state. While GPS is most common, the U.S. Space Force's reference documents for GNSS point out that "other nations are fielding, or have fielded, their own systems to provide complementary, independent PNT capability."[56] For the purposes of this chapter, the two main competitive GNSS are BeiDou Systems from the PRC (35 satellites), and *Globalnaya Navigatsionnaya Sputnikovaya Sistema* (GLONASS), from the RF (24 satellites).

With these caveats in mind, American SOF have heavily integrated GPS into their systems and tactics. NSW operators became accustomed to the ease of use and reliable accuracy that GPS provides during recent engagements in U.S. Central Command (CENTCOM). Currently, operators are issued personal GPS devices that can be preprogrammed with route data. Active GPS tracking instantly displays the operator's position and navigational data to the desired waypoint. Additionally, SOF hardware, vehicles and unmanned systems also have embedded GPS receivers to enable operators to find, fix, and finish targets appropriately and effectively. If the receiver has a clear view of the sky, it will reliably acquire GPS signal regardless of environmental conditions.[57] To operate at the speed and reliability of required of modern combat operations, this fast and accurate PNT data is a necessity.

POSITION, NAVIGATION, AND TIMING VULNERABILITIES

During the initial deployment of GPS, leveraging the speed and accuracy of GPS PNT data gave the U.S. military a tactical advantage over less capable adversaries. It was first used in major combat during the First Gulf War, where Operation Desert Storm became widely considered the first "space war" due to the technological superiority provided to American forces by space-based capabilities.[58] More specifically, GPS improved friendly force navigation and delivery of precision munitions to enemy targets to devastating effect, as shown by SOF reliance on GPS to navigate the desert on scud-hunting operations. Following the location of the missiles, aircraft received accurate position data for scud launcher targeting and destruction.[59]

GPS PNT was ultimately so impactful that a Congressional Report on the conduct of the Persian Gulf War said "perhaps one of the more important new items issued was the global positioning system."[60] Also outlined in the Congressional Report is a special operation night helicopter strike that "was possible because of technological advances in night- and low-light vision devices, precise navigational capability resulting from space-based systems such as the GPS satellites."[61] Despite this praise, the tactical advantage of GPS has diminished as adversaries adopt it as their own standard for PNT. Space-based PNT is now a tactical necessity rather than a tactical advantage, as individual nationally accessible constellations could allow a country to target an adversary network without availing itself to attack. With this knowledge, degradation of PNT data presents an exploitable vulnerability for an adversary looking to disrupt military operations.

There are many ways for an adversary to degrade GPS including destruction or jamming of satellites, receivers, or ground control stations. The GPS constellation consists of relatively few satellites; 24 satellites are required to provide the basic coverage of Earth with six satellites in reserve already in orbit around the earth.[62] GPS is not only critical for military operations but for the United States' economy. A report published in 2019 on the economic benefits of GPS for the U.S. found "that GPS has generated roughly $1.4 trillion in economic benefits (2017$) for the private sector in the years since it was made available for civilian use in the 1980s. Most of those benefits have accrued

since 2010."[63] Considering recent increases in Russian and Chinese anti-satellite weapons, the GPS constellation is insufficiently resilient for such a critical service.[64]

In addition to the threat to the GPS constellation, GPS signal jamming threatens special operations forces on the battlefield. According to the Government Accountability Office's report on GPS alternatives, "jamming is the most common and prevalent threat to GPS, largely because jammers are cheap and easily accessible."[65] Due to GPS's high altitude Medium Earth Orbit, the signal to the receiver is a low power signal and "a 1-watt jammer, about twice the power of a LED night light, can prevent the continuous tracking of the military GPS signal at a distance of about two miles and can prevent the initial acquisition of that signal at about 10 miles."[66] This low-power signal means that jammers can be easily produced and disseminated at a low-cost to disrupt SOF's ability to operate effectively. In addition to these low-cost jammers, China, Russia, North Korea, and Iran have all developed extensive jamming capabilities.[67]

One of the best examples of PNT vulnerability is the Russian invasion of Ukraine. Since the fighting began, GPS interference has "expanded on a scale that hasn't been seen before (…) What we're seeing now (…) is GPS jamming bubbles covering hundreds if not thousands of kilometers around tactical cities."[68] Russia is jamming GPS to prevent the use of GPS reliant systems such as unmanned drones and missiles against their cities. Additionally, Ukraine has also been using PNT signal manipulation to defend from incoming Russian attacks. Using a tactic known as spoofing to fool the PNT receiver onboard, Ukraine has been able to trick Russian controlled drones into accepting the wrong PNT signal that caused the drones to rapidly descend.[69]

These jammed signals are many of the same signals that are used by SOF. Whether it is unmanned systems (UxS) or handheld GPS receivers, SOF will be affected by any GPS jamming or spoofing, regardless of the intended target. According to General David Thompson, the Space Force's Vice Chief of Space Operations, "Ukraine may not be able to use GPS because there are jammers around that prevent them from receiving any usable signal".[70] As seen in Ukraine, if SOF want to operate in a GPS-degraded environment, they must

adapt their PNT tactics to account for this growing jamming and spoofing threat posed by near-peer adversaries.

More dangerously, GPS is entirely based on ground-controlled infrastructure. Referred to as the Operational Control Segment (OCS), this infrastructure "includes a master control station, an alternate master control station, 11 command and control antennas, and 16 monitoring sites."[71] In the event of a major conflict, GPS satellites and the OCS become a major target not just for SOF and DoD but also as a point of failure for civilian transport, financial, and communications systems. Future military planners must consider the ramifications of weaponizing GPS on civilian populations, which may complicate the definition and employment of force near or towards non-combatants. In particular, using non-kinetic cyber weapons that leverage GPS can still have kinetic effects. In this way, future employment of PNT has the ability to change the nature of warfare entirely.

THE FUTURE OF SOF PNT

In previous conflicts, GPS could be relied upon because of the adversaries' lack of ASAT capabilities and wide-scale jamming capabilities. This situation is no longer the operational environment for SOF. When examining the Russian electronic warfare capabilities, the American Security Project noted "the evolution of Russian EW is especially important as the *U.S.* turns to deal with new threats."[72] SOF need to find redundant PNT systems to limit the risk of operating in GPS-degraded environments. For mission critical equipment, it is common for SOF to have a PACE plan for redundancy. SOF training and equipment are lacking this level of redundancy for PNT. Currently, map and compass navigation is the main backup used by dismounted SOF. There is a need for alternative PNT systems that can bridge the capabilities gap between GPS and traditional map and compass to complete the PACE plan for SOF preparing to operate in GPS-degraded environments.

There are steps SOF can take in the immediate future to help diversify and strengthen their PNT systems. GPS is only one of multiple PNT constellations. Other nations and partnerships have their own publicly available systems to include the Russian GLONASS and European Galileo systems. Many PNT

receivers can utilize all these constellations in one device, a feature that gives users multiple sources of PNT simultaneously. However, this will not be sufficient for defense against the most common forms of jamming because these systems all operate in similar bands of the electromagnetic spectrum.[73] There are additional measures that can be taken to include utilizing the m-code signal that is designed to be more secure than the traditional GPS signal.[74] GNSS variety and resilient signal design can reduce the threat to SOF PNT, but there is no single solution that can eliminate the PNT threat altogether.

There are emerging technologies that can increase SOF PNT resiliency. For example, the increasing number of Low Earth Orbit (LEO) constellations are an opportunity for alternative PNT systems. With the reduced cost to get satellites into orbit, the commercial space market has expanded, leading to new possibilities in space. Due to their lower-altitude orbits, LEO-based navigation satellites "are thus more precise, powerful, and jam-resistant than those of traditional GNSS."[75] Additionally, LEO constellations require more satellites to cover the same region of earth as the higher altitude GPS constellation, leading to a higher density of satellites.

Historically, this was a viewed as a problem because of the high cost to send satellites to orbit, but now this density makes for a redundant and resilient PNT system.[76] In addition to the traditional space-based PNT systems, technological advances in data analysis, AI, data storage and machine vision are opening the door for many new technologies that do not depend on space. These new systems can aggregate data from various sensors and compare it with pre-existing data to give PNT information.[77] Regardless of the specific system, SOF can benefit from adoption of these emerging PNT technologies and have optionality for PNT PACE planning.

As SOF adapts to the near-peer threat environment, they will have to develop a PNT PACE solution that provides resiliency for their critical navigation data. Traditional GPS will likely be targeted by adversaries and its capabilities will likely become degraded. The ability to adapt quickly is one of the strengths of SOF, and if they are going to remain relevant in future conflict, they will

have to overcome their dependency on GPS. This mandate for adaptive and resilient PNT structures also implies a specific role for American special operations. This situation is a unique opportunity for the United States and its partners and allies to exploit their ability to both operate in and mitigate exogenous sensory "darkness" because PNT's strengths and weaknesses rely on its dual-use nature, SOF must be willing to rely upon smaller, proliferated assets for strategic superiority instead of exquisite kinetic capabilities.

COMBINED JOINT ALL-DOMAIN COMMAND AND CONTROL (CJADC2) AND SPACE FOR SOF

Secure, efficient, and robust networks are often the tipping point between success and failure on an operation. As the old adage goes, "*Two is one, and one is none*."[78] These resilient and redundant communications are essential for modern militaries to coordinate joint operations, maintain near-real-time visibility on the battlefield, gather and disseminate intelligence, and transfer information from sensors to shooters. While the previous section dealt with space-based assets as a tool for orienting operators and collecting ISR for mission planning, SOF are also a key component of CJADC2, which allows forces to seamlessly integrate capabilities to achieve an operational effect. Within this construct, one form of communication has proven especially vital to the efficacy and safety of military operations – SATCOM.

NSW forces often operate in hostile, remote, and complex environments where traditional lines of communication may be unavailable or impractical. In these challenging settings, naval SOF have increasingly come to rely on SATCOM to carry out their missions. Such reliance on SATCOM has prompted significant investment in military-specific SATCOM (MILSATCOM) infrastructure, which provides secure, reliable, and long-range communication capabilities necessary to operate effectively in various conditions. Despite the immense value that MILSATCOM has provided American forces in the wars in Afghanistan and Iraq, there are increasing operational challenges that push the boundaries of what traditional MILSATCOM can provide. More decentralized and dispersed military operations complicate MILSATCOM protocols and infrastructures, as the combined joint force needs to be able

to communicate and coordinate across vast distances and in different theatres of operation. These recent experiences in CENTCOM have highlighted the importance and vulnerability of MILSATCOM, revealing that these usual methods of command and control may not be sufficient in contested environments. Given SOF's mission set, increasing resilience in communications pathways and diversifying communications assets away from traditional SATCOM may provide opportunities to increase operational effectiveness.

Notably, the rise of proliferated low-earth-orbit (pLEO) satellite constellations presents a promising solution. Developed by commercial entities such as SpaceX, Amazon Kuiper, and OneWeb, these networks have the potential to offer low-latency, high-bandwidth communication capabilities that exhibit a high degree of resistance to jamming and other forms of interference. Commercial pLEO satellite constellations also hold the potential to revolutionize military communications. As early as 2021, the U.S. Space Force put out a Request for Proposals (RFP) to private industry for applications of pLEO satellite constellations for military use that would feature "sensors that comprise seven capability layers, to seamlessly perform data communications, track hypersonic and cruise missiles, and provide enhanced battle management, navigation, ground support, and deterrence from space."[79] Since then, these high-speed, globally accessible communication networks have paved the way for more efficient and effective coordination on the battlefield. A specific optical crosslink technology is particularly interesting, while one of the key weaknesses of traditional PNT and SATCOM is its vulnerability to jamming, these crosslinks increase robustness by "routing signals across satellites, avoiding ground stations in contested territories if necessary, reducing the risk of interference and detection" and contributing to overall mission success.[80]

The Russian military made significant efforts to deny and degrade Ukrainian military satellite communications during its 2022 invasion, often relying on the jamming weaknesses of existing space architectures. Russian forces reportedly utilized EW systems to target and jam Ukrainian military satellite communications, thus impeding their functionality and disrupting communication lines.[81] Additionally, the Russians specifically targeted

Ukrainian positions with mortar fire when traditional military communication systems were powered on, making it difficult for Ukrainian soldiers to maintain situational awareness or coordinate operations. Furthermore, Russian EW and jamming operations rendered most of the Ukrainian ViaSat ground terminals inoperable.[82]

In response, a new approach was adopted to maintain communication and situational awareness. Over 15,000 SpaceX Starlink terminals were rapidly deployed to Ukraine,[83] reinstating effective communication lines.[84] Furthermore, wearable 5G technology equipped with local mesh networking and short data burst satellite links drastically enhanced field operators' situational awareness, thus proving their viability and effectiveness.[85]

Emerging commercial pLEO constellations, however, cannot stand alone as a bulwark against communication challenges in military operations. They form a crucial component but not a comprehensive solution to the complex problem of secure and efficient communication on the modern battlefield. As the Center for Strategic and International Studies highlights in a 2023 report, "high-end sensor suites and real-time targeting data are only as effective as the communications network used to transfer information from sensor to shooter."[86] Developing next-generation, resilient, low-signature communication networks is crucial for future military operations, especially considering the escalating sophistication of potential adversaries like China. These state-of-the-art networks need to withstand not only cyberattacks but also physical damage and adversarial disruptions. These factors highlight the urgency of constructing secure, redundant communication channels that draw upon a variety of technologies that are layered and context dependent. These channels would necessitate a dynamic blend of satellite and ground-based capabilities to ensure the necessary robustness and versatility.

It is important to note that even this "layering" process of increasing communications resilience cannot be completed without substantive, consistent investment in space-based assets for military use. While there has been consistent, bipartisan support for increasing funding for space communications infrastructures in the U.S. Congress, senior vice president for government

strategy and policy at Inmarsat, Rebecca Cowen-Hirsch, states, "commercial SATCOM (should) be acquired more strategically, and not on an ad hoc, case-by-case, reactionary basis."[87] The 2020 Enterprise SATCOM Vision released by the U.S. Space Force supports this strategic investment, calling for a "single, integrated SATCOM enterprise (that) will deliver unparalleled options to joint warfighters for mission success" and "scalable solutions that can absorb new systems and products beneficial to users and the overall enterprise while preserving competition and technology innovation."[88] The U.S. DoD has also laid the bureaucratic infrastructure to support the ability to "fight SATCOM," listing the ability to "Modernize and Bolster Transport (Space and Terrestrial) and Data Link Capabilities" as its third priority in the FY23 Strategic Management Plan.[89] Force-level implementation of a resilient and robust space-based communications architecture can enable USSOF to conduct missions with less risk-to-force.

If appropriately resourced, it is not unreasonable to say that layered space-based communication networks could also be the foundation for coordinating joint SOF missions. With the U.S.' dependency on these networks, it is likely that advanced opponents, such as China, may prioritize impairing or eliminating their functionality through either kinetic or non-kinetic means. It is also prudent to consider existing components of U.S., allied, or partnered infrastructure associated with or manufactured by Chinese companies as potentially vulnerable and possibly compromised.[90] Therefore, a truly effective communication system for sensitive joint SOF missions must be secure and seamless across services, interoperable with allies, and require purchasing decisions that emphasize encryption, resilience, and interoperability. This strategic approach to developing communication networks ensures a robust, adaptable defense against the increasingly sophisticated adversarial landscape.

COMMERCIAL-DEFENSE SPACE PARTNERSHIP APPROACHES

DoD has attempted to formalize the creation of a more organized space-based communications network with the development and deployment of a Hybrid Space Architecture (HSA) spearheaded by the Defense Innovation Unit (DIU) in Silicon Valley. At its core, HSA is an excellent example of

research, development, testing, evaluation and acquisition agility, combining defense equities with best-in-class private industry technological capabilities. HSA merges commercial and governmental LEO constellations, potentially resulting in a resilient space framework suitable for a wide array of commercial, civil, and security purposes. As imagined, the HSA incorporates state-of-the-art technologies like secure, adaptive, multi-path communications, uniform standards, autonomous C2 mechanisms, cloud infrastructure, and other commercial space manufacturing efficiencies to both software and hardware.[91] Moreover, the Defense Innovation Unit is designing this architecture with the intent of fully integrating extant DoD space-based assets rather than replacing current systems or increasing complexity and load on the operator.

In the context of special operations, this initiative could significantly bolster Project Overmatch, a U.S. Navy project aimed at developing a networked warfighting system. By integrating HSA into their operations, SOF could leverage the advanced communication payloads and cybersecurity software that the DIU is developing in partnership with firms like Aalyria (Spacetime), Atlas Space Operations, Enveil, Anduril, SpiderOak Mission Systems, Amazon Web Services, Amazon's Project Kuiper, and Microsoft's Azure Space.[92] One of the primary objectives of HSA is to streamline the acquisition of imagery and intelligence for military users, including SOF units. HSA aims to enhance the relationship with commercial imagery and communications providers, offering the military, specifically SOF, the ability to make educated, individual purchases of data. This approach not only assures the data's accuracy and dependability but also motivates providers to offer high-quality analytics, thus augmenting the intelligence capabilities integral to SOF missions sets. Essentially, HSA can tighten and accelerate the decision-making process for operators and enablers when conducting sensitive, high-risk missions.

Being able to accelerate decision-making down to the tactical level is often referred to in DoD circles as "achieving decision advantage." For SOF, this simple phrase can have multiple nesting requirements. First, a flexible and adaptable space architecture must be accessible to the joint force, meaning that it can either be built or bought. This is a key issue, highlighted by the fact that there is no centralized office for data acquisition and execution of dual-use

technologies that might involve some access to sensitive government data by commercial entities.[93] Second, this infrastructure must support secure and classified communications and data transfer, thus requiring its components to meet U.S. security protocols and be resilient to adversary interdiction. Finally, this architecture must be integrated into existing networks and available to appropriate allies and partners.

The second two requirements can, and often are, at odds, forcing SOF units to accept some level of communications vulnerabilities when working with partners and allies. Recent anecdotal experiences involving less-than-secure communications in multiple areas of responsibility (AORs) suggest that while security is paramount, current protocols are not accessible or manageable downrange. The HSA is designed to fulfill this requirement, linking communication satellites across various orbits, integrating data from a wide range of sensors, and leveraging cloud computing to securely process and disseminate information from space to mission planners and operators.[94]

Overall, the strategic implications DIU's Hybrid Space Architecture are twofold. First, it highlights the capability of defense integrating with commercial industry when appropriately enabled and motivated. The barriers to entry between industry and government are permeable and perhaps exploitable for special operations. Second, and perhaps more importantly, this collaboration between public and private entities is possibly one of the single most important opportunities that the U.S. and its partners and allies have to combat threats from near-peer adversaries. Diversifying kill-chain assets to include best-in-class commercial space-based capabilities increases resilience and can impose cost on adversaries who would otherwise deny or degrade allied communications during competition or conflict.

DEFENSE ENDOGENOUS SPACE APPROACHES

It is important to note that collaborating with industry is a small but promising component of effective CJADC2. More broadly, DoD also recognized the value of independently harnessing advancements in space technologies, leading to the creation of the Space Development Agency (SDA) in 2019. This

forward-thinking agency was mandated to "move fast to put newly emerging technologies into the warfighter's hands."[95] One critical project spearheaded by the SDA was the development of the Proliferated Warfighter Space Architecture (PWSA), aiming to establish new satellite constellations. These constellations, known as the SDA transport layer, are designed to augment commercial pLEO networks and enhance the resilience, redundancy, and diversity of military communication systems.[96] This move ensures that effective communication and situational awareness are maintained in even the most demanding conditions, thereby ensuring the U.S. remains at the forefront of space innovation. This project is similar to DIU's Hybrid Space Architecture, but is designed to increase internal defense resiliency, mitigate potential supply chain vulnerabilities in commercial industry, and impose high costs on adversaries. As SDA Director Derek Tournear notes, PWSA will:

> …put up hundreds and hundreds of satellites. Now (…) our satellites are more affordable than the missiles that you need to shoot them down. So we've kind of taken that off the table. We made it to where (…) it's really difficult to shoot those satellites down just by virtue of proliferation.[97]

Both the HSA and the PWSA are examples of the U.S. military modernizing its strategies and frameworks, notably through the JADC2. This groundbreaking concept aspires to create a unified system to connect military forces and their information sharing systems, irrespective of their operating domains such as air, space, sea, land, or cyber. This connectivity enables quicker decision-making and improved situational awareness, vital aspects in modern warfare.[98] Both projects provide robust support for JADC2 by offering secure and reliable communication and data transport capabilities, even in contested and congested environments. While not SOF-specific, HSA and PWSA could provide future complementary opportunities for data collection, analysis, and promulgation to operators with their cloud computing, artificial intelligence, and autonomous command capabilities as those features mature. SOCOM's subsequent prioritization of developing these capabilities internally can accelerate implantation and adoption of these technologies.

The potential advantages of SOF-specific solutions to harness the power of pLEO constellations, HSA, PWSA, and the broader JADC2 infrastructure are significant. When paired with Multi-Domain Autonomous Systems (MDAS), these solutions could provide NSW with extended access, enhance situational awareness, and enable real-time informed decision-making during distributed maritime operations. The integration of the aforementioned frameworks is pivotal in offering robust, secure, and reliable communication networks for SOF. This digital transformation not only fortifies the existing communication infrastructures but could revolutionize 21st century military operations. The adaptability, resilience, and enhanced situational awareness provided by these integrated systems are instrumental for mission success, especially in contested environments.

As warfare evolves to become increasingly reliant on data, it is critical to focus on real-time analytics, predictive algorithms, and other data-intensive operations. These modern technologies, combined with resilient communication infrastructures, will form the bedrock for military strategies and decision-making. In an ever-evolving battlefield, where traditional communication methods can be compromised, the need for adaptive and resilient systems becomes a necessity. The U.S. Navy, and NSW in particular, can increase preparedness for future conflict by leveraging these emerging technologies and architectures across multiple domains. As the U.S. Navy and its partners and allies usher in a new era of digital, connected, and data-driven warfare, NSW has two key opportunities. First, the force can enable innovation adoption down to the unit level by equipping its people with the tools and access necessary for space-enabled operations. Second, the NSW can leverage its ability to operate in the "darkness" for strategic advantage. The next section of the paper will explore this opportunity to operate in darkness for NSW, identifying the fallacy of space as an inaccessible, doomed expanse in future conflict and suggesting avenues for NSW to leverage its unique strengths with space as a warfighting enabler.

SPACE AS A NECESSARY WARFIGHTING ENABLER

After years of "catastrophic" space scenarios briefed alongside nearly every PowerPoint presentation at the Pentagon, there is a deeply engrained assumption within the upper echelon of the NSW community, and the Navy at large, that during a conflict there will be no space assets available for use of any kind. Simply put, this assumption is overly reductionist and confuses communications degradation with communications elimination. This misunderstanding is not the fault of the U.S. Navy or even the broader defense apparatus. Early conceptions of conflict in space concerned themselves with designing small side arms that could be used in a vacuum and appropriate tactical employment similar to land warfare, often ignoring the nuances of communications and control.[99] Even when considering a possible escalatory competitive state or kinetic conflict between the U.S. and a near-peer adversary like the PRC, it is extremely unlikely that all space assets will be rendered inactive.

This outlook is not to say that space as a warfighting domain is without instability. On the contrary, scholars have identified several friction points, to include the entanglement of nuclear and conventional capabilities on space-based assets, the possibility that direct ascent anti-satellite (DA-ASAT) testing could produce substantial space debris and damage existing mega-constellations, and a dearth of agreed-upon governance for commercial and governmental space activity.[100] Furthermore, none of these complications can be directly attributed to malign intent by any space power. As Bruce Macdonald, Carla Freeman, and Alison McFarland state in their special report for the U.S. Institute of Peace, "domestic and international policymaking is hard pressed to keep up with technical advances in the (space) field."[101]

Limited normative regulation and swift technological advancements have possibly contributed to the commercial sector and not a nation-state government articulating rules and responsibilities for space development and diplomacy. Muddying the public-private Venn diagram has further entangled the U.S. with China and has resulted in common interests between these adversaries. Therefore, it is possible that the political and military risks

associated with destroying space capabilities, as well as the sheer cost required to do so, has a deterrent cooling effect on any space-based escalation in competition or conflict.

These risks present themselves in three key ways. First, it is reasonable to assume that a near-peer adversary will want to maintain access to their own satellite constellations for as long as possible to ensure speedy, accurate communications and data transfers. Therefore, it is possible that a country like China would be unwilling to accept destruction of their own space constellations just to destroy those of an enemy. Lessons learned from the Russian invasion of Ukraine in 2022 substantiate this, suggesting that even powerful nation-states are unlikely opt for the total darkness of denied or degraded communications. In order to gather intelligence, coordinate fires, deconflict engagement zones, and assess threats and battle damage, the Chinese will need to use their very own satellite systems. If non-kinetic fires are used, the resulting "high powered" signatures may render some satellites ineffective but open the door to counter-targeting of that exact same high energy jamming system.[102]

Kinetic effects are equitably imprecise as space is more densely "populated" is generally understood – even the partial destruction of proliferated mega-constellations at multiple orbital levels could create a hazardous amount of physical debris that will both grow in size and unpredictability.[103] This idea of "Kessler Syndrome" argues that it is "conceivable that some ill-planned rapid expansion in the use of low Earth orbit could produce a much more rapid increase in small debris as a result of collisional cascading."[104] Destruction of enemy space assets lacks the precision necessary to mitigate risk and presents substantial opportunities for collateral damage, thus suggesting a rational actor might forego this option and maintain some level of space communications availability in a future conflict.

The second and third presentations of risk in space operations are two sides of the same coin; they both deal with the potential use of offensive capabilities against space-based assets. The second presentation of risk has to do with the *quantity* of offensive capabilities, as it is possible that a near-peer adversary like China simply does not have enough "bullets" to threaten all space assets. More problematically, they may not desire to do so. China's

space goals are simultaneously vehicles for economic growth and crucial components of the state enterprise. Programs like those outlined in China's "Guiding Opinions of the State Council on Innovating the Investment and Financing Mechanisms in Key Areas and Encouraging Social Investment" advocate for "greater private capital to be invested in the development of civil space infrastructure, including the provision of commercial launch services," and "developing fully reusable launch vehicles, nuclear-powered space shuttles, and solar power stations to enable mining operations and manufacturing in space" as components of China's "Space Silk Road."[105]

These civil and commercial investments are significant because of the high degree of overlap between civilian and military applications in China's space sector. Since civilian investments are thus linked with defense and security in this concept of "civil-military fusion," China may not desire a conflict that would permanently endanger their access to space infrastructures that serve as the backbone for civilian financial, transportation, or telecommunications industries. In this way, space is not just a necessary warfighting enabler for China, it is also a necessary *nation-building enabler*.

The combination of commercial, civil, and military proliferation of allied satellites in low earth orbit through the advancements of private-equity or billionaire-funded space companies also means that space is now available for more users, for longer periods within the conflict, and with higher bandwidths than ever before seen. As of this writing, there are roughly 4,500 satellites in orbit, with American companies like SpaceX aggressively advocating to expand those numbers. In just the month of November 2021, roughly 38,000 new satellites were proposed to the U.S. Federal Communications Commission.[106] Removing one from a constellation requires a disproportionate amount of kinetic resources. Essentially, the bullets of space warfare are more expensive than their targets and impose substantive, decision-changing operational costs with diminishing marginal returns.

The third reason why total annihilation of space-based assets is unlikely and perhaps an unreasonable operational construct has to do with *scope* of available offensive capabilities. It is highly improbable that the Chinese will be

able to destroy all space assets in all orbits, altitudes, and complexities. These seemingly nuanced differences in each asset have compounding operational consequences, as the offensive tactics needed to destroy all these spacecrafts are extremely difficult to master and may have diminishing returns. As a 2023 Report to the Congressional Budget Office points out, "one potential advantage for constellations with many satellites is that their coverage and functionality might degrade more gradually compared with smaller constellations."[107] Additionally, pLEO satellites are more resistant to electromagnetic attack due to the complexity and rapidity of the coordinated transmitter-receiver "hand-over" happening between user terminal and quickly moving satellite, a transfer that takes place nearly every five minutes. Furthermore, the amount of power required from an uplink jammer to overwhelm a small, KU band spot beams from the relatively short distances of a low earth orbit, is much more difficult than the traditional geosynchronous orbits. These effects can be multiplied when different satellite types and functions are considered. The low earth orbit satellites may have different targeting solutions than geosynchronous orbit satellites; this is further complicated by the fact that the speeds, time limits, and payload to destroy a target vary from orbit to orbit and target to target. Unilateral total blackness is nearly impossible to achieve and would arguably play towards USSOF strengths of operating in denied and austere environments.

These offensive complications are not unique to the PRC. Top American military space leaders are doubling down on space defense, focusing on "fighting SATCOM" through a conflict.[108] Leaders refuse to "sit on their hands" during a conflict but rather make all efforts to keep SATCOM available for allied users, a sentiment that is echoed in the 2020 Defense Space Strategy Summary, which prioritizes the U.S. capability to "build a comprehensive military advantage in space" designed to leverage "on-orbit, multidomain, and cross-component operations that are fully integrated with our allies and partners."[109] American defense space professionals have taken this guidance and implemented down at the operational level, conducting similar tests and drills on a daily basis to avoid space debris collisions, a transferrable skill to an anti-satellite attack. Essentially, offense in space is much harder than a laser aimed at the starship of an enemy planet. Risk to mission and risk to force

rise when dual-use technologies, widely-proliferated assets, and blurry rules of engagement are in play. Commitment to doing space defense *well* is much easier and much less risk acceptant than playing offense *at all* against a near-peer adversary.

There is also a normative component to this decision. Despite multiple scholars listing China's revisionist or revanchist language as a break from the global order, it is clear that Chinese leadership recognize the sensitivity of their position on the world's stage. Chinese aspirations to be a world-class space power in the immediate future indicate a possible desire to position themselves as an alternative to the American way of life on the international stage and in space.[110] This is exemplified by the launch of the Tiangong Space Station and Project 921, as "the Chinese government noted in its latest white paper on space activities that China should be built 'into a space power in all respects' and use its space program to enhance its 'overall strength.'"[111] Offensive activity in space could possibly negatively impact this carefully cultivated image of the Chinese space program by generating space debris, damaging other constellations, and bluntly thwarting international norms to isolate and condemn China to the global periphery.

CONCLUSION

Prior to the advancements made in the "new space" ecosystem, DoD was forced to use antiquated, slow moving geosynchronous satellites for all assured communications in times of peace and war. This lack of a "resilient space architecture" led Joint Chiefs Vice Chair General John E. Hyten to refer to these exquisite capabilities as "big juicy targets" that represented a substantial risk to mission.[112] Luckily for American warfighters, Silicon Valley-led advancements in proliferated low earth orbit satellite constellations increased resilient communications infrastructures, and space launch capabilities have democratized and streamlined the options available to the U.S. Navy when operations require large amounts of data to be pushed to and pulled from ships operating over the horizon. Programs like Project Overmatch leverage alternate-PNT and CJADC2 concepts to enable operators at the tactical edge safely and securely. Yet, the toughest test still remains to be won: combined force integration.

Synching these technological advancements with the established norms of just U.S. SOCOM, let alone the entire conventional force, will take time, sufficient consistent resourcing from political leadership, and appropriate force design to test, evaluate, and leverage these systems for mission planning and execution. In the meantime, the U.S. and its partners and allies will still need to be able to leverage existing space-based capabilities and be able to operate in denied or degraded environments and defense communications infrastructures slowly modernize. Due to its centrality in the Space-SOF-Cyber Triad and position at the tip of the spear for INDOPACOM operational planning, NSW is ideally positioned to leverage these technologies. Furthermore, NSW is most able to operate in communications "darkness" due to years of experience during GWOT in CENTCOM in austere operational environments. SOF is more easily able to innovate with, acquire, and adopt new technologies than the conventional force and is also inherently designed to be interoperable with high level partners and allies. For NSW, space can be a critical warfighting enabler to provide operators with access and placement for future operations, if and only if it is integrated into the planning cycle properly.

Without that integration, it is possible U.S. operators and allied and partner forces will be without needed capabilities in a kinetic fight. That kind of handicap is dangerous if not irreversible. Space must be considered a critical warfighting enabler for special operations forces if the United States and its allies and partners want to attain strategic advantage over any near-peer adversary. Presuming that space will be unavailable or compromised to the point of uselessness represents a dangerous retrenchment into safe mission sets with outdated technology. U.S. SOF have the opportunity and the responsibility to leverage emerging space-based capabilities for the safety and security of the nation. They are uniquely positioned to fight and win in any domain, at any time. Space may be a vacuum, but an adversary can still scream.

CHAPTER

16

REMOTE WARFARE AND SMALLER WESTERN COUNTRIES

MAJOR CEDRIC CRANINX

Low-intensity conflict should be the domain of special operation forces (SOF) with other service components in support.[1] According to Michael Noonan's *Irregular Soldiers and Rebellious States*,[2] as a type of low-intensity conflict, irregular warfare has the features of Major Fernando Luján's "light footprints"[3] and Captain (Navy) Rob Newson's "MINFORCE."[4] Light-footprint operations often substitute for massive "boots on the ground" engagements. They instead rely "on a small number of civilian and military professionals to work patiently over many years to prevent and contain security challenges."[5] Renowned strategist and author David Kilcullen also emphasizes the importance of light, indirect, least-intrusive intervention in long-term, low-profile engagements wherever possible.[6] These notions support strategist Colin Gray's first master claim on the economy of force: "*Special Operations can achieve significant results with limited forces*."[7] Lujan asserts, "In the simplest terms possible, the light footprint is fundamentally based upon working indirectly through indigenous actors to achieve national security objectives."[8] SOF use these types of operations against non-state actors, insurgents, and criminal and terrorist networks.[9]

In the final years of the President George W. Bush's administration, a new form of "remote warfare" was pursued by the United States that involved many

of the characteristics of light-footprint operations. Mainly characterized by the use of drones in the early stages, remote warfare aims to counter threats at a distance. Moreover, the notion of remoteness denotes that militaries do not have to operate on the contact line any longer.[10] As a result, kinetic operations are carried out without exposing Western military personnel to the risks normally associated with armed conflict in a warzone.[11] Remote warfare instead focuses on "'shaping' the international security environment through technology, flexible operations, and military-to-military partnerships."[12]

The spectrum of remote warfare is very broad. It encompasses unilateral operations, partner operations, train/advise/assist, and security assistance.[13] Air support, intelligence operatives, private contractors, and SOF training teams are features of remote warfare intended to assist local forces in fighting.[14] Researchers Abigail Watson and Alasdair McKay state that this model involves the following measures:

- Supporting local security forces, either official state forces, militias or paramilitaries; for example, through the provision of training, equipment or both;
- Special operations forces, either training or sometimes even working alongside local and national forces;
- Private military and security contractors undertaking a variety of roles;
- Air strikes and air support, including unmanned aerial vehicles (UAVs) or "armed drones" and manned aircraft; and
- Sharing intelligence with state and non-state partners involved in frontline combat.[15]

Since the early 2000s, remote warfare has become a central instrument in the U.S. counterterrorism toolbox.[16] From the coalition fighting the Islamic State in Iraq and Syria (ISIS) to the saturation of Western light footprints in Niger,[17] kinetic actions are choreographed and often controlled from a distance.[18]

Under this model, military outposts and operational capabilities are being built by Western countries throughout Africa to monitor, disrupt, and contain potential threats.[19]

Following this pattern, many other Western nations have adopted the model.[20] Smaller Western countries' policy-makers engage their military in remote warfare, hoping to decrease the risk to the force, counter threats at a distance and limit budgetary costs. Problems arise, however, for smaller Western nations when they cannot access the full spectrum of remote warfare features. Due to a lack of resources, such as drones, geospatial intelligence (GEOINT), or human intelligence (HUMINT), these nations cannot or do not deploy even the minimum number of remote warfare features available when not operating under a coalition umbrella.

Executing remote warfare while lacking adequate resources increases the force's exposure to risk, jeopardizes mission success, or both. These deviations from the original remote warfare model therefore often lead to added force-protection measures and increased footprints that can adversely impact building a relationship with the population and a partnership with local forces during low-intensity conflicts.[21] Moreover, without the right deployed capabilities, smaller countries' SOF may have very limited freedom of action (FoA) and consequently may not be able to measure their remote warfare operational effectiveness. Without such measures, SOF may not receive the necessary support and funding at the strategic and political levels. This problem mainly manifests organizationally due to the hierarchical governmental and military planning and decision-making process.

Therefore, this chapter seeks to answer the question, "What forms of support make the remote warfare system effective?" by analyzing the impact of remote warfare components on operational MoEs. The study employed system dynamics modeling and simulation to analyze the effectiveness of two types of remote warfare support to a local partner: training support and intelligence support. Using insurgent force size and information availability as key measures of effectiveness (MoE) the model simulated multiple ways in which the characteristics of remote warfare may impact the dynamics of a sub-state

conflict. Data from the Islamic State insurgency case study was used to validate the model's fit over a simulated 36-month run and draw conclusions.

This research found that small Western nations should more carefully consider the proportion of different forms of remote support provided to the local partner in a conflict. Growing the partner's force size through training is ineffective if remote intelligence support is not provided. By contrast, intelligence support to a partner nation's force routinely enhances its ability to find and fix the insurgent force, reducing the latter's size and effectiveness. The study recommends three internal and one external strategic approach for SOF to collect more intelligence to more effectively help partner nations.

In the first internal approach, SOF and intelligence operatives work together under an inter-service umbrella. In the second internal approach, small Western SOF enhance their organic intelligence capability. The third internal approach represents a combination of the first two approaches. Finally, the external strategic approach stresses the importance of smaller countries joining efforts in a coalition to build partner capacity and provide a broader spectrum of remote warfare support options, most importantly, more types of intelligence.

SYSTEMS DYNAMICS MODELING AND ANALYSIS OVERVIEW

Remote warfare, at the broadest end of the spectrum, supports a local partner. That partner is often an actor engaged in an internal conflict in which two opponents confront each other for control of the political space.[22] In those conflicts, local forces, also called counter-insurgents, fight against a guerilla force called insurgents.[23] When a third-party state provides military support to a local partner's counter-insurgency, that state also becomes part of the COIN force.

To combat insurgencies effectively, it is crucial to have a clear understanding of the characteristics and capabilities of the opposing forces. Typically, insurgents have an information advantage, which means that they are better able to gather and disseminate information about their opponent's activities and objectives.

However, they often have a disadvantage in terms of the size and strength of their forces compared to counter-insurgents. Conversely, counter-insurgents typically have a force advantage, meaning that they have greater numbers and resources at their disposal. Nevertheless, they often struggle with an information disadvantage, which means that they may have limited knowledge about the insurgents' activities and objectives.

Balancing these advantages and disadvantages is essential to achieving success in COIN operations.[24] The full-scale support covers a broad spectrum of services. It is operationally effective, as evidenced by its contribution to the U.S.-led coalition militarily defeating the IS insurgency in a three-year period. Full-scale support is most effective due to the range and synergy of capabilities deployed that allow not only for a high level of intelligence, knowledge, and understanding of the OE but also a high level of protection provided by dedicated air support. Unfortunately, such comprehensive support is not achievable for countries with limited resources and risk appetites when they do not operate under a coalition umbrella.

It is therefore critical to determine how smaller Western countries' SOF can allocate their limited resources to training support and intelligence support during remote warfare to better help local partners fight insurgents. This study used system dynamics modeling and simulation to analyze the impact that these remote warfare components have in a counter-insurgency. Using force size and information availability as MOEs, the model determined the COIN size, the insurgents' size, and the COIN find and fix capability by turning on and off the training support and adding different levels of intelligence support.

In the model, there are three levels of possible intelligence support, grouped by ease of sharing. Sharing open-source intelligence (OSINT) products, unmanned aerial vehicle (UAV) images, and geospatial intelligence (GEOINT) with a partner is the minimum and easiest remote intelligence support to provide. Therefore, they are modeled as Level 1 support. Human intelligence (HUMINT) involves more risks for the agents and the sources, so it requires more risk acceptance from the supporting nation. Therefore, HUMINT is added to Level 1 inputs to constitute Level 2 support. Finally,

signals intelligence (SIGINT) is expensive and often requires a higher security classification. Therefore, SIGINT is added to the sources in Level 2 to constitute Level 3 support.

This system dynamics model was intended to demonstrate the impacts of these different types of remote warfare support provided by a Western country to a local partner force during an insurgency. Data from the Islamic State insurgency case study was used to validate the model's fit over a simulated 36-month run and draw conclusions. The results demonstrated the degree of impact on the size of the counter-insurgency, the size of the insurgency, and the counter-insurgents' find and fix capability for each type of support provided. Most importantly, the results showed which type of support is the most operationally effective in decreasing insurgency size.

FINDINGS

The remote warfare model shows the high effectiveness of intelligence support and the relative lack in effectiveness of training support when the latter is mainly focused on increasing the COIN size.

INFORMATION AS A FUNCTION OF FORCE SIZE AND MULTI-SOURCE INTELLIGENCE GATHERING

Many insurgent competition models measure the tradeoff between information and force according to various levels of conflict or stages of insurgency.[25] One of the central assumptions of such models is that the level of information available to each party is a function of the size of the insurgency and counter-insurgency effort. In this study's results, training support primarily increases the COIN size, while intelligence support dramatically increases the infor-mation component (COIN find and fix capability). These outcomes are accomplished through a synergistic effect of multiple intelligence activities including sharing intelligence with the partner, OSINT, and GEOINT (manned and unmanned aircraft included), HUMINT, and SIGINT. Information remains a function of COIN size and insurgents' size, but it is *more* a function of the added synergy of multi-intelligence provided by the remote warfare intelligence support.

IMPACT OF REMOTE WARFARE ON INSURGENCY SIZE

Within the model's variables, the maximum support is the most effective form of remote warfare in terms of decreasing insurgency size: training support and Level 3 intelligence support.

That said, intelligence support is the only type of support, to a lesser or a greater degree depending on the level, that is alone able to decrease the insurgency size. The main difference between the simulations with and without intelligence support is the capacity of the COIN force to "see" the insurgents. The analyses for the three levels of intelligence support demonstrated the relationship between an increasing find and fix capability as a result of greater intelligence support and the decreasing insurgency size. The more the COIN force can find and fix the insurgents, the more the insurgency size decreases.

However, intelligence support cannot completely defeat an insurgency on its own.[26] A complete COIN win also involves gaining control of the political environment and addressing the underlying social and political issues that gave birth to the insurgency in the first place.[27]

GROWTH IN COIN SIZE, LIMITED IMPACT OF TRAINING SUPPORT ON INSURGENCY SIZE

Finally, the growth of the counter-insurgency effort is mainly dependent on the training support provided to increase or sustain the force and reduce the force attrition rate. Still, this finding is aligned with the literature because the model shows that a growing COIN size has little to no impact on insurgency size if the insurgents are relatively invisible to COIN forces.[28] Lastly, the analysis revealed that without external intervention in the insurgent conflict, the insurgents' information advantage counterbalances their size disadvantage such that insurgency size continues to grow. Without proper intelligence, the COIN force cannot locate or target the insurgents. So only employing training support to grow a partner size produces a similar outcome to not intervening at all.

RECOMMENDATIONS FOR SMALLER COUNTRY SOF

Based on the findings of this study, when Western countries decide to support a partner nation, they should carefully consider the type of support they will provide if they want to impact the conflict. Decision-makers and SOF should recognize that training support mainly focused on growing the size of the partner force should be avoided as a stand-alone option in bilateral agreements between a small Western country and a partner nation fighting insurgents. This limited support is not operationally effective because it does not help the partner find and fix the insurgents and so does not significantly diminish the size of the insurgent forces.

Intelligence support as a stand-alone option, while not ideal compared to full-scale support, would be preferable for small countries with limited resources and a strategic culture that is averse to direct military interventions. In such cases, this approach is more operationally effective because it counterbalances the local partner's information disadvantage by increasing the COIN force's find and fix capability, thereby significantly reducing the size of the insurgent force. In the context of limited resources and budget, smaller Western countries should shift their policy from training to intelligence support, or both. If SOF must prioritize, it should direct its resources and efforts towards intelligence support instead of training support.

To do that most effectively, smaller Western countries need to generate actionable intelligence that is based on multiple sources. While major powers have the luxury to run a multi-source apparatus exclusively within SOF or the intelligence service, the interservice approach is necessary for smaller states to attain the multi-intelligence fusion level. The least expensive way for them to produce multi-intelligence today is undoubtedly by combining the three "INTs" (i.e., HUMINT, OSINT, GEOINT).

To that end, this study recommends three internal and one external strategic approach to collect intelligence to better support partner nations. The first approach proposes that SOF and intelligence operatives work together under

an inter-service umbrella. In the second internal approach, small Western SOF enhance their intelligence capability by developing a broader organic spectrum of INTs. In the third internal approach, the country opts for a combination of the first two approaches. Finally, the external strategic approach stresses the importance of smaller countries joining efforts in a coalition to build their partner capacity and provide partner nations with a broader spectrum of support options.

A LEVEL 2 INTELLIGENCE SUPPORT, MULTI-INT CONCEPT

One of the most cost-effective ways to produce multi-source intelligence is by combining three intelligence sources, or the three INTs: HUMINT, GEOINT (which includes manned and unmanned aircraft imagery and videos and OSINT). Coupled with an agreement to share intelligence with the supported partner nation, this concept has the capability to significantly impact the insurgent conflicts that smaller Western countries could be involved in. To illustrate the utility of this multi-int concept, some details about the different types of INTs are useful.

OSINT has transformed over the last decade. As Lauren Zabierek, the former Executive Director of the Cyber Project at Harvard Kennedy School's Belfer Center, has observed, the growth in data volume, variety, and velocity has been exponential.[29] The internet has become a sensor. We can easily refer to the internet as multi-int because it provides access to news, commercial satellites that can do imagery analysis, commercial signals, and snippets of audio and video and it even makes judging the veracity of human-derived information possible.[30]

HUMINT provides insight into opposing forces' intent as well as actions. Depending on the HUMINT type (i.e., clandestine, covert, or overt) and the information required, HUMINT can take time to develop because of the sources' placement and access to information. Therefore, HUMINT in many cases is less responsive to immediate needs. It remains, however, a unique capability by providing insights into the opponent's thoughts, plans, and intentions. Human sources can sit in leadership or inner circle meetings,

report on the latest enemy decisions, future locations, or pattern of life and provide unrivaled insight into what an opponent wants.

When training, advising, and assisting a partner nation, the line between human intelligence collection and security cooperation is thin due to the trust built between partners. During these operations, SOF can help confirm or deny information collected by other sources or help identify sources that the intelligence service could further exploit. Even advanced technical intelligence operations often rely to a certain extent on HUMINT-derived information and cueing in denied areas, where friendly deployed sensor arrays require proximity to the target. Therefore, HUMINT is critical for intelligence and operational synergy.

GEOINT is "information about any object – natural or man-made – that can be observed or referenced to Earth and has national security implications."[31] Geospatial intelligence "consists of imagery, imagery intelligence, and geospatial information."[32] Earth observation, UAV technologies, and AI-enabled surveillance and collection have made incredible progress in the last decade. For example, UAVs may capture long-duration, close-up full motion video. As a subset of GEOINT, activity-based intelligence (ABI), also referred to as pattern of life, involves gathering intelligence by observing behaviours that are indicative of a specific activity occurring in an area.[33] It can detect unusual behaviours or patterns that can signal the presence of an activity that is particularly relevant to friendly operations, or an imminent threat, such as individuals emplacing improvised explosive devices.[34] While aerial intelligence is the most expensive of the three INTs discussed in this study, its costs have dropped while its capacities have grown.[35] These systems enhance GEOINT collection and often achieve "persistent surveillance."[36]

The combination of these three INTs is a multi-source concept intended to build and sustain the intelligence edge necessary during a remote warfare. The combined result can give a good sense of an opponent's capabilities and intentions. It is a practical and economical way to produce actionable intelligence before sharing it with a local partner. It thus provides a small country's SOF with the necessary intelligence foundation to support a partner force in finding and fixing the insurgents in their territory.

INTERNAL STRATEGIC APPROACHES

This multi-source approach can be implemented by combining SOF and intelligence operations. The collaboration level between SOF and intelligence services varies among nations large and small. The United States and other large allied and partner nations have made great progress in intelligence sharing and collaboration since 9/11.[37] However, the smaller Western countries have not followed this trend. Small country SOF would do well to study different strategic approaches to the collection and sharing of intelligence to maximize the effectiveness of intelligence support in the context of resource-constricted remote warfare.

The first approach would consist of intelligence operatives and SOF supporting each other and pursuing the same objectives. Both actors would enable each other, cover each other's deficiencies, and would work towards the same national strategic objective, in this case related to the military defeat of an insurgency in a partner country. As an intel collection asset, SOF would participate in the current intelligence-gathering apparatus. A second approach would be to broaden SOF's own collection spectrum, develop organic capabilities and pool its intelligence with the intelligence services. A third approach would be a combination of the first two, ensuring the highest flexibility in terms of ways and means to reach intelligence end states. This inter-service approach encourages seamless coordination and information sharing, allowing for a more holistic understanding of the operational environment. By leveraging the expertise and capabilities of both entities, a more robust and efficient intelligence apparatus can be established.

Whether the intelligence service and SOF cooperate to provide actionable intelligence or whether SOF creates new capabilities and fills that gap, these paths will offer suitable solutions. All these approaches might be different in many aspects when looking at costs and benefits, at the necessary intelligence capability-building within the SOF community, or at the necessary structural inter-service collaboration, but they are all effective when it comes to gaining a better understanding of the operational environment, sharing it with a partner and effectively helping them in decreasing the size of their enemy.

The optimal solution, in terms of quality, quantity, and flexibility, is taking the third approach in which both SOF and intelligence operatives work towards the same objectives, but the overall intelligence capabilities deployed are superior due to SOF efforts in enhancing its own. It is also the best way to guarantee the multi-source intelligence benefits in support of a partner nation that is unable to find and fix its enemy during an insurgent/counter-insurgent competition. That said, in the limited resource context of smaller Western countries, employing whatever method enables finding and fixing insurgents during remote warfare should be the primary concern.

EXTERNAL STRATEGIC APPROACH

Multiple European nations often deploy to the same country, and each signs bilateral agreements to help the same supported country. Rather than each country individually offering support that meets its diplomatic, political, and economic standards, all parties should unite their efforts within a single alliance. This coalition would provide comprehensive support encompassing all types of support, most importantly intelligence support.

As observed in the Remote Warfare simulation, on the one hand, intelligence support is operationally effective. It is logical that counterbalancing the COIN disadvantage by providing COIN forces with actionable intelligence helps them better find and fix insurgents for operational effectiveness. On the other, something completely overlooked by the small Western European countries is another of this study's findings, i.e., the lack of effectiveness of training support focused on growing a partner force size to help them fight against insurgents. Here, it is important to distinguish the building partner capacity (BPC) often applied by smaller Western countries from the BPC used by major powers. For example, the BPC framework applied by the United States is an operational and fiscal authority to help build a partner's capacities across the different joint functions and to implement them by supporting the partner through their Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Policy.[38] Few smaller countries are able to provide the full capacity employed by the United States, such as persistent surveillance drone ISR (Intelligence, Surveillance, Reconnaissance) coverage. Due to

the relatively limited resources available, smaller countries mainly support training.[39] By providing their partners only training, small Western countries focus on increasing the COIN force size but too little on their effectiveness at finishing insurgents, and not at all on their find and fix capability.

Because of this tendency to provide more training support than intelligence support, discrete bilateral agreements by small countries usually result in a dearth of intelligence support. Most Western countries have bilateral agreements with African countries to support them by providing training to their troops. For example, many Western countries are involved in Niger. Whether their involvement is called capacity building, providing or guaranteeing security, or contributing to military education, it is often training support or some form of it that is provided.[40]

Among the European countries contributing to a find and fix capability in Niger are Germany, which is providing surveillance drones, and Denmark, which is providing intelligence units.[41] On top of the EU mission, five EU member states have bilateral agreements with Niger and support the same partner mainly with training. Meanwhile, Belgian SOF coordinate the SOF activities of other countries (i.e., United States, Canada, Italy, Germany, Belgium) with Nigerien demands.[42] There is not enough unclassified data to argue whether these supporting countries are merely growing the partner force size or increasing its overall effectiveness at finishing insurgents. In any case, Figure 16.1 shows that while Western countries contribute (albeit in an unbalanced way) to different forms of train-and-equip missions, there is little intelligence support provided.[43]

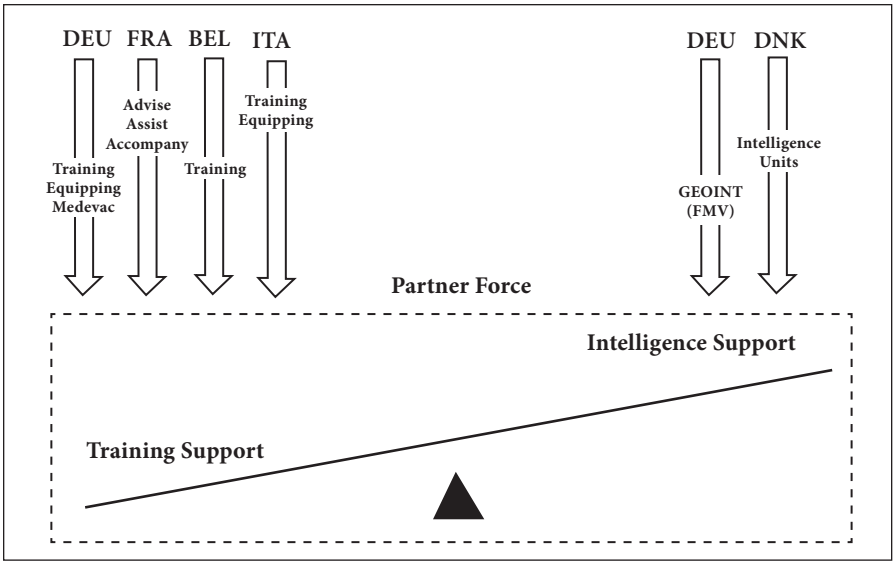


FIGURE 16.1 – Multiple Bilateral Agreements with a Partner Force and the Disequilibrium between Training Support vs Intelligence Support[44]

The result of this imbalance is far from achieving something comparable to the U.S.-led coalition in Iraq in terms of the full spectrum of support provided. There are obviously budget and resource constraints that the U.S.-led coalition did not face, but the main question is, are small Western nations optimizing their engagement, not only bilaterally, but as a whole (i.e., as EU members)?

Instead of each providing a satisficing support that meets its diplomatic/political/economic criteria, to provide sufficient intelligence support during remote warfare and thereby efficiently impact the conflict, small Western nations should combine their efforts under one alliance, a mosaic of supports. This approach would be a unique coalition offering the maximum support as defined in the model. A framework like the U.S. BPC, with its provision of complete ready-to-deploy capacities, would enhance the COIN finish component and the COIN find and fix component. Figure 16.2 shows that a coordinated spectrum of support under a coalition can provide a BPC framework and a better equilibrium between training and intelligence support.

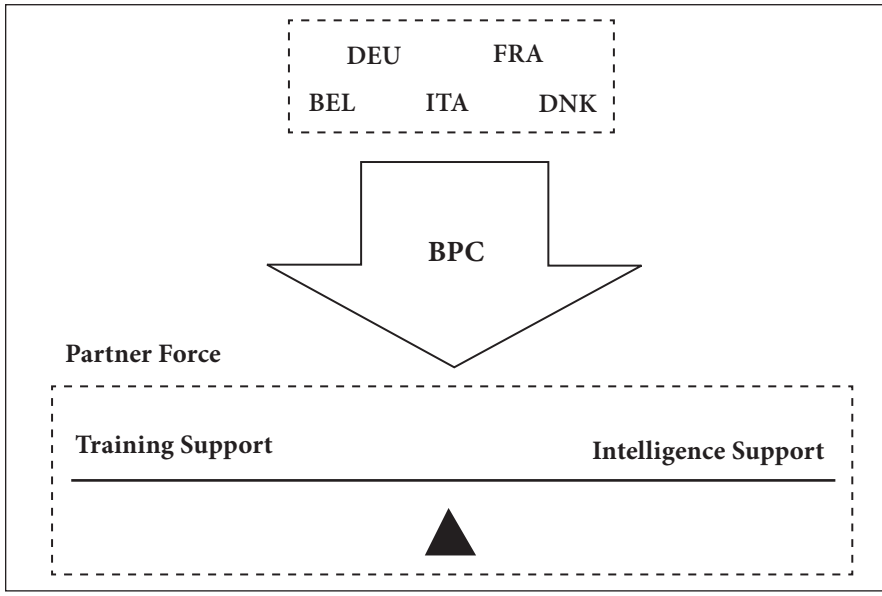


FIGURE 16.2 – Streamlined BPC under a Coalition and the Equilibrium between Training Support and Intelligence Support

There would be multiple challenges associated with such a coalition. An obvious challenge would be to align the operational objectives with each coalition member's own security objectives. These alignments are crucial for participation and funding. However, no such challenge is too great to overcome. Belgium and the Netherlands operated under a binational Special Operations Task Group (SOTG) in Iraq during Operation Inherent Resolve (OIR). In 2018, Belgium, Netherlands and Denmark signed a Memorandum of Understanding for the creation of a Composite Special Operations Component Command (C-SOCC) to participate in the NATO Response Force (NRF).[45] These cases show that smaller Western states can reconcile security objectives and reach successful agreements.

Smaller Western countries desiring to apply the remote warfare model should consider forming coalitions to increase the number of remote warfare capabilities, most importantly, intelligence synergy, to provide supported partner nation forces with greater FoA, improved MoE, increased situational awareness, and improved risk analysis. This streamlined intelligence and

operational synergy could help the supported partner nation grow its force size but also significantly improve its coefficient of effectiveness and overcome an information disadvantage by finding and fixing the insurgents and reducing their force size and influence.

CONCLUSION

Today, the concept of remote warfare means that Western countries supporting a partner nation no longer need to operate directly on the front lines. However, smaller Western nations face challenges when they lack access to the full range of remote warfare capabilities. Without resources like air support, GEOINT, or HUMINT, these nations cannot deploy even the minimum remote warfare features. Unfortunately, the available means define how small Western countries are willing to help partners, whether that assistance impacts the sub-state conflicts or not. Executing remote warfare with limited resources often leads to training support focused on increasing a partner force size. Conducting remote warfare without adequate resources can jeopardize mission success or be inefficient.

To address these problems, a system dynamic model was used to examine the effects of training support and intelligence support on COIN and insurgent forces to assess remote warfare's effectiveness in insurgent competitions. Based on the assumption that insurgents have an information advantage and a force (size) disadvantage and that counter-insurgents have an information disadvantage and a force advantage, the model showed the impact of opponents' sizes and available information on the outcome of the conflicts.

The study found that training support bolsters a partner force's size advantage, while intelligence support balances a partner force's information disadvantage. Balancing their information disadvantage and enhancing a partner's ability to find and fix insurgents significantly decreases the insurgency size. Conversely, reinforcing a partner force size advantage does not substantially affect insurgency size. However, by shifting the allocation of their limited resources from training support to intelligence support during remote warfare, smaller Western countries could better help local partners fighting insurgents.

The study proposes a set of strategic approaches, both internal and external, to augment data collection, enhance situational awareness, and effectively assist partner nations. The first internal approach involves empowering small Western SOF to bolster their intelligence capabilities. The second internal approach emphasizes close collaboration between SOF and intelligence operatives, operating under a unified inter-service umbrella. The third internal approach represents a fusion of the previous two approaches. It entails combining the efforts of small Western SOF with intelligence operatives under an inter-service framework. This integrated approach harnesses the strengths of both entities and maximizes their collective impact.

Lastly, the external strategic approach emphasizes the significance of smaller countries joining a coalition to strengthen partner capacity. By forming alliances and pooling resources, these nations can provide a broader spectrum of support options, particularly an expanded array of intelligence capabilities. This collaborative effort enhances the collective intelligence infrastructure and enables more effective assistance to partner nations. Overall, implementing these strategic approaches, both internally and externally, will facilitate the acquisition of actionable intelligence, allow partner nations to receive more effective forms of support, and increase the effectiveness of smaller Western countries' remote warfare, ultimately fostering greater security and stability.

These findings regarding how to maximize remote warfare operational effectiveness are crucial in persuading military leadership to advocate for the adoption of more SOF intelligence capabilities and an inter-service SOF/intelligence service approach to civilian bureaucrats at the national level. The findings should help them recognize the costs and benefits when considering the type of support, they aim to provide to local partners.

CHAPTER

17

WHO YOU GONNA CALL? THE STRATEGIC UTILITY OF SOF

COLONEL (RETIRED) BERND HORN

The military has always been a key instrument of national power. Its strategic utility for defending the nation and furthering national interest using direct military force or by assisting friends, allies, coalitions and/or international organizations has earned it a voice in national security policy formulation and implementation.[1] The three traditional services, the Navy, Army and Air Force, have for a long time been recognized as key players in this strategic context. The new millennium, particularly as a result of the terrorist attack on the Twin Towers of the World Trade Center on September 11, 2001 (9/11), has added SOF to that list of strategic players. Much like the theme song of the pop culture film *Ghostbusters* that asks the rhetorical question, "Who you gonna call?" in the new dynamic, complex and ambiguous security environment, SOF has earned itself a place in the rolodex of most political and military decision-makers.

The ascendency of SOF in the post 9/11 security environment, where SOF has played key roles in the counter-insurgencies in Afghanistan and Iraq, as well as in the "global war on terror," has prompted scholars, military analysts and practitioners to generate new concepts to describe SOF's strategic relevance and saliency. Specifically, "SOF Power" and "Force of Choice" have emerged as common terminology in the defence community. In fact, it is precisely

because of SOF's strategic utility that these new perspectives on SOF are well deserved and arguably will continue into the foreseeable future.

Indeed, SOF have evolved constantly over time. The birth of modern SOF is generally accepted as having started in the Second World War. At the time, SOF was generally defined as consisting of "special men, special training and special missions." Central to the evolution of SOF was the fact that they were normally marginalized by the larger military institution until crisis, or a gap in military capability, was experienced.[2] Then, normally due to champions in high ranking political and/or military leadership and command appointments, SOF were relied on to respond to the new threat or circumstances until, as a minimum, a conventional solution could be prepared, the crisis passed, or the requirement transitioned to a designated SOF capability (e.g. counterterrorism). Not surprisingly, over the Cold War and subsequent post-Cold War eras, SOF continually evolved to match the constantly changing security environment, which morphed based on global shifts and societal changes.

As a result, SOF's current structure in the post-9/11 world is a dramatic departure in form and substance from their Second World War roots. A Canadian definition of SOF is telling:

> Special Operation Forces are organizations containing specially selected personnel that are organized, equipped and trained to conduct high-risk, high value special operations to achieve military, political, economic or informational objectives by using special and unique operational methodologies in hostile, denied or politically sensitive areas to achieve desired tactical, operational and/or strategic effects in times of peace, conflict or war.[3]

Encapsulated within the definition is the key to SOF's strategic utility in the contemporary operating environment. SOF provide the government with a wide range of cost efficient and effective capabilities and options outside of the normal military context and capability set. Their ability to produce on short notice, courses of action in a number of domains, regardless of location, desirable outcomes, with a high probability of success, give them great saliency to political and military decision-makers. As the internationally renowned

strategist Colin Gray, asserted, "special operations forces are a national grand-strategic asset: they are a tool of statecraft that can be employed quite surgically in support of diplomacy, of foreign assistance (of several kinds), as a vital adjunct to regular military forces, or as an independent weapon."[4]

Notwithstanding Gray's statement, the true test of strategic utility is what an organization contributes to national power and the ability to project or defend national interests. Strategy in essence is about ends (objectives), ways (courses of action) and means (resources). Military strategy specifically is commonly understood to mean the application of, or threat of the use of, military force to achieve political ends. Therefore, for SOF to be a "force of choice" or to demonstrate "SOF Power," means that SOF must have substantive value in the exercise of national interest. In short, they must deliver capability complementary to traditional conventional capabilities delivered by the three services and they must expand the option space for political and/or military decision-makers.

Most would agree, based on events around the world in the last decade or so that SOF have demonstrated this capacity. They have achieved success through the nature of their characteristics, operating imperatives and the emphasis SOF places on the training and education of their personnel.[5] In total, these factors produce SOF capability, or what many examining the subject call "SOF Power."

In essence, SOF have been able to demonstrate their strategic utility through their ability to deal with crisis in a timely and responsive manner, usually through innovation and adaptation.[6] Central to this capability are individuals with the cognitive dexterity and agility to assess a situation, often with incomplete information and/or in conditions of ambiguity and chaos, and devise creative solutions not constrained by doctrine or convention. But, in a more macro sense, "SOF Power" speaks to SOF's ability to provide government:

1. High readiness, low profile, task-tailored Special Operation Task Forces (SOTFs) and/or SOF Teams that can be deployed rapidly, over long distances and provide tailored proportional responses to a myriad of different situations;

2. Highly trained technologically enabled forces that can gain access to hostile, denied, or politically sensitive areas;

3. Discreet forces that can provide discriminate precise kinetic and non-kinetic effects;

5. A deployed capable and internationally recognized force, yet with a generally lower profile and less intrusive presence than larger conventional forces;

6. An economy of effort foreign policy implement that can be used to assist coalition and/or allied operations;

7. A rapidly deployable force that can assess and survey potential crisis areas or hot spots to provide "ground truth" and situational awareness for governmental decision-makers;

8. A highly trained, specialized force capable of providing a response to ambiguous, asymmetric, unconventional situations that fall outside of the capabilities of law enforcement agencies (LEA), conventional military or other government departments (OGDs);

9. A force capable of operating globally in austere, harsh and dangerous environments with limited support. SOF are largely self-contained and can communicate worldwide with organic equipment and can provide limited medical support for themselves and those they support;

10. A culturally-attuned SOTF or SOF team that can act as a force multiplier through the ability to work closely with regional civilian and military authorities and organizations, as well as populations through Defence, Diplomacy and Military Assistance (DDMA)/Security Force Assistance initiatives;

11. A force capable of preparing and shaping environments or battle spaces (i.e. setting conditions to mitigate risk and facilitate successful introduction of follow-on forces); and

12. A force able to foster inter-agency and inter-departmental cooperation.

Notwithstanding the strengths and capabilities of SOF, it must be noted that, in accordance with the "fifth SOF Truth," most special operations require non-SOF assistance.[7] In other words, in no way should SOF be seen as a "silver bullet." Despite SOF's attributes and characteristics, they rely on conventional forces to assist in most of their mission sets either through supporting functions, particularly combat enablers that are not already integrated into a standing task forces (e.g., airlift, fires, Intelligence, Surveillance, Reconnaissance (ISR)), or with combat forces (e.g., follow-on forces). As such, SOF are simply another tool in the government's military "toolbox." They complement and support the nation's conventional military capability. Although able to work independently, SOF rely on, enable and work in close cooperation and coordination with, the three traditional services.

In sum, SOF provide significant strategic utility in that they can provide political and military decision-makers with a myriad of timely, precise and tailored options in response to a complex, chaotic and ambiguous strategic contemporary operating environment. The high readiness posture, small footprint, skill level and deployability of SOTFs and SOF Teams allow for a rapid and determined response, domestically or internationally. SOF have also served as a catalyst to unify, extend the reach and maximize the effects of other instruments of national power. In the end, SOF have consistently proven to be a strategic resource that provides political and military decision-makers with a wide range of precise kinetic and non-kinetic options to deter, pre-empt, disrupt, react to or shape strategic or operational effects domestically or abroad. Importantly, SOF represent a highly trained and educated, adaptive, agile-thinking force capable of dealing with the threat(s) not yet identified. As such, SOF possess the ability to provide, and have shown their effectiveness in providing, substantive value to advancing national interests.

CONCLUSION

DR. PATRICIA J. BLOCKSOME
& COLONEL (RETIRED) BERND HORN

The purpose of this book was to examine the concept of threat and how Special Operations Forces (SOF) and Special Operations (SO) have, and continue to, address new and emerging perils to national and global security. This examination is particularly relevant in the current and future security environment. In order to do so, the contributions to this edited volume were organized into three sections: Part I presented an overview of SOF/SO through a historical lens, Part II analyzed current threats and Part III discussed how SOF/SO might respond to some of the new, emerging, dynamic and ambiguous threats.

Part I focused upon the common theme of how SOF/SO typically arise as a product of their security environment, as war or conflict provides a demand for units with specialized skills and capabilities not present in conventional military forces. The chapters revealed that SOF/SO evolve and are supported due to requirements arising from crises and capability deficiencies of existing conventional military forces. As a result, they are generally not planned for in advance. Indeed, there appears to be a natural cycle in which necessity breeds the invention of a particular type of SOF/SO, which is then quickly built and employed successfully. However, once the crisis is past, and the capability gap is no longer essential, the historical record suggests that the support, funding, and billets for SOF/SO tend to decrease until the point at which a new demand for specialized competence arises. This pattern existed until the creation of U.S. Special Operations Command (USSOCOM) at which point, now masters of their own destiny, U.S. SOF were able to demonstrate their strategic utility. SOF were then in ascendency. In the aftermath of 9/11, SOF cemented their status as an invaluable military capability and earned themselves the moniker "force of choice."

This historic cycle of waxing and waning support for SOF/SO led into Part II, where attention was turned to contemporary and emerging threats which may require the use of SOF/SO. The discussion of threats in this section highlighted how the security environment has changed since the end of the long wars in Afghanistan and Iraq, the start of open warfare in Ukraine, and the rising hostilities surrounding Taiwan. These chapters provided insight into imminent challenges facing SOF. The list of challenges is long, including strategic competition in all its diverse aspects. Threats include adversarial information and influence operations focused on civilian populations, the utilization of non-military and mercenary personnel, risks from newer domains such as space and cyber, novel technologies which impose new risks to current operating procedures, and economic forms of warfare.

The threats identified in Part II may inform what requirements may arise in the near-term future for SOF/SO capabilities. If the historical cycle continues, past mission sets such as counterterrorism and counter-insurgency may be superseded by escalating new demands for new skills. Therefore, following this discussion of existing and future threats, the chapters in Part III analyzed where and how SOF/SO may be required in the future.

A number of possible response options for SOF/SO were presented in the final section of this book. As Major Christopher Boss argues, SOF can provide a critical incubator for adaptive responses to new threats, serving as a source of military institutional expertise while also providing space for innovative behaviours that may lead to new capabilities. This echoes the point made by Colonel (retired) Bernd Horn in the first section of the book, that SOF provide flexible, agile responses to a range of threats, which ultimately provide strategic decision-makers options which would otherwise be unavailable. Importantly, Part III examined several emerging and potential capabilities, including national resistance and resilience efforts; cyber and space domain SOF and SO; and technologically-enabled remote warfare. Ultimately, the ability of SOF to adapt and evolve in response to threats derived from an ever-changing security environment means that SOF/SO will continue to provide strategic utility on the world stage.

Overall, this edited volume offers diverse perspectives, built on the history of SOF/SO, of how to assess and respond to current and emerging threats in the international security environment. As SOF envision the future and develop plans and strategies for the use of SO, our hope is that this volume will help to inform debate and analysis for both practitioners and academics on the roles, missions, and effectiveness of SOF/SO in the current strategic environment.

We are grateful to all of the authors who contributed to this edited volume and we hope that their efforts provide the reader with useful insights about the vital roles, from past, to current, to the future, that SOF/SO perform.

ENDNOTES

FOREWORD

1 The VUCA concept was more fully exposited later, in Herbert F. Barber, "Developing Strategic Leadership: The US Army War College Experience," *Journal of Management Development,* Vol. 11, no. 6 (June 1992): 4-12.

2 Winston S. Churchill, *The Second World War,* Vol. I, *The Gathering Storm* (Boston: Houghton Mifflin Company, 1948), iv-v.

INTRODUCTION

1 Department of Defense, *Special Operations Forces Reference Manual, Fourth Edition* (Tampa, FL: JSOU Press, 2015), A8.

2 Ibid., A9; and NATO, *AJP-3.5 Allied Joint Doctrine for Special Operations* (Brussels: NATO Standardization Agency, 2009), Lex 5. A Canadian 2009 doctrinal publication defined SOF as "organizations containing specially selected personnel that are organized, equipped, trained and educated to conduct high-risk, high value special operations to achieve military, political, economic or informational objectives by using special and unique operational methodologies in hostile, denied or politically sensitive areas to achieve desired tactical, operational and / or strategic effects in times of peace, conflict or war." Canada, *Canadian Special Operation Forces Command. An Overview* (DND: Ottawa, 2008), 7.

CHAPTER 1

1 The losses at Dunkirk for the British Expeditionary Force amounted to 68,111 killed, wounded, or taken prisoner. Equally significant, the British left behind 2,472 guns, 63,879 trucks, 76,000 tons of ammunition and 600,000 tons of fuel and supplies. The RN lost 243 ships (out of more than 1,000 engaged). See Christopher Hibbert, "Operation Dynamo," *History of the Second World War*, Part 6, 164; Cesare Salmaggi and Alfredo Pallavisini, *2194 Days of War* (New York: Gallery Books, 1988), 4 June 1940; I.C.R. Dear, ed., *The Oxford Companion to World War II* (Oxford: Oxford University Press, 1995), 312-313; and A.J. Barker, *Dunkirk: The Great Escape* (London: J.M. Dent & Sons Ltd., 1977), 224. Exact numbers vary between these sources and others, but they all reflect the general magnitude. A major problem with determining numbers is the actual categorization / description of weapons and equipment.

2 John Parker, *Commandos. The Inside Story of Britain's Most Elite Fighting Force* (London: Headline Book Publishing, 2000), 15.

3 Cecil Aspinall-Oglander, *Roger Keyes. Being the Biography of Admiral of the Fleet Lord Keyes of Zeebrugge and Dover* (London: Hogarth Press, 1951), 380.

4 Ibid., 380. Vice-Admiral Lord Louis Mountbatten put it in simpler terms. He declared, "We cannot win this war by bombing and blockade alone." Cited in in John Terraine, *The Life and Times of Lord Mountbatten* (London: Arrow Books, 1980), 83.

5 Churchill, *Their Finest Hour*, 243.

6 Ibid., 246-247. See also Colonel J.W. Hackett, "The Employment of Special Forces," *Royal United Service Institute* (henceforth RUSI), Vol. 97, no. 585 (February 1952): 28.

7 Memorandum, "Memorandum on the Re-Organization of the Commandos," n.d., 1. UK National Archives (NA), WO 201/731.

8 Hugh McManners, *Commando. Winning the Green Beret* (London: Network Books, 1994), 7; and "Commandos," *Canadian Army Training Memorandum* (*CATM*), no. 20 (November 1942): 20.

9 Colonel D.W. Clarke, "The Start of the Commandos," 30 October 1942, 2. NA, DEFE 2/4, War Diary Combined Operations Command (COC).

10 "Early History - Interview with Colonel Dudley Clark," 30 October 1942. NA, DEFE 2/4, War Diary COC; Brigadier Peter Young, *Storm from the Sea* (London: Wrens Park, reprint 2002), 8; *Combined Operations*, 4; Parker, *Commandos,* 19-21; Brigadier John Durnford-Slater, *Commando* (Annapolis: Naval Institute Press, reprint 1991), 14.

11 "Hand-out to Press Party Visiting The Commando Depot Achnacarry, 9-12 January 1943," 2. NA, DEFE 2/5, War Diary COC [henceforth "Hand-out"].

12 "Hand-out," 2; and Brigadier Peter Young, *Commando* (New York: Ballantine Books, 1969), 12.

13 "Hand-out," 2. Each Commando had a HQ (consisting of 36 all ranks) and ten troops each consisting of three officers and 47 other ranks (ORs).

14 Charles Messenger, *The Commandos 1940-1946* (London: William Kimber, 1985), 411.

15 "Notes on Commando Training," 1 November 1942, para 5. NA, DEFE 2/4, War Diary, COC.

16 Ibid., paras 1-18; *Combined Operations*, 6-8; and Saunders, *The Green Beret*, 36-38, 41-42.

17 Young, *Commando*, preface.

18 Churchill, *Their Finest Hour*, 467.

19 See Hilary St. George Saunders, *The Green Beret. The Story of the Commandos 1940-1945* (London: Michael Joseph, 1949); *Combined Operations. The Official Story of the Commandos* (New York: The Macmillan Company, 1943); Peter Wilkinson and Joan Bright Astley, *Gubbins and the SOE* (London: Leo Cooper, 1997), 50-68; John Parker, *Commandos. The Inside Story of Britain's Most Elite Fighting Force* (London: Headline Book Publishing, 2000); Brigadier John Durnford-Slater, *Commando* (Annapolis: Naval Institute Press, reprint 1991); Brigadier Peter Young, *Commando* (New York: Ballantine Books, 1969); Brigadier

T.B.L. Churchill, "The Value of Commandos," *RUSI*, Vol. 65, no. 577 (February 1950): 85; Tony Geraghty, *Inside the SAS* (Toronto: Methuen, 1980); and Charles Messenger, *The Commandos 1940-1946* (London: William Kimber, 1985).

20 See Bernd Horn, *A Most Ungentlemanly Way of War: The SOE and the Canadian Connection* (Toronto: Dundurn, 2016).

21 "Precis of a Memorandum by Commander 1 Airborne Corps on the Value and Future Use of SAS Regiment," 1. NA, WO 193/705, "Future of SAS Regiment."

22 Emphasis of underlining is in the original report.

23 "Precis of a Memorandum by Commander 1 Airborne Corps…," 1.

24 Ibid., 2.

25 Aaron Bank, *From OSS to Green Berets: the birth of Special Forces* (Novato, CA: Presidio, 1986), 147.

26 Michael E. Haas, *In the Devil's Shadow* (Annapolis, Maryland: Naval Institute Press, 2000), 11. This book is an excellent source for a detailed account of SOF actions in the Korea War.

27 The CIA program in Korea consisted of three specific missions:

a. Special Action Teams - infiltrated by air and sea to conduct hit and run raids intended to acquire North Korean documentation and local-area intelligence;

b. Special Mission Groups - conducted amphibious commando raids for purposes of intelligence collection, kidnapping of local officials and sabotage along the eastern coast; and

c. Resistance Cadre - organized into small cells with the mission of establishing resistance movements in North Korea.

28 This pitted FEC (the military) squarely against the CIA who were actually running large partisan forces themselves under the control of the Joint Advisory Commission – Korea (JACK). FEC's intent for the partisan / guerrilla forces was:

a. Defend Eight Army's left flank and divert approximately 150,000 communist troops away from the main line of resistance;

b. Sabotage enemy supplies, communications, port, road, and railroad facilities;

c. Gather and forward intelligence concerning the enemy order of battle, troop movements, supply routes, gun positions, and military installations; and

d. Support the defense of strategic partisan-held islands. Haas, 53.

29 The Royal Marine Commandos and UDT frogmen were combined into an ad hoc Special Operations Group. Their primary mission was destroying the vulnerable coastal rail line in North Korea that was the primary logistical lifeline for enemy forces operating in the south. They also conducted beach reconnaissance.

30 Haas, *In the Devil's Shadow*, 82.

31 See Ken Connor, *Ghost Force* (London: Orion, 1998), 13-14; Anthony Kemp, *The SAS. Savage Wars of Peace 1947 to the Present* (London: Penguin, 2001), 37-41; and Adrian Weale, *Secret Warfare* (London: Coronet, 1997), 145.

32 See Thomas K. Adams, *US Special Operations Forces in Action. The Challenge of Unconventional Warfare* (London: Frank Cass, 1998), 47, 56; Mark Lloyd, *Special Forces. The Changing Face of Warfare* (London: Arms and Armour, 1995), 117-119; and Charles M. Simpson III, *Inside the Green Berets. The Story of the US Army Special Forces* (New York: Berkley Books, 1984), 35.

33 See Simpson, *Inside the Green Berets*, 35-54; Weale, *Secret Warfare*, 147-148; and Joseph Nadel, *Special Men and Special Missions* (London: Greenhill Books, 1994), 33-34.

34 See Geraghty, *Inside the SAS*, 23-39; and Kemp, *The SAS. Savage Wars…*, 15-35.

35 See Kenneth Macksey, *Commando Strike: The Story of Amphibious Raiding in World War II* (London: Leo Cooper, 1985), 208; Conner, *Ghost Force*, 54-55, 84-85; Kemp, *The SAS. Savage Wars…*, 38 and 84-86; and Geraghty, *Inside the SAS,* 49.

36 See John A. Nagl, *Learning to Eat Soup with a Knife* (Chicago: University of Chicago Press, 2005), 59-114; Michael Asher, *The Regiment* (London: Penguin, 2008), 293-448; Geraghty, *Inside the SAS*, 23-85; Kemp, *The SAS. Savage Wars…*, chapters 2, 4-6; Conner, *Ghost Force*, 56-262; Robin Neillands, *In the Combat Zone. Special Forces Since 1945* (London: Weidenfeld and Nicolson, 1997), 105-154; Peter Dickens, *SAS The Jungle Frontier* (London: Arms and Armour Press, 1983); and David Charters and Maurice Tugwell, *Armies in Low-Intensity Conflict* (New York: Brassey's 1989).

37 See Colonel Bernd Horn, "Love 'Em or Hate 'Em: Learning to Live with Elites," *Canadian Military Journal*, Vol. 8, no. 4 (Winter 2007-2008): 32-43.

38 Jon E. Lewis, *The Mammoth Book of Covert Ops* (Philadelphia: Running Press, 2014), 360.

39 See Robert M. Gillespie, *Black Ops, Vietnam. The Operational History of MACVSOG* (Annapolis, MD: Naval Institute Press, 20011); Colonel Scott Crerar, "The Special Force Experience with the Civilian Irregular Defence Group (CIDG) in Vietnam," in Bernd Horn, Paul B. de Taillon, and David Last, eds., *Force of Choice: Perspectives on Special Operations Forces* (Kingston: McGill-Queen's Press, 2004), Chapter 5; Robin Moore, *The Green Berets* (New York: Ballantine, 1965); 99-119; and Susan Marquis, *Unconventional Warfare. Rebuilding US Special Operations Forces* (Washington, DC: Brookings Institutions Press, 1997), 14-20.

40 Alan & Frieda Landau, *US Special Forces* (Osceola, WI: MBI Publishing Company, 1992), 288-295; and Marquis, *Unconventional Warfare*, 20-33.

41 See John L. Plaster, *SOG* (New York: Onyx, 1997); Richard H. Shultz, *The Secret War Against Hanoi. The Untold Story of Spies, Saboteurs and Covert Warriors in North Vietnam* (New York: Perennial, 2000); and Adams, chapters 4 & 5.

42 John D. Lock, *To Fight with Intrepidity. The Complete History of the US Army Rangers* (New York: Pocket Books, 1998), 330-438; and Landau, *US Special Forces*, 32-33.

43 D.M. Horner, *SAS Phantoms of the Jungle. A History of the Australian Special Air Service* (Nashville: The Battery Press, 1989), 170-391; Weale, 194-200; and Neillands, *In the Combat Zone*, 152-153 and 178-181.

44 See Weale, *Special Warfare*, 192-194; William H. McRaven, *Spec Ops. Case Studies in Special Operations Warfare: Theory and Practice* (Novato, CA: Presidio, 1995), 287-331; and Benjamin F. Schemmer, *The Raid. The Son Tay Prison Rescue Mission* (New York: Ballantine Books, 2001).

45 Simpson, *The Green Berets*, 72-73.

46 Plaster, *SOG*, 251, 267 and 355. SEALs had a kill ratio of 50:1 (Nadel, 75). USMC reports indicated that their Force Recon soldiers had a kill ratio of 38:1 as compared to the USMC overall kill ratio of 8:1. Neillands, *In the Combat Zone*, 38.

47 Ibid., 357.

48 Cited in Adams, *US Special Forces*, 70, 148. See also Michael Duffy, Mark Thompson, and Michael Weisskopf, "Secret Armies of the Night," *Time,* Vol. 161, no. 25 (23 June 2003).

49 Captain Roger Crossland stated, "Naval spec ops after Vietnam War were the bottom of the food chain." He stated seniors made public statements that they would never use spec ops again. He recalled, there was "hardly any money for gas" and that they were "Very dark times." Captain Roger Crossland, "What kinds of Special Forces Do we Need and how do we support them?" at West 2006 Conference, 11 January 2006, San Diego.

50 Marquis, *Unconventional Warfare*, 4, 35, 40 & 78. Special Forces manning went from the tens of thousands to 3,600 personnel.

51 Ibid., 68.

52 Ibid., 160.

53 See Peter Harclerode, *Secret Soldiers. Special Forces in the War Against Terrorism* (London: Cassell & Co, 2000); Paul de B. Taillon, *The Evolution of Special Forces in Counter-Terrorism* (Westport: Praeger, 2001); Benjamin Netanyahu, *Fighting Terrorism* (New York: Noonday Press, 1995); Christopher Dobson and Ronald Payne, *The Terrorists* (New York: Facts on File, 1995); and Brian MacDonald, ed., *Terror* (Toronto: The Canadian Institute of Strategic Studies, 1986).

54 Harcelrode, *Secret Soldiers*, 51.

55 A few examples include: the storming of the Turkish embassy by three Armenian men on March 12, 1985 (Armenian Revolutionary Army); the paralyzation of the Toronto public transit system on April 1, 1985, as a result of a communiqué sent by a group identifying itself as the Armenian Secret Army for the Liberation of our Homeland in which they threatened death to passengers of the transit system; and the downing of an Air India flight off the coast of Ireland on June 23, 1985, killing 329 people as a result of a bomb that was planted prior to its departure from Toronto's Pearson International Airport.

56 See Major-General Ulrich Wegener, "The Evolution of Grenzschutzgruppe (GSG) 9 And the Lessons of 'Operation Magic Fire' in Mogadishu," in Horn et al, *Force of Choice*,

Chapter 7; David Miller, *Special Forces* (London: Salamander Books, 2001), 18-73; Harclerode, *Secret Soldiers*, 264-285 & 411; Adams, *US Special Forces*, 160-162; Marquis, *Unconventional Warfare*, 63-65; Weale, *Secret Warfare*, 201-235; Colonel Charlie Beckwith, *Delta Force* (New York: Dell, 1983); Neillands, 204-246; and Leroy Thompson, *The Rescuers. The World's Top Anti-Terrorist Units* (London: A David & Charles Military Book, 1986).

57 The SAS was not without its share of scandals that reinforced the stereotype of SOF as "above the law." For example, a number of shootings of Irish Republican Army (IRA) fighters raised allegations of a "shoot to kill" policy (e.g., Operation Judy – the "Loughgall Ambush on May 8,1987; Operation Flavius in Gibraltar on March 6, 1988, as well as the Strabane and Dunloy incidents).

58 The conflict revolved around a new runway that was being built that was much longer than required for commercial airliners. In fact, it was capable of receiving advanced Soviet and / or Cuban fighter bombers. Moreover, on 12 October 1983, as the runway was near completion a military coup replaced the incumbent Marxist Leader, who had made overtures to the Americans, with a more radical Marxist Revolutionary Council aligned with the Soviet and Cuban governments. President Ronald Regan decided the Caribbean Island now represented a national security threat and ordered the invasion to restore a more amenable government and protect American lives. The enemy force amounted to 50 Cuban advisors, approximately 700 Cuban construction workers and 1,200 Grenada People's Revolutionary Army members.

59 Marquis, *Unconventional Warfare*, 91-106.

60 U.S. Department of Defense (DoD). *United States Special Operations Command History* (Washington DC: USSOCOM, 1999), 3-16; Marquis, *Unconventional Warfare*, 69-226; DoD, *US Special Operations Forces. Posture Statement 2000* (Washington DC: USSOCOM, 2000), 11-14; and Clancy, *Special Forces,* 10-27.

61 The Iraqi Skud missiles were known as the al-Hussein (aka al-Hosseih) and the al-Abbas (aka al-Hijarah), which had a range of 750-900 km. Both were Iraqi modifications of the Soviet R-17 ballistic missile known as the SS-IC Scud B in NATO. The Iraqi versions had less payload but were effective as a terror weapon. They launched 203 against Iran in the 1980-1988 Iran-Iraq war. They possessed five fixed launchers and an estimated 36 mobile launchers. The mobile Transporter-Erector-Launchers (TELs) were of two types. One type was the Soviet made eight wheeled MAZ-543 and the second type was the Al Waleed, a modified civilian Saab-Scania tractor trailer. In addition, a large number of vehicles (i.e., fuel, and missile resupply) that were disguised as civilian buses supported the launchers. The Iraqis used high fidelity decoys and deployed in gullies, wadis, and culverts as well as highway underpasses to thwart aerial reconnaissance. Iraqi crews could prepare and launch a missile in under 30 minutes. The first US SOF teams began searching for mobile Transporter-Erector-Launchers (TELs) on February 7, 2001. U.S. SOF and the SAS divided the responsibility for searching for the Skud 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 "Skud Alley." The teams also destroyed fiber-optic links, blew up microwave relay towers and communication bunkers and attacked enemy vehicles. 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; Maquis, *Unconventional Warfare*, 227-249; Adams, 231-244; Carney and Schemmer, 224-236; and Connor, *Ghost Force*, 456-501.

62 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, 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. William Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets. Lesson from Vietnam and the Persian Gulf War* (Santa Monica, CA: RAND, 2001), 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*, Vol. 160, no. 26 (23 December 2002): 34; and Cameron Spence, *Sabre Squadron* (London: Michael Joseph, 1997).

63 Marquis, 228; and Waller, *Commando,* 34 & 241; Schemmer, "Special Ops Teams," 36.

64 Clancy, *Special Forces*, 12; Waller, *Commandos*, 231 and D.C. Waller, "Secret Warriors," *Newsweek* (17 June 1991): 21.

65 Schemmer, "Special Ops Teams," 36; and Waller, *Commandos,* 34 & 241. Waller states that 7,705 SOF personnel participated.

66 DoD, *USSOCOM History,* 44-69; *US SOF Posture Statement 2000*, 15-23; and Adams, *US Special Forces*, 244-286.

67 James C. Hyde, "An Exclusive Interview with James R. Locher III," *Armed Forces Journal International,* (November/December 1992): 34; and Lieutenant-General Peter J. Schoomaker, "Army Special Operations: Foreign Link, Brainy Force," *National Defense* (February 1997): 32-33.

68 Scott Gourlay, "Boosting the Optempo," *Janes Defence Weekly* (14 July 1999): 26.

69 As one USSF officer captured during a classified briefing in October 2001:

> "This is not war as you have ever known it before. This is vengeance for the women and children they murdered on 9/11. Our responsibility is to implement that vengeance. Fight as though your own families were killed in New York. You are America's avenging angels. Your goal is justice and you are authorized to use all means necessary towards that end."

Robin Moore, *The Hunt for Bin Laden. Task Force Dagger* (New York: Ballantine Books, 2003), 233.

70 Glenn Goodman, "Tip of the Spear," *Armed Forces Journal International* (June 2002): 35; and Moore, *The Hunt for Bin Laden*, xix, 2. This number represents 18 Operational Detachment – Alpha 12-man teams. Initially only four SF teams were inserted by helicopter in the north to link up with Northern Alliance commanders in late October

and early November when the U.S.-backed anti-Taliban offensive appeared to be bogged down. The growing importance of their role as combat control teams is evident. In Afghanistan, 60 percent of munitions dropped were precision guided compared to 35 percent during the Kosovo air campaign in 1999 and 6 percent in the Gulf War in 1991. Dr. Elinor Sloan, "Terrorism and the Transformation of US Military Forces," *Canadian Military Journal,* Vol. 3, no. 2, (Summer 2002).

71 Air strikes brought down by one of the first SF teams in the country, aided by a lone Air Force combat controller, are credited with killing as many as 3,500 fighters and destroying up to 450 vehicles. Another Team, Tiger Team 2, was attributed with 2,500 enemy killed, over 50 vehicles destroyed and over 3,500 prisoners captured, as well as the liberation of over 50 towns and cities. Moore, *The Hunt for Bin Laden*, 103-104, 136 &139.

72 "Lessons From the Iraq War," *Strategic Comments*, Vol. 9, no. 3 (May 2003) (http://www.iss.org) report went on to say "the combination of GPS-guided all-weather bombs, better all-weather sensors and real time joint communications networks denied Iraqi forces any sanctuary."

73 Michael Duffy, Mark Thompson, and Michael Weisskopf, "Secret Armies of the Night," *Time*, Vol. 161, no. 25.

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

75 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.

76 This includes an active force element of 29,164 personnel and a reserve component of 10,043. DoD, *US SOF, Posture Statement 2000*, 41.

77 Roxane Tiron, "Demand for Special Ops Forces Outpaces Supply," *National Defense*, Vol. 87, no. 594 (May 2003): 18. There were more than 12,000 deployed to Iraq and approximately 8,000 deployed to Afghanistan.

78 See Colonel Bernd Horn, *More Than Meets the Eye: The Invisible Hand of SOF in Afghanistan* (Kingston: CANSOFCOM PDC, 2011).

79 Jim Thomas and Chris Dougherty, *Beyond the Ramparts. The Future of US Special Operations Forces* (Center for Strategic and Budgetary Assessments, 2013), 32. Of note, the raid on Bin Laden on May 2, 2011, was only one of 14 operations conducted that night. Ibid., 6.

80 Rafael Epstein, "Diggers in Afghan hit squads," *The Age,* 5 May 2011.

81 Carlotta Gall, "Night Raids Curbing Taliban, but Afghans Cite Civilian Toll," *The New York Times*, 8 July 2011. Another example from May 2010 through April 2011, demonstrates that out of 2,245 total CT missions conducted by SOF in Afghanistan, 1,896 (84 per cent) saw no shots fired, while 1,862 missions captured or killed the intended target and /or their associates (83 per cent); Thomas and Dougherty, *Beyond the Ramparts…* (2013), 19.

82 Sean D. Naylor, "Chinook crash highlights rise in spec ops raids," *Army News*, 21 August 2011.

83 A RAND research report explains that "Special Warfare campaigns stabilize or destabilize a regime by operating 'through and with' local state or non-state partners, rather than through unilateral US action." It goes on to explain that Special Warfare involves the comprehensive orchestration of all governmental capabilities to advance policy objectives. These campaigns have six central features:

1. Their goal is stabilizing or destabilizing the targeted regime;
2. Local partners provide the main effort;
3. US forces maintain a small (or no) footprint in the country;
4. They are typically of long duration and may require extensive preparatory work better measured in months (or years) than days;
5. They require intensive interagency cooperation; and
6. They employ 'political warfare' methods to mobilize, neutralize, or integrate individuals or groups from the tactical to the strategic levels.

Dan Madden, Dick Hoffman, Michael Johnson, Fred Krawchuk, John Peters, Linda Robinson, Abby Doll, "Special Warfare. The Missing Middle in US Coercive Options," RAND Research Report, 2014, 1-2.

84 The situation greatly deteriorated with the French withdrawal from Mali in 2022 and subsequently from Burkina Faso the same year. The arrival of the Russian mercenary firm, Wagner Group, in the wake of the French departure simply exacerbated the internal chaos and human rights abuses in both countries.

85 See David Axe, "British and French Commandos Take Charge of Mali War," http://www.wired.com/dangerroom/2013/01/mali-commandos/, accessed 28 November 2013; and Murielle Delaporte, "Mali: France's Version Of Shock And Awe, Add Allies, Crush AQIM," February 19, 2013, http://breakingdefense.com/2013/02/mali-frances-version-of-shock-and-awe-add-allies-crush-aqim/ accessed 28 November 2013.

86 The Islamic State (IS) was officially created in April 2013. However, it is an offshoot of the former Sunni insurgent organization al-Qaeda in Iraq (AQI), which was formed in 2003.

87 Written Statement of Admiral William H. McRaven, USN Commander, United States Special Operations Command Before the 113th Congress Senate Armed services Committee Emerging Threats and Capabilities Subcommittee, April 9, 2013.

88 Steff Thomas, "Post-Afghanistan, Special Operations to Shift to Conflict Prevention," *National Defense*, http://www.national defensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1220, accessed 1 August 2013.

89 Ibid.

90 Patrick Hennessy, "Special forces face big cuts in support network," *The Telegraph*, 2 February 2013.

91 NATO doctrine lists only three SOF core tasks, i.e., DA, SR and Military Assistance. However, sub-tasks under the three core tasks capture activities from the larger list. Important to note is "High Value Tasks," as this in essence is the outlet for SOF to meet the requirement to respond to any crisis situation or task its government's may face.

92 General David Barno and Travis Sharp, "SOF Power," *Foreign Policy*, http://www.foreignpolicy.com/articles/2012/02/14/sof_power, accessed 19 July 2014.

93 Richard Fadden, Keynote Speaker, "The Strategy Bridge" Conference, Ottawa, May 13, 2015.

CHAPTER 2

1 Maurice Tugwell and David Charters, "Special Operations and the Threats to United States Interests in the 1980's," in *Special Operations in U.S. Strategy* (Washington D.C.: National Defense University Press, 1984), 35.

2 Robert Graves in Frank R. Barnett, B. Hugh Tovar, and Richard H. Shultz eds., *Special Operations in U.S. Strategy* (New York: National Defense University Press, 1984).

3 Sun Tzu, *The Art of War,* translated by Ralph D. Sawyer (New York: Basic Books, 1994).

4 Carl von Clausewitz, *On War*, translated by Michael Eliot Howard and Peter Paret (Princeton, NJ: Princeton University Press, Revised ed., 1989); and Christopher Daase and James W. Davis, eds. *Clausewitz on Small War* (Oxford: Oxford University Press, 2015).

5 Christopher Marsh, James Kiras and Patricia Blocksome, "Special Operations Research: Out of the Shadows." *Special Operations Journal,* Vol. 1, no. 1 (2015): 1-6.

6 Tom Searle, "Outside the Box: A Theory of Special Operations," in Peter McCabe and Paul Lieber, eds., *Special Operations Theory* (Tampa, FL: JSOU Press, 2017), 104.

7 Colin Gray, *Explorations in Strategy* (London: Praeger, 1996), 149.

8 John Arquilla, *From Troy to Entebbe: Special Operations in Ancient and Modern Times* (Lanham, Md: University Press of America, 1996), xv-xvi.

9 Searle, "Outside the Box…"

10 Harry Yarger, Harry, *21st Century SOF: Toward an American Theory of Special Operations* (Tampa, FL: JSOU Press, 2013), 46.

11 Ibid., 21.

12 Richard Rubright, *A Unified Theory of Special Operations* (Tampa, FL: JSOU Press, 2017), 20.

13 Ibid., 7.

14 Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York: Anchor, 1967).

15 Ibid., 116-117.

16 Jack L. Snyder, "The Soviet strategic culture: Implications for limited nuclear operations." (Santa Monica, CSA: RAND, 1977), 4-8.

17 Jack Snyder, "The Concept of Strategic Culture: Caveat Emptor," in Carl G. Jacobsen, ed., *Strategic Power: USA/USSR* (New York: St Martin's Press, 1990), 7.

18 Colin Gray, *Explorations in Strategy* (London: Praeger, 1996), 143.

19 William McRaven, *Spec Ops: Case Studies in Special Operations Warfare* (New York: Presidio, 1996).

20 Robert A. Spulak, Jr., *A Theory of Special Operations: The Origin, Qualities, and Use of SOF* (Hurlburt Field, Fl: JSOU Press, 2007), 1.

21 Colin Gray, *Tactical Operations for Strategic Effect: The Challenge of Currency Conversion* (Tampa, FL: JSOU Press, 2015), 41.

22 For a more in-depth discussion on attrition and annihilation see: Gordon A. Craig, "Delbruck: The Military Historian," in Peter Paret, ed., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, N.J.: Princeton Univ. Press, 1986), 341-342.

23 James Kiras, "A Theory of Special Operations: 'These Ideas Are Dangerous,'" *Special Operations Journal* Vol. 1, no. 2 (2015): 75-88.

24 Colin Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 17.

25 Gray, *Explorations in Strategy,* 149.

26 Colin Gray, "Handfuls of heroes on desperate ventures: When do Special Operations succeed?" *The US Army War College Quarterly: Parameters* Vol. 29, no. 1 (1999): 4.

27 Colonel Bernd Horn, "The Strategic Utility of Special Operations Forces," *Canadian Military Journal*, Vol. 14, no. 4 (2014): 67.

CHAPTER 3

1 According to the Department of Defense Dictionary of Military Terms (Joint Pub 1-02) the current definition of Unconventional Warfare (UW), approved by USSOCOM in 2009, is: Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. UW is one of five core activities of Irregular Warfare (IW). The other activities are Counter-Insurgency (COIN), Counterterrorism (CT) Foreign Internal Defense (FID) and Stabilization Operations.

2 Two of the greatest practitioners in modern times were Lieutenant Colonel Thomas Edward Lawrence who was renowned for his role in the Arab Revolt (1916-1918) and the Sinai and Palestine campaign (1915-1918) against the Ottoman Empire, and the arguably equally prominent practitioner of irregular warfare, the famous 'Lion of Africa' German

General Paul von Lettow-Vorbeck whose small force of 14,000 held in check 300,000 Allied troops in German East Africa.

3 Jay Jakub D. Phil, *Spies and Saboteurs: Anglo-American Collaboration and Rivalry in Human Intelligence Collection and Special Operations, 1940-45* (New York: St. Martin's Press, 1999), 22-23.

4 Francis Mackay, *Overture to Overlord: Special Operations in Preparation for D-Day* (South Yorkshire: Pen and Sword, 2005), 143.

5 A. R. B. Linderman, *Rediscovering Irregular Warfare: Colin Gubbins and the Origins of Britain's Special Operations Executive* (Oklahoma: University of Oklahoma Press, 2016), 61-67.

6 Ibid., 67-71.

7 Major-General Sir Colin Gubbins, "SOE and the coordination of Regular and Irregular War" in *The Fourth Dimension of Warfare, Volume 1 Intelligence/ Subversion/ Resistance,* ed. Michael Elliott-Bateman (New York: Praeger Publishers, 1970), 86.

8 Linderman, *Rediscovering Irregular Warfare*, 63.

9 Ibid., 39.

10 The British Principles of War are Selection and Maintenance of the Aim, Maintenance of Morale, Offensive Action, Security, Surprise, Concentration of Force, Economy of Effort, Flexibility, Cooperation and Sustainability. See http://www.in command.co.uk/ten-principles-of-war, accessed 12 December 2021.

11 Linderman, *Rediscovering Irregular Warfare*, 39. See also, Brian Lett, *SOE's Mastermind: An Authorized Biography of Maj. Gen. Sir Colin Gubbins KCMG, DSO, MC* (South Yorkshire, England: Pen and Sword, 2016), 82-96.

12 Linderman, *Rediscovering Irregular Warfare*, 61.

13 Ibid., 164.

14 Ibid., 164.

15 Nigel West, *Secret War: The Story of SOE Britain's Wartime Sabotage Organization* (Barnsley: Frontline Books, 2019), 231.

16 See Jessica Glicken Turnley, *Special Operations Forces as Change Agents* (JSOU Press, March 2017).

17 John Nelson Rickard, *The Politics of Command: Lieutenant-General A. G. L. McNaughton and the Canadian Army 1939-1943* (Toronto: University of Toronto Press, 2010), 150-159.

18 For a contemporary overview of counterintelligence and irregular warfare see Graham H. Turbiville, *Guerrilla Counterintelligence: Insurgent Approaches to Neutralizing Adversary Intelligence Operations* (Hurlburt Field: JSOU report, 09-01 2009).

19 Mackay, *Overture to Overlord*, 153.

20 Linderman, *Rediscovering Irregular Warfare*, 166.

21 Mackay, *Overture to Overlord*, 155.

22 Ibid., 154-155.

23 West, *Secret War,* 231.

24 John Mendelsohn, ed., *Covert Warfare: Intelligence, Counterintelligence, and Military Deception During the World War II Era* (New York: Garland Publishing, 1989), ii.

25 Office of Strategic Services, *Special Services Field Manual-Strategic Services (Provisional)* (Washington, DC: Office of Strategic Services, 1944), 5.

26 Will Irwin, *The Jedburgh: The Secret History of the Allied Special Forces, France 1944* (New York: Public Affairs, 2005), 34-39.

27 West, *Secret War*, 233.

28 Mendelsohn, ed., *Covert Warfare*, 1.

29 S.J. Lewis, *Jedburgh Team Operations in Support of the 12th Army Group, August 1944* (Fort Leavenworth: Combat Studies Institute, 1991), 11.

30 Special Operations Executive and Special Operations, *Basic Directive on Jedburghs* (OSS, SO Working Document: December 1943), Vol. 12, 38-39.

31 Wyman W. Irwin, Zoom Interview (6 December 2021). Retired Special Forces Lieutenant Colonel and author of *The Jedburgh: The Secret History of the Allied Special Forces*.

32 Albert Lulushi, *Donovan's Devils: OSS Commandos Behind Enemy Lines-Europe, World War II* (New York: Arcade Publishing, 2016), 155.

33 Lett, *SOE's Mastermind,* 233-234.

34 Ibid., 233.

35 Gubbins, "SOE and the Coordination of Regular and Irregular War," 96-97.

36 Ibid., 97-98.

37 Benjamin F. Jones, *Eisenhower's Guerrillas: The Jedburgh, the Maquis, and the Liberation of France* (New York: Oxford University Press, 2016), 4.

38 Harry Butcher, *My Three Years with Eisenhower: The Personal Diary of Capt. Harry C. Butcher, USNR, Naval Aide to General Eisenhower, 1942-1945* (New York: Simon and Schuster, 1946). As quoted in Irwin, *The Jedburghs*, 241.

39 Richard H. Smith, *OSS: The Secret History of America's First Central Intelligence Agency* (Berkeley, CA: University of California Press, 1981), 221.

40 J. G. Beevor, *SOE: Recollections and Reflections 1940-45* (London: The Bodley Head Ltd, 1981), 160.

41 James Stejskal, *No Moon as Witness: Missions of the SOE and OSS in World War II* (Oxford, UK: Casement Publishers, 2021). Extract from https://www.casematepublishing.co.uk/blog/2021/06/02/jedburgh-team-and-operation-overlord-the-battle-of-normandy/, accessed 15 December 2021.

42 The Canadian acronym for two-spririted, lesbian, gay, bisexual, transgender, queer, intersex and others.

CHAPTER 4

1 Terrorism is defined as "The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instil fear and coerce governments or societies in pursuit of goals that are usually political." U.S. Special Operations Command, *Special Operations Forces Reference Manual Fourth Edition* (Tampa Bay: JSOU, 2015) A-10. The term "new" is used because although terrorism is not a new concept or tactic, when it became pervasive in the West, it was seen as "new."

2 Canada, "Trends in Terrorism," *Perspectives. A Canadian Security Intelligence Service Publication*, Report #20000/01, 18 December 1999, 1.

3 Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 16-17.

4 Ibid., 63.

5 Canada, "Trends in Terrorism," 1.

6 Cited in Hoffman, *Inside Terrorism*, 64.

7 The hostages included David Berger, Ze'ev Friedman, Eliezer Halfin, Mark Slavin, Amitzur Shapira, Kehat Shorr, Andre Spitzer, Yakov Springer and Yossef Gutfreund.

8 "Munich Massacre," *This Day in History*, 24 May 2021, https://www.history.com/topics/1970s/munich-massacre-olympics, accessed 22 March 2023.

9 Ibid.

10 The police officers apparently took a vote and decided the plan was far too dangerous and risky for them, so they left without informing their command centre.

11 There is discrepancy on the number of police officers posing as aircrew. Most sources cite five, while at least one states there were 17. The military was bettered equipped to deploy snipers; however, the FDR's postwar constitution limited the use of the army in domestic affairs in peacetime.

12 George Jones, *Vengeance* (Toronto: HarperCollins, 2005 ed.), 1-7; and Peter Harclerode, *Secret Soldiers. Special Forces in the War Against Terrorism* (London: Cassell & Co., 2000), 22 and 263.

13 Hoffman, *Inside Terrorism*, 67.

14 The FDR had consciously decided to minimize security to display a benign atmosphere that had none of the militaristic hallmarks of the 1936 Munich Olympics held by Hitler. As such, only unarmed security personnel were employed to secure the games.

15 Allegations were raised that the FDR colluded with the Palestinians to hijack the aircraft so that they could release the three terrorists in hopes of preventing further acts of terrorism against the FDR with the aim of getting the release of the imprisoned Black September terrorists. See Noga Tarnapolsky and Rob Hyde, "'Proof' West Germany staged 1972 plane hijack to free Munich Olympics killers," *TheJC*, 11 August 2022, https://www.thejc.com/news/world/proof-west-germany-staged-1972-plane-hijack-to-free-munich-olympics-killers-49mqppQPxDYek8XLzkUf38, accessed 23 March 2023; and "Lufthansa Flight 615," Infogalactic.Com, n.d., https://infogalactic.com/info/Lufthansa_Flight_615, accessed 23 March 2023.

16 See George Jonas, *Vengeance* (Toronto: HarperCollins, 1985); and Michael Bar-Zohar and Nissim Mishal, *Mossad* (New York: HarperCollins, 2012) for details on Operation Wrath of God.

17 General (retired) Ulrich Wegener, "The Evolution of *Grenzshutzgruppe* (GSG) 9 and the Lessons of 'Operation Magic Fire' in Mogadishu" in Bernd Horn, J. Paul de B. Taillon and David Last, eds., *Force of Choice. Perspectives on Special Operations* (Kingston: McGill-Queen's University Press, 2004), 109.

18 James Doubek, "50 years ago, the Munich Olympics massacre changed how we think about terrorism," *National Public Radio* (*npr*), 4 September 2022, https://www.npr.org/2022/09/04/1116641214/munich-olympics-massacre-hostage-terrorism-israel-germany, accessed 22 March 2023.

19 Susan L. Marquis, *Unconventional Warfare* (Washington D.C.: Brookings Institute Press, 1997), 63.

20 OPEC did not hold another summit meeting for twenty-five years. See Harclerode, *Secret Soldiers*; Benjamin Netanyahu, *Fighting Terrorism* (New York: Noonday Press, 1995); Christopher Dobson and Ronald Payne, *The Terrorists* (New York: Facts on File, 1995); Marquis, *Unconventional Warfare,* 62-65; and Brian MacDonald, ed., *Terror* (Toronto: The Canadian Institute of Strategic Studies, 1986).

21 In the aftermath of the Munich Olympics the Belgians created Group Diane as a CT force. The name was changed to SIE (*Speciaal Interventie Eskadron* or ESI in French: *Escadron spécial d'intervention*) in 1974.

CHAPTER 5

1 Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (New York: Everyman's Library, Alfred A. Knopf, 1993), 731.

2 Robert Coalson, "The Value of Science is in the Foresight," *Military Review* (January-February 2016): 29.

3 Cited in Seth G. Jones, *Three Dangerous Men. Russia, China, Iran and the Rise of Irregular Warfare* (New York: W.W. Norton & Company, 2021), 190. A conventional war is defined as "a form of warfare between states that employ direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies. The focus of conventional military operations is normally an adversary's armed forces with the objective of influencing the adversary's government. It generally assumes that the indigenous populations within the operational area are non-belligerents and will accept whatever political outcome the belligerent governments impose, arbitrate, or negotiate. A fundamental military objective in conventional military operations is to minimize civilian interference in those operations." U.S. Department of Defense, *The Irregular Warfare Joint Operating Concept* (*IW JOC*), Version 1.0, dated 11 September 2007.

4 Robert Farley, "Welcome to the All-Consuming Great Power Competition," *The Diplomat*, 23 February 2021. https://thediplomat.com/2021/02/welcome-to-the-all-consuming-great-power-competition/, accessed 24 February 2021.

5 For example, it was reported that American policy-makers increasingly see the U.S.-Chinese rivalry not as a traditional great-power competition but as a struggle pitting democracy against communism. In July 2020, then-Secretary of State Mike Pompeo delivered a speech that cast the U.S.-Chinese antagonism in ideological terms. Christopher Layne, "Coming Storms. The Return of Great-Power War," *Foreign Policy* (November/December 2020), https://www.foreignaffairs.com/articles/united-states/2020-10-13/coming-storms, accessed 3 November 2020.

6 Kaley Scholl, "The Use of US Special Operation Forces in Great Power Competition: Imposing Costs on Chinese Gray Zone Operations," *Small Wars Journal* (7 December 2020), https://smallwarsjournal.com/jrnl/art/use-us-special-operation-forces-great-power-competition-imposing-costs-chinese-gray-zone, accessed 8 December 2020.

7 The February 2022 Russian invasion of Ukraine is arguably an outlier/miscalculation on President Vladimir Putin's part.

8 András Rácz, *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs, FIIA Report 43, 41. The Americans use a term called "Gray Zone Conflict" to describe Hybrid Warfare. Gray Zone Conflict is defined "as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks." USSOCOM White Paper, *The Gray Zone*, 9 September 2015, 1.

9 Kerry K. Gershaneck, *Political Warfare. Strategies for Combating China's Plan to "Win without Fighting,"* (Quantico, VA: Marine Corps University Press, 2020), 26. The concept of Hybrid Warfare, also known as "Gray Zone operations" in American doctrine, is not new. The concept of "political warfare," which is the term George Keenan coined in 1948, stating that political warfare encompassed "all the means at a nation's command, short of war, to

achieve its national objectives." In the 1990s, the term military operations other than war (MOOTW) became in vogue. The concept was based on "deterring war, resolving conflict, promoting peace, and supporting civil authorities." Specific operations included arms control, counterterrorism, humanitarian assistance, peace operations, and show-of-force operations. This concept combined the concept of the application of military power combined with other levers of national power to achieve political objectives. "Keenan Long Telegraph," https://digitalarchive.wilsoncenter.org/document/116178.pdf, accessed 6 July 2021; and David A. Broyles and Brody Blankenship, *The Role of Special Operations Forces in Global Competition* (Arlington, VA: CNA Analysis & Solutions, 2017), 10.

10 Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds., *Hybrid Conflict: The Roles of Russia, North Korea and China* (Wassenaar: Clingendael Institute, 2018), 1.

11 Cited in Stefan Hadjitodorov and Martin Sokolov, "Blending New-Generation Warfare and Soft Power: Hybrid Dimensions of Russia-Bulgaria Relations," *Connections: The Quarterly Journal*, Vol. 17, no. 1 (2018): 11.

12 David Knoll, Kevin Pollpeter and Sa Plapinger, "China's Irregular Approach to War: The Myth of A Purely Conventional Future Fight," *The Modern War Institute*, 27 April 2021.

13 Broyles and Blankenship, *The Role of Special Operations Forces,* 13-14.

14 Ibid.

15 Ibid. Further insight on how Russia views contemporary conflict was provided by Colonel S.G. Chekinov and Lieutenant-General S.A. Bogdanov in a 2013 article entitled "The Nature and Content of a New-Generation War." Similar to General Gerasimov, they extracted lessons from how the West, particularly the Americans, have conducted their military campaigns. As a result, they identified eight particular steps of new-generation warfare:

1. Non-military measures that blend moral, information, psychological, ideological, and economic measures that aim at establishing a more favorable political, economic, and military environment;
2. Media, diplomatic channels, and top government and military agencies carry out coordinated special operations so as to mislead political and military leaders. This can include leaking false data, orders, directives, and instructions;
3. Bribing, deceiving, and/or intimidating government and military officers, to force them to abandon their duties;
4. Fueling discontent among the population. This can be further enhanced by the arrival of Russian "volunteers";
5. Establish no-fly zones and blockades over the targeted country. Cooperation between private military contractors and armed opposition;
6. Initiate large-scale reconnaissance and subversion operations that are initiated immediately followed up upon with military action;
7. Launch a combination of information, electronic warfare, and air force operations that are complimented with high-precision weapons; and

8. Eliminate the last points of resistance through reconnaissance operations, special operations, and artillery and missile bombardment.

Cited in Hadjitodorov and Sokolov, "Blending New-Generation Warfare," 12-13.

16 Cited in Tom Wilhelm, "A Russian Military Framework for Understanding Influence in Competition Period," *Military Review* (July-August 2020): 36.

17 Ibid.

18 For a detailed study of Hybrid Warfare see Colonel Bernd Horn, *On Hybrid Warfare* (Kingston: CANSOFCOM PDC Press, 2016).

19 Maria Snegovaya, "Putin's Information Warfare in Ukraine Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War*, September 2015, 7 and 10.

20 Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Forces Quarterly*, Vol. 79 (2015): 47.

21 Travis Clemens, *Special Operations Forces Civil Affairs in Great Power Competition JSOU Report 20-4* (Tampa: JSOU, 2020), 22. The Congressional Research Service has noted that key features of the current situation of renewed great power competition include but are not necessarily limited to the following:

- the use by Russia and China of new forms of aggressive or assertive military, paramilitary, information, and cyber operations—sometimes called Hybrid Warfare, gray-zone operations, ambiguous warfare, among other terms, in the case of Russia's actions, and salami-slicing tactics or gray-zone warfare, among other terms, in the case of China's actions;
- renewed ideological competition, this time against 21st-century forms of authoritarianism and illiberal democracy in Russia, China, and other countries;
- the promotion by China and Russia through their state-controlled media of nationalistic historical narratives, some emphasizing assertions of prior humiliation or victimization by Western powers, and the use of those narratives to support revanchist or irredentist foreign policy aims;
- challenges by Russia and China to key elements of the U.S.-led international order, including the principle that force or threat of force should not be used as a routine or first-resort measure for settling disputes between countries, and the principle of freedom of the seas (i.e., that the world's oceans are to be treated as an international commons); and
- additional features alongside those listed above, including:
    - continued regional security challenges from countries such as Iran and North Korea;
    - a continued focus (at least from a U.S. perspective) on countering transnational terrorist organizations that have emerged as significant non-state actors (now including the Islamic State organization, among other groups); and

- weak or failed states, and resulting weakly governed or ungoverned areas that can contribute to the emergence of (or serve as base areas or sanctuaries for) non-state actors, and become potential locations of intervention by stronger states, including major powers.

Ronald O'Rourke, *Renewed Great Power Competition: Implications for Defense – Issues for Congress* (Washington D.C.: Congressional Research Service, 4 March 2021), 22.

22 Special Warfare (SW) is defined as "the execution of activities that involve a combination of lethal and non-lethal actions taken by specially trained and educated forces that have a deep understanding of cultures and foreign language, proficiency in small-unit tactics, subversion, sabotage and the ability to build and fight alongside indigenous combat formations in a permissive, uncertain or hostile environment." Its activities range from influence operations and political action to economic sanctions and diplomacy. SW can improve a government's contextual understanding of potential partners and the situation on the ground before it commits to a course of action. SW strategic advantages:

1. Improved understanding and shaping of the environment;
2. Cost Effective / cost imposing strategy – small footprint for you; opponent needs to spend disproportionate amounts of money;
3. Managed escalation and credibility risk – make no promises of larger commitments; and
4. Sustainable solutions – sustainable two parts – fiscal and political.

SW Limits and Risks

1. Divergent partner objectives;
2. Ineffective partner capability;
3. Unacceptable partner behaviour;
4. Policy Fratricide; and
5. Disclosure.

Dan Madden, Dick Hoffman, Michael Johnson, Fred Krawchuk, John Peters, Linda Robinson, Abby Doll, "Special Warfare. The Missing Middle in US Coercive Options," RAND Research Report, 2014, 3.

23 For a detailed breakdown of "under-threshold" activities see Colonel (retired) Bernd Horn, *Strategic Competition: Implications for SOF* (Kingston: CANSOFCOM ERC Press, 2022).

24 Eric Schmitt, "Terrorism Threat in West Africa Soars as U.S. Weighs Troop Cuts," *New York Times*, 27 February 2020, https://www.nytimes.com/2020/02/27/world/africa/terrorism-west-africa.html, accessed 27 February 2020.

25 Ben Connable, Stephanie Young, Stephanie Pezard, Andrew Radin, Raphael S. Cohen, Katya Migacheva, James Sladden, *Russia's Hostile Measures* (Santa Monica, CA: RAND, 2020), x, 4.

26 John Taft, Liz Gormisky and Joe Mariani, *Special Operations Forces and Great Power Competition, A Report from the Deloitte Center for Government Insights*, n.d., 3, https://www2.deloitte.com/content/dam/insights/us/articles/4980_special-operations-forces/DI_special-operations-forces.pdf, accessed 26 April 2021.

CHAPTER 6

1 U.S. Department of Defense (DoD), *Military and Security Developments Involving the People's Republic of China 2022: Annual Report to Congress* (Washington, D.C.: Office of the Secretary of Defense, 29 November 2022), 1-2. Hereafter "2022 CMPR."

2 Ibid., 1.

3 Ibid., 34; and Joel Wuthnow, ed., *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context* (Washington, D.C: National Defense University Press, 2021), 151.

4 Xia Hua, "The Taiwan Question and China's Reunification in the New Era," *Xinhua*, 10 August 2022, 18; and The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing, China: Foreign Languages Press, 2019), 7.

5 Hua, "The Taiwan Question," 1; and The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 4.

6 Ryan Haas, "From Strategic Reassurance to Running Over Roadblocks: A Review of Xi Jinping's Foreign Policy Record," *China Leadership Monitor* Fall 2022, no. 73 (September 1, 2022): 1.

7 Ibid., 14.

8 Ibid., 14; and Edward J. Barss, *Chinese Election Interference in Taiwan*, Politics in Asia (New York: Routledge, Taylor & Francis Group, 2022), 3.

9 Haas, "From Strategic Reassurance…," 2; and "Great Rejuvenation of the Chinese Nation | The Center for Strategic Translation," https://www.strategictranslation.org/glossary/great-rejuvenation-of-the-chinese-nation, accessed 29 May 2023.

10 DoD, "2022 CMPR," 2.

11 Ibid., 23.

12 Hua, "The Taiwan Question," 10.

13 Ibid., 14.

14 Ibid., 18.

15 Ibid., 34.

16 Phillip C. Saunders, "China's Role in Asia: Attractive or Aggressive?" in David L. Shambaugh, ed., *International Relations of Asia, Third edition, Asia in World Politics* (Lanham: Rowman & Littlefield, 2022), 118.

17 Ibid., 119.

18 The Center for Strategic Translation, "Community of Common Destiny For All Mankind," 2022, https://www.strategictranslation.org/glossary/community-of-common-destiny-for-all-mankind, accessed 29 May 2023.

19 Susan L. Shirk, ed., *China: Fragile Superpower*, 2nd Edition (Oxford: Oxford University Press, 2017), 182-195.

20 Ibid., 185.

21 Ibid., 193.

22 Ibid., 182.

23 Ibid., 182.

24 Shelley Rigger Chan Lev Nachman, Chit Wai John Mok, and Nathan Kar Ming, "Why Is Unification So Unpopular in Taiwan? It's the PRC Political System, Not Just Culture," *Brookings* (blog), February 7, 2022, https://www.brookings.edu/blog/order-from-chaos/2022/02/07/why-is-unification-so-unpopular-in-taiwan-its-the-prc-political-system-not-just-culture/.

25 Shirk, *China: Fragile Superpower*, 195; and Nathan F. Batto, "Taiwan Is Already Independent," *Foreign Affairs*, December 12, 2022, https://www.foreignaffairs.com/taiwan/taiwan-already-independent.

26 Shirk, *China: Fragile Superpower*, 195; and Batto, "Taiwan Is Already Independent."

27 Shirk, *China: Fragile Superpower*, 183.

28 Batto, "Taiwan Is Already Independent."

29 Shirk, *China: Fragile Superpower*, 183.

30 Batto, "Taiwan Is Already Independent"; Taiwan News, "76% of Taiwanese Believe Taiwan Already Independent under Status Quo," 4 March 2022, https://www.taiwannews.com.tw/en/news/4462234.

31 Shirk, *China: Fragile Superpower*, 195.

32 Jude Blanchette and Gerard DiPippo, "'Reunification' with Taiwan through Force Would Be a Pyrrhic Victory for China," November 22, 2022, https://www.csis.org/analysis/reunification-taiwan-through-force-would-be-pyrrhic-victory-china.

33 William Sposato, "Beijing's Taiwan Aggression Has Backfired in Tokyo," *Foreign Policy* (blog), August 8, 2022, https://foreignpolicy.com/2022/08/08/china-taiwan-japan-military-response/.

34 Ibid.

35 DoD, "2022 CMPR," 34.

36 Barss, *Chinese Election Interference in Taiwan*, 3; and Richard C. Bush, "Taiwan's Democracy and the China Challenge," *Brookings* (blog), 22 January 2021, https://www.brookings.edu/articles/taiwans-democracy-and-the-china-challenge/.

37 Bush, "Taiwan's Democracy and the China Challenge."

38 Barss, *Chinese Election Interference in Taiwan*, 4.

39 Ibid., 4 and 40.

40 Ibid., 42.

41 Ibid., 42.

42 Ibid., 4.

43 Erin Hale, "Incumbent Tsai Wins Taiwan's Presidential Election," https://www.aljazeera.com/news/2020/1/11/tsai-ing-wen-wins-landslide-in-taiwan-presidential-election, accessed 20 June 2023.

44 Anne Applebaum, "China's War Against Taiwan Has Already Started," *The Atlantic*, 14 December 2022, https://www.theatlantic.com/ideas/archive/2022/12/taiwan-china-disinformation-propaganda-russian-influence/672453/.

45 John Lee, *Policy Memo: "Chinese Information and Influence Warfare in Asia and the Pacific,"* (Washington, D.C.: Hudson Institute, September 2022), 6.

46 Applebaum, "China's War Against Taiwan Has Already Started"; and Matthew Fulco, "China Intensifies Taiwan Social Media Influence Operations," *Taiwan Business TOPICS* (blog), 21 September 2022, https://topics.amcham.com.tw/2022/09/china-intensifies-taiwan-social-media-influence-operations/.

47 Applebaum, "China's War Against Taiwan Has Already Started"; and "Chinese Kansai Evacuation Story 'Fake News': DPP," *Taipei Times*, 9 September 2018, https://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087.

48 Applebaum, "China's War Against Taiwan Has Already Started."

49 Wuthnow, *The PLA Beyond Borders*, 151.

50 Ibid., 151.

51 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era, China Strategic Perspectives 13* (Washington, D.C: National Defense University Press, 2018), 2.

52 Ibid., 40.

53 Ibid., 39.

54 Ibid., 12.

55 Kevin Pollpeter, Michael Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, Research Report, RR-2058-AF (Santa Monica, Calif: RAND Corporation, 2017), ix.

56 *PLA Aerospace Power: A Primer on Trends in China's Military Air, Space, and Missile Forces (3rd Edition)* (China Aerospace Studies Institute, 15 August 2022), 70, https://cle.nps.edu/access/content/group/57ff57bb-cb12-4a0b-8af3-8cc734e27397/Readings/Class%2014.%20PLARF%20and%20SSF/CASI-2022-08-15%20PLA%20Primer%203rd%20edition.pdf; and Wuthnow, *The PLA Beyond Borders*, 170.

57 Wuthnow, *The PLA Beyond Borders*, 154.

58 Ibid., 154.

59 *PLA Aerospace Power,* 70-75.

60 Wuthnow, *The PLA Beyond Borders*, 155.

61 Ibid., 172.

62 Ibid., 172; and Costello and McReynolds, *China's Strategic Support Force*, 9.

63 Wuthnow, *The PLA Beyond Borders*, 173.

64 Ibid., 173; and Costello and McReynolds, *China's Strategic Support Force,* 49.

65 *PLA Aerospace Power,* 70.

66 Costello and McReynolds, *China's Strategic Support Force,* 10.

67 Morgan Martin, "China's Three Information Warfares," *U.S. Naval Institute Proceedings,* Vol. 147, no. 3 (March 2021): 1417, https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares.

68 Lee, "Chinese Information and Influence, 6.

69 Ibid., 9.

70 Ibid., 9-10.

71 Ibid., 12-13.

72 A. A. Bastian, "China Is Stepping Up Its Information War on Taiwan," *Foreign Policy*, https://foreignpolicy.com/2022/08/02/china-pelosi-taiwan-information/; and "China's Application of the 'Three Warfares' in the South China Sea and Xinjiang," *Orbis*, Vol. 63, no. 2 (2019): 199-207.

73 Phillip Saunders, "China's Role in Asia: Attractive or Aggressive?" in David Shambaugh, ed., *International Relations of Asia* (Lanham, MD: Rowman & Littlefield, 2022), 122.

74 The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, 15.

75 Saunders, "China's Role in Asia," 122; and The Select Committee on the Chinese Communist Party, *Ten for Taiwan: Policy Recommendations to Preserve Peace and Stability in the Taiwan Strait* (Washington, DC: U.S. Congress, 26 May 2023), 12-13, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/ten-for-taiwan-final-with-cover-page-2.pdf.

76 Svenja Meike Kirsch and Bethan Saunders, *Addressing Russian and Chinese Cyber Threats* (Cambridge, Massachusetts: Harvard Kennedy School Belfer Center, May 2023), 42.

77 Barss, *Chinese Election Interference in Taiwan*, 39.

78 Ian Easton et al., "China's Space and Counterspace Activities: Prepared for The U.S.-China Economic and Security Review Commission" (Project 2049 Institute, March 30, 2020), 7, https://permanent.fdlp.gov/gpo154588/China_Space_and_Counterspace_Activities.pdf.

79 Ibid., 19.

80 Costello and McReynolds, *China's Strategic Support Force,* 36.

81 Easton et al., "China's Space and Counterspace Activities, 17.

82 Ibid., 17; and DoD, "2022 CMPR."

83 Brian Weeden, "2007 Chinese Anti-Satellite Test Fact Sheet" (Secure World Foundation, 23 November 2010), 1, https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf.

84 DoD, "2022 CMPR," 9, 88.

85 Ibid., 93.

86 Reuters, "Taiwan Says China Planning to Briefly Close Airspace Amid Military Drills," *NBC News*, 12 April 2023, https://www.nbcnews.com/news/world/taiwan-says-china-planning-briefly-close-airspace-military-drills-rcna79284.

87 Yimou Lee and Liz Lee, "Taiwan Says It Convinced China to Rein In No-Fly Zone Plan," *Reuters*, 13 April 2023, https://www.reuters.com/world/asia-pacific/taiwan-determined-safeguard-freedom-democracy-president-tsai-says-2023-04-12/.

CHAPTER 7

1 K.D. Suarez, "PH Navy in standoff with Chinese ships," *Rappler*, 11 April 2012, https://www.rappler.com/nation/3671-ph-navy-in-standoff-with-chinese-ships/.

2 Betsy Reed, "Philippine warship in standoff with China vessels," *The Guardian*, 10 April 2012, https://www.theguardian.com/world/2012/apr/11/philippines-china-stand-off-south-china-sea.

3 Renato Cruz De Castro, "The 2012 Scarborough Shoal stand-off," in Leszek Buszynski and Christopher B. Roberts, *The South China Sea Maritime Dispute* (London: Routledge, 2016), 111-129.

4 Roel Landangin and Kathrin Hille, "Philippines and China in Naval Standoff," *Financial Times*, 11 April 2012, https://www.ft.com/content/2bcc70f2-837f-11e1-ab78-00144feab49a.

5 Michael Green, Kathleen Hicks, Zack Cooper, John Schaus and Jake Douglas, "Countering Coercion in Maritime Asia – The Theory and Practice of Gray Zone Deterrence," (Center for Strategic and International Studies, May 2017), 100, https://www.csis.org/analysis/countering-coercion-maritime-asia.

6 Cruz De Castro, "The Scarborough Shoal stand-off," 118.

7 Thai News Service Group, "China/Philippines: China seeks preservation of over-all friendly relations with Philippines as tension over Scarborough Shoal ebbs momentarily," *Asia News Monitor*, 12 April 2012, https://www.proquest.com/docview/993552866/138B64F7C717082.

8 John Grady, "SECNAV, Navy Maritime Intel Director Give Warnings About Illegal Chinese Fishing," *USNI News*, 6 March 2023, https://news.usni.org/2023/03/06/secnav-navy-maritime-intel-director-give-warnings-about-illegal-chinese-fishing.

9 Conor Kennedy and Andrew Erickson, "China Maritime Report No. 1: China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA," *CMSI China Maritime Reports* 1 (2017), https://digital-commons.usnwc.edu/cmsi-maritime-reports/1.

10 "国防后备力量" [National Defense Reserve Force], Jinhu County People's Government Double-Support Office, 20 October 2016, http://www.jinhu.gov.cn/art/2016/10/20/art_96_19469.html.

11 Kennedy and Erickson, "China Maritime Report," 2-3.

12 Shinji Yamaguchi, "Strategies of China's Maritime Actors in the South China Sea," *China Perspectives; Wanchai* 3 (2016): 24.

13 "三沙市推动军警民联防机制 构建三线海上维权格局" [Sansha City Advances its Joint Military, MLE, Militia Defense System—Constructs a Three-line Maritime Rights Protection Layout], *China News Online*, 22 November 2014, http://www.chinanews.com/gn/2014/11-21/6803776.shtml; Interview with PLA Major General Liu Lianhua: "军队代表: 应从战略层面构建军警民海防体系" [Military Representative: [We] Should Strategically Construct a Military, Police, Militia Maritime Defense System], *China News Online*, 15 March 2013, http://www.chinacourt.org/article/detail/2013/03/id/922031.shtml.

14 Kennedy and Erickson, "China Maritime Report," 4.

15 Abhijit Singh, "Deciphering Grey-Zone Operations in Maritime-Asia," ORF (blog), https://www.orfonline.org/research/42978-deciphering-grey-zone-operations-in-maritime-asia/.

16 "破解海上民兵建设难题" [Resolving Issues in Maritime Militia Construction], *National Defense News*, 28 July 2016, www.81.cn/gfbmap/content/2016-07/28/content_151895.htm; and 张践 [Zhang Jian], "围绕'六化'抓建 推动海上民兵转型" [Advance Transformation of the Maritime Militia Centered on Six Changes], *National Defense* 10 (2015), http://kns55.en.eastview.com/kcms/detail/detail.aspx?recid=&FileName=GUOF201510009&DbName=CJFD2015&DbCode=CJFD.

17 Andrew Erickson and Conor Kennedy, "Shedding Light on China's Maritime Militia," *The Maritime Executive*, 3 November 2015, https://maritime-executive.com/editorials/shedding-light-on-chinas-maritime-militia.

18 Conor Kennedy and Andrew Erickson, "Model maritime militia: Tanmen's leading role in the April 2012 Scarborough shoal incident," *CIMSEC*, 21 April 2016, https://cimsec.org/model-maritime-militia-tanmens-leading-role-april-2012-scarborough-shoal-incident/.

19 Green et al., "Countering Coercion," 202-223.

20 Ibid., 202-223.

21 Kennedy and Erickson, "China Maritime Report," 10-11.

22 The Defense Department, "Summary of the Irregular Warfare Annex to the National Defense Strategy" (Washington DC, 2 October 2022), 2, https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.

23 Jeff Himmelman, "A Game of Shark and Minnow," *The New York Times*, 24 October 2013, https://www.nytimes.com/newsgraphics/2013/10/27/south-china-sea/index.html.

24 "Timeline: China's Maritime Disputes," *Council on Foreign Relations*, https://www.cfr.org/timeline/chinas-maritime-disputes, accessed 12 July 2023.

25 Green et al., "Countering Coercion," 52-65.

26 Ibid., 52.

27 Ibid., 52-65.

28 Ibid., 95-123.

29 Brad Lendon, "Beijing Has a Navy It Doesn't Even Admit Exists, Experts Say. And It's Swarming Parts of the South China Sea," *CNN*, 13 April 2021, https://www.cnn.com/2021/04/12/china/china-maritime-militia-explainer-intl-hnk-ml-dst/index.html.

30 The White House, "Statement by National Security Council Spokesperson Emily Horne on National Security Advisor Jake Sullivan's Call with National Security Advisor Hermogenes Esperon of the Philippines," The White House, 1 April 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/statement-by-national-security-council-spokesperson-emily-horne-on-national-security-advisor-jake-sullivans-call-with-national-security-advisor-hermogenes-esperon-of-the-philippines/.

31 "China Accused of Fresh Territorial Grab in South China Sea," *Bloomberg.Com*, 20 December 2022, https://www.bloomberg.com/news/articles/2022-12-20/china-accused-of-building-on-unoccupied-reefs-in-south-china-sea.

32 Alastair Johnston, "China in a World of Orders: Rethinking Compliance and Challenge in Beijing's International Relations," *International Security*, Vol. 44, no. 2 (2019): 57; and Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM | National Defense University*, November 2018, 33.

33 Johnston, "China in a World of Orders," 29-31.

34 Ronald O'Rourke, "U.S.-China Strategic Competition in South and East China Seas: Background and Issues for Congress" *Congressional Research Service*, 26 January 2022, 5, https://crsreports.congress.gov/search/#/?termsToSearch=R42784&orderBy=Relevance.

35 Ibid., 11.

36 M. Taylor Fravel, "Threading the Needle: The South China Sea Disputes and U.S.-China Relations," 2016, 27, https://papers.ssrn.com/abstract=2807181.

37 Ketian Zhang, "Cautious Bully: Reputation, Resolve, and Beijing's Use of Coercion in the South China Sea," *International Security*, Vol. 44, no. 1 (2019): 119.

38 David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 175.

39 Molly Dunigan et al., "What Is Maritime Irregular Warfare?," in *Characterizing and Exploring the Implications of Maritime Irregular Warfare* (Santa Monica: RAND Corporation, 2012), 14, https://www.jstor.org/stable/10.7249/mg1127navy.9.

40 Andrew Erickson and Conor Kennedy, "China's Maritime Militia," *Center for Naval Analyses Cooperation*, 2016, 28, https://www.cna.org/archive/CNA_Files/pdf/chinas-maritime-militia.pdf.

41 Ibid., 28.

42 Andrew S. Erickson, *Maritime Gray Zone Operations: Challenges and Countermeasures in the Indo-Pacific*, 1st ed. (London: Routledge, 2022), 136.

43 Erickson, 135-139.

44 Andrew Erickson and Conor Kennedy, "Trailblazers in Warfighting: The Maritime Militia of Danzhou | Center for International Maritime Security," 1 February 2016, https://cimsec.org/trailblazers-warfighting-maritime-militia-danzhou/.

45 Ibid.

46 Office of the Secretary of Defense, "DoD Releases 2021 Report on Military and Security Developments Involving the People's Republic of China," U.S. Department of Defense, 2021, https://www.defense.gov/News/Releases/Release/Article/2831819/dod-releases-2021-report-on-military-and-security-developments-involving-the-pe.

47 James Kraska and Raul A. Pedrozo, *Disruptive Technology and the Law of Naval Warfare* (New York: Oxford University Press, 2022), 61-62.

48 Ibid., 63.

49 NATO Special Operations Headquarters, *Comprehensive Defence Handbook*, Vol. 1, (Mons: NATO, 2020), 15.

50 Michael A. McDevitt, *China as a Twenty-First-Century Naval Power: Theory, Practice, and Implications* (Annapolis, MD: Naval Institute Press, 2020), 176.

51 Hoffman, "Examining Complex Forms of Conflict," 33.

52 Ibid., 38.

53 John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare* (Cambridge; Medford: Polity, 2021), 78-82.

54 Ibid., 80.

55 Ibid., 82.

56 Kilcullen, *The Dragons and the Snakes*, 198-199.

57 Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Coercion: The Evolving Character of Cyber Power and Strategy* (New York: Oxford University Press, 2018), 150-151; and Office of the Secretary of Defense, "DOD Releases 2021," act 34.

58 Mark A. Stokes, "China's Maritime Militia and Reconnaissance-Strike Operations," in *China's Maritime Gray Zone Operations*, ed. Andrew S. Erickson and Ryan D. Martinson (Annapolis, Maryland: Naval Institute Press, 2019), 155-167.

59 Ibid., 156.

60 Ibid., 158.

61 Ibid., 156, 160.

62 Kraska and Pedrozo, *Disruptive Technology*, 68-70.

63 "YJ-18," Missile Threat, 28 July 2021, https://missilethreat.csis.org/missile/yj-18/.

64 Kraska and Pedrozo, *Disruptive Technology*, 68.

65 "Mind the Gap: How China's Civilian Shipping Could Enable a Taiwan Invasion," *War on the Rocks*, 16 August 2021, https://warontherocks.com/2021/08/mind-the-gap-how-chinas-civilian-shipping-could-enable-a-taiwan-invasion/.

66 Richard K. Betts, "The Lost Logic of Deterrence," *Foreign Affairs*, Vol. 92, no. 2 (March-April 2013).

67 "SOUTHCOM's 2023 Posture Statement to Congress," March 2023, 6, https://www.southcom.mil/Media/Special-Coverage/SOUTHCOMs-2023-Posture-Statement-to-Congress/.

68 Office of the Secretary of Defense, "DoD Releases 2021," 7.

69 Ibid., 90.

70 Erickson and Martinson, *China's Maritime Gray Zone Operations*, 141 and 160.

71 Office of the Secretary of Defense, "DoD Releases 2021," iv.

72 Liang Qiao and Xiangsui Wang, *Unrestricted Warfare* (Brattleboro: Echo Point Books & Media, 2015).

73 Ibid., xxi–xxii.

74 Ibid., 38-43.

CHAPTER 8

1 Stelios Michalopoulos and Elias Papaioannou, "The scramble for Africa and its legacy," in Palgrave MacMillan, ed., *The New Palgrave Dictionary of Economics* (London: Palgrave MacMillan, 2016).

2 Agnieszka Paczyńska, "Russia in Africa: Is great power competition returning to the continent?" *Deutsches Institut für Entwicklungspolitik (DIE)*, (2020).

3 David Ehl, "Russia's Wagner Group in Africa: More than mercenaries." *Deutsche Welle*, 17 April 2023, https://www.dw.com/en/more-than-mercenaries-russias-wagner-group-in-africa/a-64822234.

4 Nosmot Gbadamosi, "Will Wagner Stay in Africa?" *Foreign Policy*, 28 June 2023, https://foreignpolicy.com/2023/06/28/will-wagner-stay-in-africa/.

5 Paczyńska, "Russia in Africa."

6 Statement of General Michael E. Langley, United States Marine Corps Commander, United States Africa Command Before the Armed Services Committee, 118th United States Congress, 1-19 (2023) (General Michael E. Langley, United States Marine Corps).

7 "SOCAFRICA: U.S. Special Operations Command Africa," USSOCOM, socom.mil/socaf, accessed 7 June 2023.

8 Paul Stronski, "Russia's Growing Footprint in Africa's Sahel Region," *Carnegie Endowment for International Peace*, 28 February 2023, https://carnegieendowment.org/2023/02/28/russia-s-growing-footprint-in-africa-s-sahel-region-pub-89135.

9 Hotaka Nakamura, "Russia's new military: The rise of Prigozhin and the Wagner Group," *Middle East Institute*, 16 December 2022, https://www.mei.edu/publications/russias-new-military-rise-prigozhin-and-wagner-group.

10 "Who is the head of the Russian mercenary group bashing the military's role in Ukraine?" *The Associated Press*, 24 May 2023, https://apnews.com/article/russia-wagner-prigozhin-ukraine-war-fa08125fb220b1bc49e6d12fe5a7159d; Nakamura, "Russia's new military"; and Pjotr Sauer, "Putin ally Yevgeny Prigozhin admits founding Wagner mercenary group," *The Guardian*, 26 September 2023, https://www.theguardian.com/world/2022/sep/26/putin-ally-yevgeny-prigozhin-admits-founding-wagner-mercenary-group.

11 Raphael Parens, Colin P. Clarke, Christopher Faulkner and Kendal Wolf, "The Wagner Group's Expanding Global Footprint," *Foreign Policy Research Institute*, 27 April 2023, https://www.fpri.org/article/2023/04/the-wagner-groups-expanding-global-footprint/.

12 Nicolas Camut, "Wagner's feud with Russian army escalates amid reports of not so friendly fire," *Politico*, 5 June 2023, https://www.politico.eu/article/russia-soldiers-friendly-fire-wagner-group-yevgeny-prigozhin-bakhmut-ukraine-war/.

13 "Timeline: How Wagner Group's revolt against Russia unfolded," *Al Jazeera*, 24 June 2023, https://www.aljazeera.com/news/2023/6/24/timeline-how-wagner-groups-revolt-against-russia-unfolded; Nicolas Camut, "Putin met Prigozhin in Moscow after Wagner mutiny,"

Politico, 10 July 2023, https://www.politico.eu/article/vladimir-putin-met-wagner-group-yevgeny-prigozhin-moscow-after-mutiny/; Kevin Shalvey, "Russian rebellion timeline: How the Wagner uprising against Putin unfolded and where Prigozhin is now," *ABC News*, 10 July 2023, https://abcnews.go.com/International/wagner-groups-rebellion-putin-unfolded/story?id=100373557.

14 Ehl, "Russia's Wagner Group in Africa."

15 Ibid; and Stronski, "Russia's Growing Footprint."

16 Alessandro Arduino, "Wagner Group in Africa: Russia's presence on the continent increasingly relies on mercenaries." *The Conversation*, 9 February 2023, https://theconversation.com/wagner-group-in-africa-russias-presence-on-the-continent-increasingly-relies-on-mercenaries-198600; Colin P. Clarke, "How Russia's Wagner Group is Fueling Terrorism in Africa." *Foreign Policy*, 25 January 2023, https://foreignpolicy.com/2023/01/25/russia-wagner-group-africa-terrorism-mali-sudan-central-african-republic-prigozhin/; Ehl, "Russia's Wagner Group in Africa;" Greg Miller and Robyn Dixon, "Wagner Group surges in Africa as U.S. influence fades, leak reveals," *The Washington Post*, 23 April 2023, https://www.washingtonpost.com/world/2023/04/23/wagner-russia-africa-leaked-documents/; and Stronski, "Russia's Growing Footprint."

17 Colin P. Clarke, Raphael Parens, Christopher Faulker and Kendal Wolf, "Is Wagner Pivoting Back to Africa?," *Foreign Affairs*, 11 May 2023, https://www.foreignaffairs.com/africa/ukraine-wagner-pivoting-back-africa; and Parens et al., "The Wagner Group's Expanding Global Footprint."

18 Sauer, "Putin ally Yevgeny Prigozhin."

19 Clarke et al., "Is Wagner Pivoting Back to Africa?"

20 Gbadamosi, "Will Wagner Stay in Africa?"

21 Ibid.; Jason Burke, "'It is like a virus that spreads': business as usual for Wagner group's extensive Africa network," *The Guardian*, 6 July 2023, https://www.theguardian.com/world/2023/jul/06/putin-wagner-africa-business-yevgeny-prigozhin-kremlin.

22 Judicael Yongo, "Central African Republic says Wagner troop movement is rotation not departure," *Reuters*, 8 July 2023, https://www.reuters.com/world/africa/central-african-republic-says-wagner-troop-movement-is-rotation-not-departure-2023-07-08/.

23 András Rácz, "Band of Brothers: The Wagner Group and the Russian State," *Center for Strategic & International Studies*, 21 September 2020, https://www.csis.org/blogs/post-soviet-post/band-brothers-wagner-group-and-russian-state.

24 Ibid.

25 Ibid.

26 Catrina Doxsee, "How Does the Conflict in Sudan Affect Russia and the Wagner Group?" *Center for Strategic and International Studies*, 20 April 2023, https://www.csis.org/analysis/how-does-conflict-sudan-affect-russia-and-wagner-group; and Ehl, "Russia's Wagner Group in Africa."

27 Miller and Dixon, "Wagner Group surges in Africa."

28 Clarke, "How Russia's Wagner Group."

29 Miller and Dixon, "Wagner Group surges in Africa."

30 Wassim Nasr, "How the Wagner Group Is Aggravating the Jihadi Threat in the Sahel," *CTC Sentinel*, November/December 2022, https://ctc.westpoint.edu/how-the-wagner-group-is-aggravating-the-jihadi-threat-in-the-sahel/.

31 Clarke, "How Russia's Wagner Group."

32 Nasr, "How the Wagner Group Is Aggravating the Jihadi Threat."

33 Clarke, "How Russia's Wagner Group."

34 Nasr, "How the Wagner Group Is Aggravating the Jihadi Threat."

35 Ehl, "Russia's Wagner Group in Africa."

36 Lee Komminoth, "Russia's Wagner Group could make millions from exploitation of African rainforest." *African Business*, 15 September 2022, https://african.business/2022/09/resources/russias-wagner-group-involved-in-central-african-forestry-trade.

37 Ehl, "Russia's Wagner Group in Africa."

38 Danielle Paquette, "Russian mercenaries have landed in West Africa, pushing Putin's goals as Kremlin is increasingly isolated," *The Washington Post*, 9 March 2022, https://www.washingtonpost.com/world/2022/03/09/mali-russia-wagner/.

39 Ehl, "Russia's Wagner Group in Africa."

40 Ibid.

41 Doxsee, "How Does the Conflict in Sudan."

42 Geoffrey F. Gresh, "Europe's New Maritime Security Reality: Chinese Ports, Russian Bases, and the Rise of Subsea Warfare," *Brookings Institute*, February 2023.

43 Joseph Siegle, Russia in Africa: Undermining Democracy through Elite Capture," *Africa Center for Strategic Studies*, 24 September 2021, https://africacenter.org/spotlight/russia-africa-undermining-democracy-elite-capture/.

44 "US accuses Wagner Group of supplying missiles to Sudan's RSF." *Al Jazeera*, 25 May 2023, https://www.aljazeera.com/news/2023/5/25/us-accuses-wagner-group-of-supplying-missiles-to-sudans-rsf.

45 Nathaniel Reynolds, "Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group," *Carnegie Endowment*, 8 July 2019, https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442.

46 Doxsee, "How Does the Conflict in Sudan."

47 Stronski, "Russia's Growing Footprint."

48 Miller and Dixon, "Wagner Group Surges in Africa."

49 Clarke, "How Russia's Wagner Group"; and Clarke et al., "Is Wagner Pivoting Back to Africa?"

50 Ehl, "Russia's Wagner Group in Africa."

51 Siegle, "Russia in Africa."

52 Gbadamosi, "Will Wagner Stay in Africa?"

53 Miller and Dixon, "Wagner Group surges in Africa."

54 Ehl, "Russia's Wagner Group in Africa."

55 Parens et al., "The Wagner Group's Expanding Global Footprint."

56 Ibid.

57 T. Clifton Morgan, Constantinos Syropoulos and Yoto V. Yotov. "Economic sanctions: Evolution, consequences, and challenges," *Journal of Economic Perspectives*, Vol. 37, no. 1 (2023): 3-29.

58 Brehima Sow, "The rise of terrorism in Mali: A review of the historical causes and the failures of both Malian and International efforts," Master's Thesis, Naval Postgraduate School, 2018.

59 Nasr, "How the Wagner Group Is Aggravating the Jihadi Threat."

60 Sauer, "Putin ally Yevgeny Prigozhin."

61 Molly Dunigan and Ben Connable, "Russian Mercenaries in Great-Power Competition: Strategic Supermen or Weak Link?" *The RAND Blog*, 9 March 2021, https://www.rand.org/blog/2021/03/russian-mercenaries-in-great-power-competition-strategic.html.

62 Nasr, "How the Wagner Group Is Aggravating the Jihadi Threat."

63 Dunigan and Connable, "Russian Mercenaries in Great-Power Competition."

64 Clarke et al., "Is Wagner Pivoting Back to Africa?"

65 Parens et al., "The Wagner Group's Expanding Global Footprint."

66 Nasr, "How the Wagner Group Is Aggravating the Jihadi Threat."

67 Lisa Hultman, "Battle losses and rebel violence: Raising the costs for fighting," *Terrorism and Political Violence*, Vol. 19, no. 2 (2007): 205-222; and Sara M.T. Polo and Belén González, "The power to resist: mobilization and the logic of terrorist attacks in civil war," *Comparative Political Studies*, Vol. 53, no. 13 (2020): 2029-2060.

68 Dursun Peksen, "When do imposed economic sanctions work? A critical review of the sanctions effectiveness literature," *Defence and Peace Economics*, Vol. 30, no. 6 (2019): 635-647.

69 Navin A. Bapat, "Transnational terrorism, US military aid, and the incentive to misrepresent," *Journal of Peace Research*, Vol. 48, no. 3 (2011): 303-318.

70 Joseph K. Young and Michael G. Findley, "Can peace be purchased? A sectoral-level analysis of aid's influence on transnational terrorism," *Public Choice*, Vol. 149 (2011): 365-381.

CHAPTER 9

1 "Beachhead (U.S. DoD Definition)," https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=702, accessed 25 February 2022.

2 Geoffrey A. Moore, *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers*, Third edition (New York, NY: HarperBusiness, an imprint of HarperCollins Publishers, 2014), 66.

3 David A. Baldwin and Ethan B. Kapstein, *Economic Statecraft*, New edition (Princeton: Princeton University Press, 2020), 18-24.

4 Congressional Research Service, "Renewed Great Power Competition: Implications for Defense - Issues for Congress," 7 October 2021, 4, chrome-extension://efaidnbmnnnibcajpcglclefindmkaj/https://apps.dtic.mil/sti/pdfs/AD1105860.pdf.

5 Joint Chiefs of Staff, "Joint Concept for Competing" (Washington D.C.: Department of Defense, 2022), 5.

6 William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (Novato: Presidio, 1995), 5.

7 Odd Arne Westad, *The Cold War: A World History*, First edition (New York: Basic Books, 2017), 32.

8 Martin Shubik, "Unconventional Methods of Economic Warfare," *Conflict*, Vol. 1, no. 3 (1979): 222; and William J. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control* (London: Cornell University Press, 2016), 13.

9 See NPS MA thesis on this subject at https://calhoun.nps.edu/handle/10945/72164.

10 Ministry of Justice and Public Security, "Government Blocks Sale of Bergen Engines," Government.no (regjeringen.no, 26 March 2021), https://www.regjeringen.no/en/aktuelt/government-blocks-sale-of-bergen-engines/id2841869/.

11 "Engine Supplier to Norwegian Spy Ship Bought by Russian-Controlled Company," *The Independent Barents Observer*, https://thebarentsobserver.com/en/security/2021/02/russian-company-buys-builder-engines-norwegian-spy-ship, accessed 16 November 2021.

12 "Skriftlig spørsmål fra Emilie Mehl (Sp) til forsvarsministeren," [Written question from Emilie Mehl (Sp) to the Minister of Defense], DOK15, Stortinget, March 1, 2021, https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=83591.

13 "Company History | About," *Bergen Engines* (blog), https://www.bergenengines.com/about/history/, accessed 2 December 2022.

14 "Acquires Rolls-Royce Commercial Marine - Kongsberg," https://www.kongsberg.com/no/kmagazine/2018/7/acquires-rolls-royce-commercial-marine/, accessed 2 December 2022.

15 "Who we are, Kongsberg," https://www.kongsberg.com/no/who-we-are/, accessed 2 December 2022.

16 "*Metoderapport Skup 2021 - Salget Av Bergen Engines* [Methodology Report Skup 2021 - The Sale of Bergen Engines] (Bergen, Norway: Bergens Tidende, 2021), 39, https://www.skup.no/rapporter/2021/salget-av-bergen-engines.

17 "Press Releases," https://www.rolls-royce.com/media/press-releases.aspx, accessed 23 May 2023.

18 Justis- og Beredskapsdepartementet [Ministry of Justice], "Kongelig Resolusjon - Stans av salget av Bergen Engines AS," [Royal Decree - Stopping the sale of Bergen Engines AS], 2021, 21/1898, 47.

19 "Russlands største togprodusent kjøper Bergen Engines fra Rolls-Royce [Russia's largest train manufacturer buys Bergen Engines from Rolls-Royce]," February 4, 2021, https://e24.no/i/x3OLrl.

20 "Skriftlig spørsmål fra Emilie Mehl (Sp) til forsvarsministeren," [Written question from Emilie Mehl (Sp) to the Minister of Defense].

21 "Bergen Engines-saken: – Regjeringen må stoppe salget, vitner om komplett svikt i alle ledd [The Bergen Engines case: - The government must stop sales, evidence of complete failure at all levels]," 2 March 2021, https://e24.no/i/aP3WkO.

22 "Stortinget retter hard kritikk mot regjeringen i Bergen Engines-saken [The Parliament harshly criticizes the government in the Bergen Engines case]," 19 May 2021, https://e24.no/i/39v9xP.

23 According to *Forbes*, Makhmudov is listed as the 380th richest person in the world, with a total wealth of more than 6.5 billion USD, "Iskander Makhmudov," *Forbes*, https://www.forbes.com/profile/iskander-makhmudov/, accessed 2 December 2022.

24 "Andrei Bokarev," *Forbes*, https://www.forbes.com/profile/andrei-bokarev/, accessed 2 December 2022.

25 Benjamin J. Cohen, "Sovereign Wealth Funds and National Security: The Great Tradeoff," *International Affairs*, Vol. 85, no. 4 (July 1, 2009): 713-731.

26 "Foreign Direct Investment," SSB, https://www.ssb.no/en/utenriksokonomi/fordringer-og-gjeld-overfor-utlandet/statistikk/direkteinvesteringer, accessed 27 February 2022.

27 "11322: Direct Investments (NOK Million), by Transaction, Country, Contents and Year. Statbank Norway," SSB, https://www.ssb.no/en/system/, accessed 27 February 2022.

28 Waage et al, "Utenlandske investeringer og andre økonomiske virkemidler - når truer de nasjonal sikkerhet?," [Foreign Investments and Other Economic Means - When Do They Threaten National Security?], 46.

29 Ibid., 52.

30 "ТМХ Пошел За Двигателями в Норвегию [TMH Went to Norway for Engines]," Портньюс, https://portnews.ru/digest/22304/, accessed 2 December 2022.

31 *Metoderapport Skup 2021 - Salget Av Bergen Engines* [Methodology Report Skup 2021 - The Sale of Bergen Engines].

32 "Engine Supplier to Norwegian Spy Ship Bought by Russian-Controlled Company," *The Independent Barents Observer*, https://thebarentsobserver.com/en/security/2021/02/russian-company-buys-builder-engines-norwegian-spy-ship, accessed 16 November 2021.

33 *Metoderapport Skup 2021 - Salget Av Bergen Engines,* [Methodology Report Skup 2021 - The Sale of Bergen Engines], 7.

34 Konstantin Nikolayevich Dorokhin, trans., review of *Transmashholding Magazine for Partners*, by Larisa Rudakova, *Futura Media*, 2017, 16.

35 Ibid., 16.

36 *Metoderapport Skup 2021 - Salget Av Bergen Engines,* [Methodology Report Skup 2021 - The Sale of Bergen Engines], 36.

37 Ibid., 38.

38 Reuters, "Despite Putin's Swagger, Russia Struggles to Modernize Its Navy," *The Moscow Times*, 21 February 2019, https://www.themoscowtimes.com/2019/02/21/despite-putins-swagger-russia-struggles-to-modernise-its-navy-a64582.

39 *Metoderapport Skup 2021 - Salget Av Bergen Engines,* [Methodology Report Skup 2021 - The Sale of Bergen Engines], 12.

40 Ibid., 51.

41 "Kongelig Resolusjon - Stans av salget av Bergen Engines AS," [Royal Decree - Stopping the sale of Bergen Engines AS], 4.

42 Justis- og Beredskapsdepartementet [Ministry of Justice], "Kongelig Resolusjon - Stans av salget av Bergen Engines AS [Royal Decret - Stopping the sale of Bergen Engines AS]," 5.

43 Erlend Hammer, "Haakonsvern orlogsstasjon [Haakonsvern Naval Base]," in *Store norske leksikon*, 7 July 2022, http://snl.no/Haakonsvern_orlogsstasjon.

44 "Lov Om Informasjon Om Bestemt Angitte Områder, Skjermingsverdige Objekter Og Bunnforhold [Act on Information on Specified Areas, Objects Worthy of Protection and Bottom Conditions] - Lovdata," https://lovdata.no/dokument/NL/lov/2017-06-21-88, accessed 31 December 2022.

45 Justis- og Beredskapsdepartementet [Ministry of Justice], "Kongelig Resolusjon - Stans av salget av Bergen Engines AS," [Royal Decree - Stopping the sale of Bergen Engines AS], 4.

46 Yen Nee Lee, "China Took Control of an Italian Military Drone Maker without Authorities Knowing It, Report Says," *CNBC*, 16 November 2021, https://www.cnbc.com/2021/11/16/china-reportedly-took-control-of-an-italian-military-drone-maker-quietly.html.

47 Kurt M. Campbell and Ely Ratner, "The China Reckoning: How Beijing Defied American Expectations," *Foreign Affairs* (2018): 2.

48 Kadri Kaska, Henrik Beckvard, and Tomáš Minárik, "Huawei, 5G and China as a Security Threat" (Brussels: NATO Cooperative Cyber Defence Centre of Excellence, 2019), 11.

49 Jānis Bērziņš, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *The Journal of Slavic Military Studies*, Vol. 33, no. 3 (July 2, 2020): 359-362; Kerry K. Gershaneck, *Political Warfare: Strategies for Combating China's Plan to "Win without Fighting"* (Quantico, VA: Marine Corps University Press, 2020), 48-49; and Liang Qiao and Xiangsui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America*, 1st Indian ed (Dehradun: Natraj Publishers, 2007), 118.

CHAPTER 10

1 Steve Hendricks, *A Kidnapping in Milan: The CIA on Trial* (New York: W.W. Norton, 2010).

2 Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, Eighth edition (Thousand Oaks: CQ Press, 2019), 238.

3 Hendricks, *A Kidnapping in Milan*.

4 Cortney Weinbaum and John N. T. Shanahan, "Intelligence in a Data-Driven Age," *Joint Forces Quarterly*, Vol. 90, 3rd Quarter (2018): 4.

5 Jonathan Lord, "Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age," *International Journal of Intelligence and CounterIntelligence*, Vol. 28, no. 4 (2015): 666-691.

6 Non-uniformed military personnel can lose protection under the Geneva Conventions (e.g., treatment as prisoners of war) and be charged for espionage, which is an act punishable by lengthy prison terms or, in some countries, the death penalty. The chapter does not cover an in-depth discussion of legal considerations for covert SOF operations. Furthermore, the chapter does not discuss the U.S. legal term of "covert action," an official and defined task for the U.S. CIA.

7 NATO, *Allied Joint Doctrine for Special Operations AJP-3.5*, Edition B Version 1 (Norfolk, Virginia: NATO Standardization Office, 2019), 1.

8 Ibid., 1.

9 NATO's SOF doctrine AJP-3.5, Edition B Version 1 (2019) does not include the term "covert," while the U.S. Army Doctrine Publication (ADP) 3-05 (2019) names both "covert" and "clandestine" capabilities for U.S. Army SOF units; NATO, *Allied Joint Doctrine for*

Special Operations AJP-3.5; Department of the Army, *Army Special Operations*, Army Doctrine Publication, ADP 3-05 (Washington, D.C.: Headquarters Department of the Army, 2019).

10 NATO, *NATO Glossary of Terms and Definitions AAP-06*, 2021 ed (Norfolk, Virginia: NATO Standardization Office, 2021), 35.

11 Ibid., 26.

12 Lowenthal, *Intelligence: From Secrets to Policy*, 447.

13 David V. Gioe, Michael S. Goodman, and David S. Frey, "Unforgiven: Russian Intelligence Vengeance as Political Theater and Strategic Messaging," *Intelligence and National Security*, Vol. 34, no. 4 (June 7, 2019): 562.

14 Rafael Epstein and Dylan Welch, "Secret SAS Squadron Sent to Spy in Africa," *The Sydney Morning Herald*, 12 March 2012, https://www.smh.com.au/politics/federal/secret-sas-squadron-sent-to-spy-in-africa-20120312-1uwjs.html.

15 Lowenthal, *Intelligence: From Secrets to Policy*, 105 and 125.

16 João Rafael Gonçalves Evangelista et al., "Systematic Literature Review to Investigate the Application of Open-Source Intelligence (OSINT) with Artificial Intelligence," *Journal of Applied Security Research*, Vol. 16, no. 3 (2021): 345-369.

17 Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *SSRN Electronic Journal* (2018).

18 John A. Gentry, "Intelligence Services and Special Operations Forces: Why Relationships Differ," *International Journal of Intelligence and CounterIntelligence*, Vol. 30, no. 4 (October 2, 2017): 647-686.

19 Lowenthal, *Intelligence: From Secrets to Policy*, 132.

20 Fátima C. Carrilho Santos, "Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis," *Journalism and Media*, Vol. 4, no. 2 (June 3, 2023): 679-687.

21 Michael Althoff, "Human Intelligence," in Mark M. Lowenthal and Robert M. Clark, eds., *The Five Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, Sage Publications, 2016), 74.

22 Purchasing local hardware and communication devices can have detrimental consequences. For example, SIM-card registration can be challenging as most countries demand personal data, including passport information, and several countries require biometrical data like fingerprints. Paul Bischoff, "Which Governments Impose SIM-Card Registration Laws to Collect Data on Their Citizens?" *Comparitech* (blog), 20 March 2023, https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/.

23 Andrew Hayward, "What Is a Blockchain Phone? A Look at 7 Current and Upcoming Crypto Handsets," *Decrypt* (blog), 26 October 2019, https://decrypt.co/10794/best-blockchain-phones/.

24 Mathieu Couillard, "The Role of Deceptive Defense in Cyber Strategy," unpublished Master's Thesis, NPS, 2023), https://hdl.handle.net/10945/72146.

25 Vasileios Mavroeidis et al., "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications*, Vol. 9, no. 3 (2018).

26 Cortney Weinbaum et al., *Mapping Chinese and Russian Military and Security Exports to Africa* (Santa Monica: RAND Corporation, 2022).

27 John Tullius, "Intelligence for Special Operations Forces," Unpublished Manuscript, 2022; and African Union, *African Union Strategy for a Better Integrated Border Governance* (Addis Ababa: African Union Commission, 2020).

28 The PRC's social-control system serves as a striking example of the combination of biometrics, databases, and AI to form an enormous surveillance system that is also utilized for substantial counterintelligence efforts. Derek Grossman et al., *Chinese Views of Big Data Analytics* (Santa Monica, CA: RAND Corporation, 2020); Blake W. Mobley and Carl Anthony Wege, "Evading Secret Police: Counterintelligence Vulnerabilities in Authoritarian States," *International Journal of Intelligence and CounterIntelligence*, Vol. 36, no. 1 (January 2, 2023): 179-198; Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, Whitehall Report 2-15 (London: RUSI, 2015).

29 Michael Lyons, "Number of CCTV Cameras in the UK Reaches 5.2 Million," *Counter Terror Business*, 19 November 2020, https://counterterrorbusiness.com/news/19112020/number-cctv-cameras-uk-reaches-52-million.

30 While the British government has invoked clear legal guidelines for their surveillance system, the same legal frameworks governing Western democracies may not apply in other regions and countries with authoritarian regimes where SOF might be deployed.

31 Linda Schlegel and Amarnath Amarasingam, *Examining the Intersection Between Gaming and Violent Extremism* (New York: United Nations Office of Counter-Terrorism (UNCCT), 2022); Radicalisation Awareness Network, *Extremists' Use of Video Gaming – Strategies and Narratives* (European Union Radicalisation Awareness Network, 2020).

32 Small SIGINT devices that can pick up the phones' individual International Mobile Subscriber Identity (IMSI) number from up to a few hundred meters away.

33 Sophisticated tracking software can infect smartphones and laptops without any unintended support or knowledge by the user. Especially private companies like NSO (Israel) or RCS Labs (Italy) are setting the pace in the development of digital surveillance tools. Colm Healy, "Pegasus, Predator, Hermit Spyware - NSO and Its Clones," *Corrata*, 3 April 2023, https://corrata.com/pegasus-predator-hermit-spyware-nso-and-its-clones/.

34 Habtamu Fuje, Saad Quayyum, and Tebo Molosiwa, "Africa's Growing Crypto Market Needs Better Regulations," *International Monetary Fund Blog* (blog), 22 November 2022, https://www.imf.org/en/Blogs/Articles/2022/11/22/africas-growing-crypto-market-needs-better-regulations#.

35 Lonnie Keene and Alan Brill, "Cryptocurrencies: The Next Generation of Terrorist Financing?" *Defence Against Terrorism Review*, Vol. 6, no. 1 (2014): 7-30.

36 Depending on the specific circumstances of the situation – peace, crisis, conflict, or war – strategic decision-makers have to accept a trade-off between safety and effectiveness. Urgency or relevance can enforce a higher risk acceptance for the forces on the ground.

37 David R. Shedd, "The Intelligence Posture America Needs in an Age of Great-Power Competition," *Index of U.S. Military Strength*, The Heritage Foundation, no. Essays 2021 (2021): 71.

CHAPTER 11

1 Micah Zenko, "100% Right 0% of the Time," *Foreign Policy* (blog), October 16, 2012, https://foreignpolicy.com/2012/10/16/100-right-0-of-the-time/, accessed 12 June 2023.

2 For the intents and purposes of this chapter, innovation simply refers to any change adopted by an organization close to the level of the invention's tipping point. Therefore, innovation does not guarantee implementation to the organization as a whole.

3 Similar to the biological evolutionary definition: "Any change in the structure or functioning of successive generations of a population that makes it better suited to its environment." "Adaptation," Oxford Reference, accessed 12 June 2023, https://doi.org/10.1093/oi/authority.20110803095350199.

4 "Combat Darwinism" is the natural selection which occurs during war. This concept is explored throughout Chapter 2: Adaptive Enemies and primarily refers to the changes in non-state enemies' tactics, techniques and procedures. David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 38-65.

5 Hugh W. Howard III, "NSWC Posture Statement of Rear Admiral H.W. Howard III, USN Commander, Naval Special Warfare Command, Before the 117TH Congress, Senate Armed Service Committee" (Washington, DC, April 27, 2022), 1.

6 Mark Moyar, *Oppose Any Foe: The Rise of America's Special Operations Forces*, First edition (New York: Basic Books, 2017), 127-128.

7 Ibid.

8 Evolution remains a contentious word within the innovation community, but military innovation is significantly more contentious. Barry Scott looks at 15 leading definitions of "military innovation" and then posits his own definition, while Michael Horowitz and Shira Pindyck look at over 65 interpretations of military innovation and also develop a new definition. Barry Scott, "Strategy Wars: An Ethnographic, Historical Case Study of the Chief of Naval Operations Strategic Studies Group, 1981-2016" (West Lafayette, IN: Purdue University, 2023), 44-69. Horowitz looks at over 65 interpretations of military innovation and also develops a new definition. Michael C. Horowitz and Shira Pindyck,

"What Is A Military Innovation and Why It Matters," *Journal of Strategic Studies*, March 22, 2022, https://www.tandfonline.com/doi/epdf/10.1080/01402390.2022.2038572?needAccess=true&role=button.

9 In this context, the user is applying the old technology/tactic for a purpose it was not originally intended for and is similar to the evolutionary concept of exaptation.

10 Dr. Nick Dew pointed out to the author that from a behavioural perspective, the opposite is often true; people tend to adopt small changes, while rejecting big changes. This claim is not disputed. The referenced statement simply implies that significant changes within an organization's rival spurs new practices, big or small, within its own organization.

11 Tai Ming Cheung, Thomas G. Mahnken, and Andrew L. Ross, "Assessing the State of Understanding of Defense Innovation," Research Brief, The Study of Innovation and Technology in China (La Jolla, CA: University of California Institute on Global Conflict and Cooperation, May 2018), 2.

12 "Success" here refers to the required degree of implementation needed to facilitate an organization's adaptation.

13 Mazes generated by Discovery Education's "maze generator". DiscoveryEducation, "Maze Generator," March 2023, https://puzzlemaker.discoveryeducation.com/maze.

14 Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, N.J: Princeton University Press, 2010), 30.

15 Ibid., 32.

16 Ibid., 33.

17 Ibid., 39.

18 Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford: Stanford University Press, 2010), 2.

19 Ibid., 16.

20 Adamsky describes holistic-dialectical thought as the practice of considering the entire environment as a single unit, similar to inductive reasoning, as well as recognizing contradictions and changes in the context, and then seeking a synthesis between opposing viewpoints. He also describes logical-analytical thought as focusing on a particular object, separating it from its surroundings, and then classifying it into groups using formal logic to understand and anticipate its actions, similar to deductive reasoning. Additionally, analytical thinking eliminates contradictions and does not encounter gaps in concepts. Ibid., 18-20.

21 Cheung, Mahnken, and Ross, "Assessing the State of Understanding of Defense Innovation," 3.

22 Benjamin M. Jensen, *Forging The Sword: Doctrinal Change in the U.S. Army* (Stanford, California: Stanford Security Studies, an imprint of Stanford University Press, 2016), 1-2.

23 Ibid., 1.

24 Mazes generated by Discovery Education's "Maze Generator." DiscoveryEducation, "Maze Generator."

25 Eric von Hippel, "'Sticky Information' and the Locus of Problem Solving: Implications for Innovation," *Management Science*, Vol. 40, no. 4 (April 1994): 429-439.

26 Tony Bertuca, "House Defense Appropriators Move to Cut Procurement, Raise R&D Spending," *InsideDefense.Com*, June 14, 2022, sec. Unmanned Systems Alert. In fact, the current House bill "proposes $131.7 billion for research, development, test and evaluation, an increase of $1.6 billion above the budget request and an increase of $12.5 billion above the level enacted in FY-22."

27 Artwork by author.

28 Kendrick Kuo, "Dangerous Changes: When Military Innovation Harms Combat Effectiveness," *International Security*, Vol. 47, no. 2 (October 1, 2022): 49.

29 Grace Noto, "5 Proposed Military Technologies That Failed Hilariously," *Electronic Products* (blog), March 14, 2014, https://www.electronicproducts.com/5-proposed-military-technologies-that-failed-hilariously/.

30 Ibid.

31 Artwork by author.

32 Joseph M. Molloy et al., "Musculoskeletal Injuries and United States Army Readiness Part I: Overview of Injuries and Their Strategic Impact," *Military Medicine*, Vol. 185, no. 9-10 (September 18, 2020): e1462.

33 Baris K. Gun et al., "Prevalence and Risk Factors for Musculoskeletal Back Injury Among U.S. Army Personnel," *Military Medicine*, Vol. 187, no. 7-8 (July 1, 2022): e819.

34 Mark Thompson uses data from the Pentagon which demonstrates that "80% of recent troops come from a family where at least one parent, grandparent, aunt or uncle, sibling or cousin has also worn their nation's uniform." Mark Thompson, "Here's Why the U.S. Military Is a Family Business," *Time*, 10 March 2016, https://time.com/4254696/military-family-business/.

35 Paul A. Geroski, *The Evolution of New Markets* (Oxford: Oxford University Press, 2017), 46.

36 Ibid., 53-55.

37 "Failure" refers to an innovation's inability to excel past its tipping point (Author's definition). Statistics and claim derived from John T. Gourville, "Eager Sellers and Stony Buyers: Understanding the Psychology of New-Product Adoption," *Harvard Business Review*, no. 4516 (June 2006): 1.

38 Gourville, "Eager Sellers," 6.

39 See "The endowment effect," Ibid., 5.

40 Ibid., 7.

41 Jensen, *Forging the Sword*, 3.

42 Adamsky for culture's role in grasping change. Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*; Horowitz for organizational capital and the willingness to accept innovation. Michael C. Horowitz, *The Diffusion of Military Power*, 30.

43 Ron Adner, "Match Your Innovation Strategy to Your Innovation Ecosystem," *Harvard Business Review* (April 2006): 3-5.

44 The assigned "Likely Approval Rate" for each individual in Figure 11.4 is arbitrary. However, this attribute is of little consequence, as the primary objective of this illustration is to accentuate the magnitude of interdependence risks that any innovation must undergo. Concept was derived from Ron Adner. Ibid., 5.

45 Nick Dew, Kathryn Aten, and Geraldo Ferrer, "How Many Admirals Does It Take To Change A Light Bulb? Organizational Innovation, Energy Efficiency, and the United States Navy's Battle Over LED Lighting," *Energy Research & Social Science*, Vol. 27 (May 2017): 57-67.

46 Ibid., 59.

47 Ibid., 63-65.

48 Steve Blank, "Why Innovation Heroes Are a Sign of a Dysfunctional Organization," *Steve Blank* (blog), August 2021, https://steveblank.com/2021/08/25/why-innovation-heroes-are-a-sign-of-a-dysfunctional-organization/.

49 Ibid.

50 Ibid.

51 Department of Defense, *2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 10.

52 "The author would like to express his heartfelt gratitude to Professor Nicholas Dew for his invaluable contributions to the refinement and development of this chapter. His exceptional expertise and guidance in the fields of innovation adoption and implementation, as well as navigating innovation ecosystems, have been instrumental in shaping the ideas presented herein. Thank you Professor Dew!"

CHAPTER 12

1 ajeyaseelan, "John Maynard Keynes (1883–1946)," Collection at Bartleby.com, June 25, 2022, https://www.bartleby.com/lit-hub/respectfully-quoted/john-maynard-keynes-18831946-2/.

2 Department of Defense (DoD), *ATP 3-18.1 Special Forces Unconventional Warfare* (Washington D.C.: Department Of The Army, March 21, 2019), XV, https://Armypubs.Army.Mil/Productmaps/Pubform/Details.Aspx?PUB_ID=1006688.

3 Ivan Arreguín-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security*, Vol. 26, no. 1 (2001): 93-128.

4 Otto C. Fiala, *Resistance Operating Concept (ROC)* (Tampa: The Joint Special Operations University Press, 2020); and *NATO Comprehensive Defence Handbook*, A, Vol. 1, 2 vols. (Brussels: NATO Special Operations Headquarters, 2020).

5 *ATP 3-18.1*, 1-3.

6 "Revisiting the Social Movement Approach to Unconventional Warfare," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/revisiting-the-social-movement-approach-to-unconventional-warfare, accessed 15 June 2023.

7 *The Wiley Blackwell Companion to Social Movements*, 1st ed. (John Wiley & Sons, Ltd, 2018).

8 Robert D. Benford and David A. Snow, "Framing Processes and Social Movements: An Overview and Assessment," *Annual Review of Sociology*, Vol. 26 (2000): 611-639.

9 Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science*, Vol. 359, no. 6380 (March 9, 2018): 1146-1151.

10 *Comprehensive Defence Handbook*, 1:12.

11 Eran Amsalem and Alon Zoizner, "Real, but Limited: A Meta-Analytic Assessment of Framing Effects in the Political Domain," *British Journal of Political Science*, Vol. 52, no. 1 (January 2022): 221-237.

12 "Did Russia Influence Brexit? | Brexit Bits, Bobs, and Blogs | CSIS," https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit, accessed 15 June 2023.

13 Taras Kuzio, "Old Wine in a New Bottle: Russia's Modernization of Traditional Soviet Information Warfare and Active Policies Against Ukraine and Ukrainians," *The Journal of Slavic Military Studies*, Vol. 32, no. 4 (2 October 2019): 485-506.

14 "Chinese Communist Party Information Warfare: US–China Competition during the COVID-19 Pandemic," *Air University (AU)- Journal of Indo-Pacific Affairs Article Display*, https://www.airuniversity.af.edu/JIPA/Display/Article/2173156/chinese-communist-party-information-warfare-uschina-competition-during-the-covi/, accessed 16 June 2023.

15 Rory Cormac and Richard J. Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability," *International Affairs*, Vol. 94, no. 3 (May 2018): 477-494.

16 Amsalem and Zoizner, "Real, but Limited."

17 Christian Scheibenzuber et al., "Dialog in the Echo Chamber: Fake News Framing Predicts Emotion, Argumentation and Dialogic Social Knowledge Building in Subsequent Online Discussions," *Computers in Human Behavior*, Vol. 140 (March 1, 2023): 107587.

18 "Countering Russian Disinformation," unpublished Master's Thesis, Naval Postgraduate School, https://nps.primo.exlibrisgroup.com, accessed 15 June 2023.

19 Fletcher Schoen, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, *Strategic Perspectives,* no. 11 (Washington, D.C: National Defense University Press, 2012).

20 "[H.A.S.C. No. 117-8] Disinformation in The Gray Zone: Opportunities, Limitations, And Challenges," legislation, http://www.congress.gov/event/117th-congress/house-event/LC67589/text, accessed 16 June 2023.

21 David Boyns and James David Ballard, "Developing a Sociological Theory for the Empirical Understanding of Terrorism," *American Sociologist*, Vol. 35, no. 2 (Summer 2004): 5-25.

22 "Another Look at Jujitsu Politics | START.Umd.Edu," https://www.start.umd.edu/news/another-look-jujitsu-politics, accessed 16 June 2023.

23 Mette Eilstrup-Sangiovanni and Calvert Jones, "Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Threatening Than Many Think," *International Security*, Vol. 33, no. 2 (October 1, 2008): 7-44.

24 J. Bowyer Bell, "Revolutionary Dynamics: The Inherent Inefficiency of the Underground," *Terrorism and Political Violence*, Vol. 2, no. 2 (1990): 193-211.

25 Sambuddha Ghatak, Aaron Gold and Brandon C. Prins, "Domestic Terrorism in Democratic States: Understanding and Addressing Minority Grievances," https://journals.sagepub.com/doi/full/10.1177/0022002717734285, accessed 16 June 2023.

26 "Challenging the State: Effect of Minority Discrimination, Economic Globalization, and Political Openness on Domestic Terrorism, unpublished Master's Thesis, Naval Postgraduate School, https://nps.primo.exlibrisgroup.com, accessed 16 June 2023.

27 Gordon H. McCormick and Frank Giordano, (2007) "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," *Third World Quarterly*, Vol. 28, no. 2: 295-320.

28 U.S. Africa Command, "What We Do," https://www.africom.mil/what-we-do, accessed 16 June 2023.

29 "A Social Movement Theory Typology of Militant Organisations: Contextualising Terrorism," https://www.tandfonline.com/doi/epdf/10.1080/09546553.2014.954039?needAccess=true&role=button, accessed 16 June 2023.

30 Deniz Aksoy, "Elections and the Timing of Terrorist Attacks," *The Journal of Politics*, Vol. 76, no. 4 (October 2014): 899-913.

31 Ibid.

32 Will Irwin, *Support to Resistance: Strategic Purpose and Effectiveness*, JSOU Report 19 (Tampa: JSOU Press, 2019).

33 Mao Zedong, *On Guerrilla Warfare* (Westport, CT: Praeger, 1961).

34 Erica Chenoweth, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict*, Columbia Studies in Terrorism and Irregular Warfare (New York: Columbia University Press, 2011).

35 Elizabeth Tompkins, "A Quantitative Reevaluation of Radical Flank Effects within Nonviolent Campaigns," in *Research in Social Movements, Conflicts and Change*, Vol. 38 (2015): 103-135.

36 Michael Stohl and George A. Lopez, *The State as Terrorist: The Dynamics of Governmental Violence and Repression*, Contributions in Political Science, no. 103 (Westport, CT: Greenwood Press, 1984).

37 Pearce Edwards and Daniel Arnon, "Violence on Many Sides: Framing Effects on Protest and Support for Repression," *British Journal of Political Science*, Vol. 51, no. 2 (2021): 488-506.

38 Ibid.

39 Michael L. Gross, "Backfire: The Dark Side of Nonviolent Resistance," *Ethics & International Affairs*, Vol. 32, no. 3 (ed 2018): 317-328.

40 Monica Duffy Toft and Yuri M. Zhukov, "Denial and Punishment in the North Caucasus: Evaluating the Effectiveness of Coercive Counter-Insurgency," *Journal of Peace Research*, Vol. 49, no. 6 (2012): 785-800.

41 Erica Chenoweth, *Civil Resistance: What Everyone Needs to Know* (Oxford: Oxford University Press, 2021).

42 Maria J. Stephan and Erica Chenoweth, "Mobilization and Resistance: A Framework for Analysis," in *Rethinking Violence* (Cambridge, MA: MIT Press, 2010).

43 *Lukashenko Calls Himself a "dictator" in Annual Address*, 2022, https://www.youtube.com/watch?v=nmuG0kSghIQ.

44 "Belarus' Parliamentary Elections Fail to Meet OSCE Democratic Election Commitments," CSCE, February 12, 2016, https://www.csce.gov/international-impact/belarus-parliamentary-elections-fail-meet-osce-democratic-election-commitments; Deutsche Welle (www.dw.com), "EU Rejects Belarus Presidential Election Result | DW | 19.08.2020," DW.COM, https://www.dw.com/en/eu-rejects-belarus-presidential-election-result/a-54622050, accessed 5 September 2022; Franak Viačorka [@franakviacorka], "According to Various Estimates, from 80 to 250 Thousands Joined the Rally Today. Many Rallies Are Taking Part in Other Cities Today as Well. According to Organizers, More than 0.5 Million Are Protesting Today across the Country, https://T.Co/BVz5AGXFZA," Tweet, *Twitter*, August 23, 2020, https://twitter.com/franakviacorka/status/1297528231168483328.

45 Dave DeCamp, "US Looking to Give More Technology Support to Belarus' Opposition," *News From Antiwar.Com* (blog), May 2, 2022, https://news.antiwar.com/2022/05/02/us-looking-to-give-more-technology-support-to-belarus-opposition/.

46 "Хвалі Аптытанняў," https://belaruspolls.org/volny-oprosov, accessed 5 September 2022.

47 David Vine, "No Bases? Assessing the Impact of Social Movements Challenging US Foreign Military Bases," *Current Anthropology*, Vol. 60, no. S19 (February 2, 2019): S158-S172.

48 Amy Austin Holmes, *Social Unrest and American Military Bases in Turkey and Germany* (Cambridge University Press, 2014).

49 Ryhor Astapenia, "Lukashenko Is Dragging Belarus Closer to a War That Most of Its Citizens Don't Want," *The Guardian*, March 21, 2022, sec. Opinion, https://www.theguardian.com/commentisfree/2022/mar/21/lukashenko-belarus-war-citizens-dont-want-putin-sanctions.

50 "Anti-War Movement Manifest / Official Web-Site of Sviatlana Tsikhanouskaya," https://tsikhanouskaya.org/en/events/news/b66f8091f11bb20.html, accessed 5 September 2022.

51 "Хвалі Аптытанняў."

52 Xander Landen, "Russia Arrests over 4,000 for Anti-War Protest, Most since Ukraine War Began," *Newsweek*, March 6, 2022, https://www.newsweek.com/russia-arrests-over-4000-anti-war-protest-most-since-ukraine-war-began-1685300.

53 "Rosgvardiya: Hurtling Towards Confrontation?" https://www.csis.org/blogs/post-soviet-post/rosgvardiya-hurtling-towards-confrontation, accessed 5 September 2022.

54 "Russia Loses More than 900 Elite Military Personnel in Ukraine – BBC," *Ukrainska Pravda,* https://www.pravda.com.ua/eng/news/2022/09/1/7365645/, accessed 5 September 2022.

55 "Putin May Declare War against 'World's Nazis' on "Victory" Day:' UK Official," *Newsweek*, April 29, 2022, https://www.newsweek.com/putin-may-declare-war-against-worlds-nazis-victory-day-1702276.

56 Michal Smetana and Michal Onderco, "From Moscow With a Mushroom Cloud? Russian Public Attitudes to the Use of Nuclear Weapons in a Conflict With NATO," *Journal of Conflict Resolution*, August 10, 2022.

CHAPTER 13

1 U.S. Department of the Navy, *2021 Unmanned Campaign Framework*, 15 March 2021, https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf?ver=LtCZ-BPlWki6vCBTdgtDMA%3D%3D.

2 John J. Chin, Kiron Skinner and Clay Yoo, "Understanding the National Security Strategy Through Time." *Texas National Security Review,* Vol. 6, no. 4 (Fall 2023), https://tnsr.org/2023/09/understanding-national-security-strategies-through-time/.

3 *U.S. National Security Strategy*, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

4 Ibid.

5 *2022 U.S. National Defense Strategy*, 27 October 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

6 Ibid.

7 Leo Blanken, Philip Swintek, and Justin Davis, "Special Operations as an Innovation Laboratory," *War on the Rocks,* 25 February 2020, https://warontherocks.com/2020/02/special-operations-as-an-innovation-laboratory/.

8 U.S. Department of the Navy, *2021 Unmanned Campaign Framework*.

9 Eliot Cohen, Commandos and Politicians: Elite Units in Modern Democracies (Cambridge, MA: Harvard University Press of America, 1978).

10 U.S. Department of the Navy, *2021 Unmanned Campaign Framework*.

11 "2023 National Defense Science and Technology Strategy." U.S. Department of Defense. Published 09 May 2023, https://media.defense.gov/2023/May/09/2003218877/-1/-1/0/NDSTS-FINAL-WEB-VERSION.PDF.

12 Ibid.

13 Ibid.

14 SOFWERX, "SBIR Statistics Through SOFWERX," https://www.sofwerx.org/impact/2023.

15 Government Accountability Office, GAO Report GAO-10-1036R: "Hybrid Warfare," 10 September 2010, https://www.gao.gov/assets/a97054.html.

16 Kevin D. Stringer, "Jomini and Naval Special Operations Forces—An Applied-Competition Approach to Russia," *Naval War College Review,* Vol. 74, no. 4 (2021): Article 7, https://digital-commons.usnwc.edu/nwc-review/vol74/iss4/7.

17 Admiral (retired) James Stavridis, "Maritime Hybrid Warfare is Coming." *Proceedings,* Vol. 142/12/1, (December 2016): 366.

18 Ibid.

19 Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: The Potomac Institute for Policy Studies, 2007), https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

20 Jim Garamone. "Military Must Be Ready To Confront Hybrid Threats," U.S. Department of Defense, 4 September 2019, https://www.defense.gov/News/News-Stories/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intel-official-says/.

21 John Harper. "Pentagon Gets Around $7.5 Billion for Unmanned Systems," *National Defense Magazine,* 27 May 2021, https://www.nationaldefensemagazine.org/articles/2021/5/27/pentagon-gets-$7-5-billion-for-unmanned-systems.

22 Ibid.

23 "2021 Defense Budget for Unmanned Systems and Robotics," *Association for Unmanned Vehicle Systems International (AUVSI),* 2021, https://www.auvsi.org/dod-unmanned-systems-budget-report#:~:text=The%20United%20States%20Department%20of,billion%20budget%20for%20FY%202021.

24 Christian Trotti, "What does the future of autonomous warfare look like? Four critical questions, answered," *Forward Defense, Atlantic Council,* 13 May 2022, https://www.atlanticcouncil.org/content-series/automating-the-fight/what-does-the-future-of-autonomous-warfare-look-like-four-critical-questions-answered/.

25 Patrick Tucker, "'Collaborative, Portable Autonomy' Is the Future of AI for Special Operations," *Defense One: Science and Technology,* 25 May 2022, https://www.defenseone.com/technology/2022/05/collaborative-portable-autonomy-future-ai-special-operations/367408/.

26 Leo Blanken, Jason Lepore and Cecilia Panella, "From The Lighthouse To The Christmas Tree: Enabling Distributed Innovation In The US Military," *Modern War Institute,* 27 July 2022, https://mwi.westpoint.edu/from-the-lighthouse-to-the-christmas-tree-enabling-distributed-innovation-in-the-us-military/.

27 Mark Pomerleau, "Special ops will look to invest in new technologies to compete with advanced nation-state actors," *Defense Scoop,* 10 March 2023, https://defensescoop.com/2023/03/10/special-ops-will-look-to-invest-in-new-technologies-to-compete-with-advanced-nation-state-actors/.

28 Greg Myre, "How Ukraine created an 'Army of Drones' to take on Russia," *National Public Radio (NPR),* 20 June 2023, https://www.npr.org/2023/06/20/1183050117/how-ukraine-created-an-army-of-drones-to-take-on-russia.

29 Philip E. Ross, "Budget Drones in Ukraine Are Redefining Warfare," *Institute for Electrical and Electronics Engineers* (*IEEE Spectrum),* 17 May 2023, https://spectrum.ieee.org/drone-warfare-ukraine.

30 H.I. Sutton, "World's First Specialized Explosive Naval Drone Unit Formed In Ukraine," *Naval News,* 31 August 2023, https://www.navalnews.com/naval-news/2023/08/worlds-first-specialized-explosive-naval-drone-unit-formed-in-ukraine/.

31 Tim Lister, Victoria Butenko and Olga Voitovych, "Russian warship seen listing in Black Sea after Ukrainian sea drone attack on major base," *CNN,* 5 August 2023, https://www.cnn.com/2023/08/04/europe/ukraine-sea-drone-russian-warship-black-sea-intl/index.html.

32 Sutton, "World's First Specialized…"

33 Scott Savitz, Irv Blickstein, Peter Buryk, Robert W. Button, Paul DeLuca, James Dryden, Jason Mastbaum, Jan Osburg, Phillip Padilla, Amy Potter, Carter C. Price, Lloyd Thrall, Susan K. Woodward, Roland J. Yardley, and John M. Yurchak, "U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs)," *RAND Corporation,* 2013, https://www.rand.org/pubs/research_reports/RR384.html.

34 Ibid.

35 Program Executive Office Littoral and Mine Warfare (Peo-Lmw), *Navy Unmanned Surface Vehicle Master Plan* (Washington D.C.: Defense Technical Information Center, 23 July 2007), https://apps.dtic.mil/sti/citations/ADA504867.

36 Sam LaGrone, "Navy Rethinking Medium Unmanned Surface Vehicle After Middle East Tests, Says CNO Gilday," *USNI News,* 28 April 2022, https://news.usni.org/2022/04/28/navy-rethinking-medium-unmanned-surface-vehicle-after-middle-east-tests-says-cno-gilday.

37 Ibid.

38 Megan Eckstein, "US Navy more certain of role for medium surface drones following tests," *Defense News,* 12 January 2023, https://www.defensenews.com/naval/2023/01/12/us-navy-more-certain-of-role-for-medium-surface-drones-following-tests/.

39 Mallory Shelbourne, "Unmanned Surface Vehicle Mariner Next Ghost Fleet Vessel to Join the Navy," *USNI News,* 23 August 2022, https://news.usni.org/2022/08/23/unmanned-surface-vehicle-mariner-next-ghost-fleet-vessel-to-join-the-navy.

40 Ibid.

41 H.I. Sutton, "Ukraine's New Weapon To Strike Russian Navy In Sevastopol," *Naval News,* 21 September 2022, https://www.navalnews.com/naval-news/2022/09/ukraines-new-weapon-to-strike-russian-navy-in-sevastopol/.

42 Ibid.

43 H.I. Sutton, "Suspected Ukrainian Explosive Sea Drone Made From Recreational Watercraft Parts," *USNI News,* 11 October 2022, https://news.usni.org/2022/10/11/suspected-ukrainian-explosive-sea-drone-made-from-jet-ski-parts.

44 Ibid.

45 "Ukrainian ingenuity is ushering in a new form of warfare at sea," *The Economist,* 7 December 2022, https://www.economist.com/science-and-technology/2022/12/07/ukrainian-ingenuity-is-ushering-in-a-new-form-of-warfare-at-sea.

46 Paul Maso, "Never has this been more true than in today's military: innovate or die," *The New European,* 9 November 2022, https://www.theneweuropean.co.uk/never-has-this-been-more-true-than-in-todays-military-innovate-or-die/.

47 Scott Savitz, "The Age of Uncrewed Surface Vessels," *The RAND Blog,* 15 November 2022, https://www.rand.org/blog/2022/11/the-age-of-uncrewed-surface-vessels.html.

48 "Ukrainian Navy creates a brigade of naval drones," *Miltarnyi,* 26 August 2023, https://mil.in.ua/en/news/ukrainian-navy-creates-a-brigade-of-naval-drones/.

49 Peter Ong and Scott Savitz, "RAND Corporation Offers Insights On Kamikaze USVs," *Naval News,* 4 September 2023, https://www.navalnews.com/naval-news/2023/09/rand-corporation-offers-insights-on-kamikaze-usvs/.

50 Kyle Mizokami, "The Surprising History of Unmanned Navy Systems," *USNI Proceedings,* Vol. 146/6/1,2020, 408, https://www.usni.org/magazines/proceedings/2020/june/surprising-history-unmanned-navy-systems#:~:text=The%201930s%20saw%20another%20attempt,and%20controlled%20by%20radio%20signals.

51 Jeremy Hsu, "When US Navy Suicide Drones Went to War," *Discover Magazine,* 18 February 2017, https://www.discovermagazine.com/technology/when-us-navy-suicide-drones-went-to-war.

52 Kenneth P. Werrell, "The Evolution of the Cruise Missile," *Air University Press,* September 1985, https://media.defense.gov/2017/apr/07/2001728474/-1/-1/0/b_0006_werrell_evolution_cruise_missile.pdf.

53 Grace V. Jean, "Drones Becoming Special Operations Forces' Indispensible Tools of War," *National Defense*, Vol. 95, no. 690 (2011): 28-34, http://www.jstor.org/stable/45369996.

54 Megan Eckstein, "US Navy injects first-of-kind unmanned experiments into multinational exercise," *Defense News,* 8 August 2022, https://www.defensenews.com/naval/2022/08/08/us-navy-injects-first-of-kind-unmanned-experiments-into-multinational-exercise/.

55 Ibid.

56 Ibid.

57 Amanda Miller, "US Includes ScanEagle ISR Drones in Ukraine's Latest Aid Package," *Air and Space Forces Magazine,* 22 August 2022, https://www.airandspaceforces.com/us-includes-scaneagle-isr-drones-in-ukraines-latest-aid-package/.

58 Sebastien Roblin, "Drone Warfare Accelerates Over Ukraine," *Inside Unmanned Systems,* 14 November 2022, https://insideunmannedsystems.com/drone-war-accelerates-over-ukraine/.

59 Ibid.

60 Scott Simon, "How the use of drones in Ukraine has changed war as we know it," *National Public Radio,* 5 August 2023, https://www.npr.org/2023/08/05/1192343968/how-the-use-of-drones-in-ukraine-has-changed-war-as-we-know-it.

61 J. Craiger and D.M. Zorri, "Current Trends in Small Unmanned Aircraft Systems: Implications for U.S. Special Operations Forces," JSOU Press Occasional Paper, 2019, https://commons.erau.edu/publication/1472.

62 William S. Angerman, "Coming Full Circle with Boyd's OODA Loop Ideas: An Analysis of Innovation Diffusion and Evolution," 2004, https://scholar.afit.edu/etd/4085.

63 Adam Lowther and Mahbube Siddiki, "Combat Drones in Ukraine," *Air and Space Operations Review,* Vol. 1, no. 4 (Winter 2022), https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf.

64 Major Douglas W. Jaquish, "Uninhabited Air Vehicles for Psychological Operations—Leveraging Technology for PSYOP Beyond 2010," Air University, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/jaquish.pdf.

65 J. Watling and N. Reynolds, "Ukraine at War Paving the Road from Survival to Victory," Royal United Services Institute, Special Report, 4 July 2020, https://static.rusi.org/special-report-202207-ukraine-final-web_0.pdf; and Dominika Kunertova, "The war in Ukraine shows the game-changing effect of drones depends on the game," *Bulletin of the Atomic Scientists*, Vol. 79, no. 2 (2023): 95-102.

66 Greg Myre, "A Chinese drone for hobbyists plays a crucial role in the Russia-Ukraine war," *National Public Radio: All Things Considered,* 28 March 2023, https://www.npr.org/2023/03/21/1164977056/a-chinese-drone-for-hobbyists-plays-a-crucial-role-in-the-russia-ukraine-war.

67 Kristina Marintseva, Gennadiy Yun, and Igor Vasilenko, "Delivery of Special Cargoes Using the Unmanned Aerial Vehicles," Chapter 2 in *Unmanned Aerial Vehicles in Civilian Logistics and Supply Chain Management. Advances in Logistics, Operations, and Management Science (ALOMS) Book Series,* 2019, https://scholar.google.com/scholar_url?url=https://www.researchgate.net/profile/Kristina-Marintseva/publication/332815274_Delivery_of_Special_Cargoes_Using_the_Unmanned_Aerial_Vehicles/links/5d063f1e92851c90043fad13/Delivery-of-Special-Cargoes-Using-the-Unmanned-Aerial-Vehicles.pdf&hl=en&sa=X&ei=fKURZYC3H6G_y9YP4-Se0AM&scisig=AFWwaeasEvWXn5T_xf_Up05V-NIA&oi=scholarr.

68 Mark Jacobsen, "The Dubious Prospects For Cargo-Delivery Drones In Ukraine," *War on the Rocks,* 25 May 2022, https://warontherocks.com/2022/05/the-dubious-prospects-for-cargo-delivery-drones-in-ukraine/.

69 Marcin Frąckiewicz, "The Pioneering Role of Drones in Ukraine's Military Logistics," *TS2 SPACE,* 20 June 2023, https://ts2.space/en/the-pioneering-role-of-drones-in-ukraines-military-logistics/.

70 Heiko Borchert, "Why Unmanned Systems are Ideal for 'Gray Zone' Ops in the Gulf," *The Maritime Executive,* 12 August 2019, https://maritime-executive.com/editorials/why-unmanned-systems-are-ideal-for-gray-zone-ops-in-the-gulf.

71 Paul Mozur and Valerie Hopkins, "Ukraine's War of Drones Runs Into an Obstacle: China," *The New York Times,* 30 September 2023, https://www.nytimes.com/2023/09/30/technology/ukraine-russia-war-drones-china.html.

72 Ibid.

73 Paul Mozur, Aaron Krolik and Keith Bradsher, "As War in Ukraine Grinds On, China Helps Refill Russian Drone Supplies," *The New York Times,* 21 March 2023, https://www.nytimes.com/2023/03/21/business/russia-china-drones-ukraine-war.html.

74 "See the ultralight cardboard drone donated to Ukraine," *C4ISRNet,* 13 September 2023, https://www.c4isrnet.com/unmanned/2023/09/13/see-the-ultralight-cardboard-drone-donated-to-ukraine/.

75 "CORVO Next Generation Autonomous Delivery System," https://corvouas.com.au/wp-content/uploads/CORVO-PPDS-web-version-23082023-compressed.pdf.

76 Mia Jankowicz, "Ukraine is fielding new $3,500 'cardboard' drones against Russia — they're flat-packed and could prove deadly," *Insider Magazine,* 30 August 2023, https://www.businessinsider.com/ukraine-is-using-a-cheap-flat-pack-cardboard-drone-australia-2023-8.

77 Samya Kullab, "Ukraine Is Building an Advanced Army of Drones. For Now, Pilots Improvise with Duct Tape and Bombs," *Military Times,* 25 September 2023, https://www.military.com/daily-news/2023/09/25/ukraine-building-dadvanced-army-of-drones-now-pilots-improvise-dcut-tape-and-bombs.htnl?utm_source=Twitter#Ecgibix=1695639055-1.

78 Megan Eckstein, "Cardboard drone vendor retools software based on Ukraine war hacks," *Defense News,* 13 September 2023, https://www.defensenews.com/air/2023/09/13/cardboard-drone-vendor-retools-software-based-on-ukraine-war-hacks/.

79 Director of National Intelligence, "The Future of the Battlefield," NIC-2021-02493, April 2021, https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02493--Future-of-the-Battlefield--Unsourced--14May21.pdf.

CHAPTER 14

1 The author wishes to thank Dr. John Arquilla, Colonel (retired) Brian Greenshields, Lieutenant-Colonel David Johnston, Lieutenant-Colonel Gary Wolfman, Lieutenant-Colonel P. Travis Jardine, and Major David Dunsiger for their contributions to this work.

2 John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy*, Vol. 12, no. 2 (1993):141-165.

3 David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, 6 January 2011, 10.

4 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, no. 2 (October 2013): 41-73.

5 Lennart Maschmeyer and Nadiya Kostyuk, "There Is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict," *War on the Rocks*, 8 February 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

6 Mark Pomerleau, "US Cyber Command Releases First Full Budget," *DefenseScoop* (blog), 13 March 2023, https://defensescoop.com/2023/03/13/us-cyber-command-releases-first-full-budget/.

7 "SOF Week 2023: USSOCOM Plans to Boost Investment in Cyber and Space Capabilities | Shephard," https://www.shephardmedia.com/news/special-operations/sof-week-2023-ussocom-plans-to-boost-investment-in-cyber-and-space-capabilities/, accessed 28 June 2023.

8 "New 'Influence Triad' Will Fuse SOF, Cyber, and Space Command Satellite Intelligence," *Defense One*, 9 August 2022, https://www.defenseone.com/threats/2022/08/new-influence-triad-will-fuse-sof-cyber-and-space-command-satellite-intelligence/375600/.

9 "Hearing to Receive Testimony on the Posture of United States Special Operations Command and United States Cyber Command" (Washington, D.C.), 90, https://www.armed-services.senate.gov/imo/media/doc/23-05_03-07-2023.pdf, accessed 28 June 2023.

10 Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?," *Joint Forces Quarterly*, no. 63 (2011): 64-69.

11 "U.S. Cyber Command - Components," https://www.cybercom.mil/Components.aspx, accessed 28 June 2023.

12 William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice*, 6th Edition (Novato: Presidio Press, 1996).

13 Ibid., 11.

14 Colin S. Gray, "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?," *The US Army War College Quarterly: Parameters*, Vol. 29, no. 1 (10 March 1999).

15 "Jimmy Carter and the Iranian Hostage Crisis," *White House History Association*, 1, https://www.whitehousehistory.org/teacher-resources/jimmy-carter-and-the-iranian-hostage-crisis?, accessed 10 August 2023.

16 Beckwith narrates this experience in the opening pages of his memoirs and relates his efforts to create Delta throughout. See Charlie A. Beckwith and Donald Knox, *Delta Force* (New York: Harper Collins, 2000).

17 Eric Haney, *Inside Delta Force: The Story of America's Elite Counterterrorist Unit* (New York: Random House, 2003), 1-3.

18 Beckwith and Knox, *Delta Force*, 211.

19 Justin Williamson, *Operation Eagle Claw 1980: The Disastrous Bid to End the Iran Hostage Crisis* (Oxford: Osprey Publishing, 2020), 14.

20 Edward T. Russell, "Crisis in Iran: Operation Eagle Claw," in *Short of War: Major USAF Contingency Operations*, 1997, 128-131, https:// media.defense.gov/2012/Aug/23/2001330106/-1/-1/0/Eagleclaw.pdf, accessed 7 September 2023.

21 Beckwith and Knox, *Delta Force*, 244.

22 RH-53Ds would have insufficient fuel to carry the hostages and Delta operators back to Desert One, so a new airfield was required. Further, C-130s had insufficient lift to transport all personnel and equipment, so they were substituted for the C-141s. See Beckwith and Knox, 263.

23 Williamson, *Operation Eagle Claw 1980*, 22.

24 Beckwith and Knox, *Delta Force*, 163.

25 Colonel James H. Kyle and John Robert Eidson, *The Guts to Try: The Untiold Story of the Iran Hostage Rescue Mission by the On-Scene Desert Commander* (New York: Ballantine Books, 2002), 120-122.

26 Rod Lenahan, *Crippled Eagle: A Historical Perspective* (Magnolia, TX: Narwhal Press, 1998), 105.

27 Beckwith and Knox, *Delta Force*, 10.

28 Ibid., 301-316.

29 The Holloway Commission mandated a restructuring of SOF, including SOF aviation. See Williamson, *Operation Eagle Claw 1980*, 72.

30 160th SOAR was originally created as TF 160. See "160th SOAR (A)," https://www.soc.mil/USASOAC/160th.html, accessed 14 August 2023.

31 "427 Special Operations Aviation Squadron," https://www.canada.ca/en/special-operations-forces-command/corporate/organizational-structure/427-so-aviation-squadron.html, accessed 15 August 2023.

32 Beckwith and Knox, *Delta Force*, 332.

33 Ibid., 332.

CHAPTER 15

1 "To Receive Testimony on United States Special Operations Command's Efforts to Sustain the Readiness of Special Operations Forces and Transform the Force for Future Security Challenges." *Senate Armed Services Committee,* 27 April 2022, https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-united-states-special-operations-commands-efforts-to-sustain-the-readiness-of-special-operations-forces-and-transform-the-force-for-future-security-challenges, accessed 30 August 2023.

2 Statement of Lieutenant General Jonathan Braga Commanding General United States Army Special Operations Command (USASOC) Before the Senate Armed Services Committee Emerging Threats and Capabilities," *Senate Armed Services Committee,* 27 April 2022. https://www.armed-services.senate.gov/imo/media/doc/2022%20USASOC%20Posture%20-%20LTG%20Braga%20-%20SASC-ETC%20(27%20April)%20(Final).pdf, accessed 30 August 2023.

3 Posture Statement of Rear Admiral H. W. Howard III, USN Commander, Naval Special Warfare Command Before The 117th Congress Senate Armed Service Committee," *Senate Armed Services Committee,* 27 April 2023, "https://www.armed-services.senate.gov/imo/media/doc/2022%20NSWC%20POSTURE%20-%20RADM%20Howard%20-%20SASC-ETC%20(27%20April)%20(Final).pdf, accessed 30 August 2023.

4 Will Beaurpere and Ned Marsh. "Space, Cyber, And Special Operations: An Influence Triad for Global Campaigning," *Modern Warfare Institute.* 6 September 2022, https://mwi.

usma.edu/space-cyber-and-special-operations-an-influence-triad-for-global-campaigning/, accessed 30 August 2023.

5 Ibid.

6 Max Polyakov, "A Brief History of Satellites in Military Conflicts (Part 1)," 3 November 2022, https://maxpolyakov.com/brief-history-of-satellites-in-military-conflicts/.

7 Sylvia Katherine Kraemer, "NASA, Monopolies, and the Cold War: The Origins and Consequences of NASA Patent Policy, 1958-1996," October 1999, https://www.hq.nasa.gov/office/codez/plans/R&D/SHOTOCT99.html, accessed 30 August 2023.

8 Andrew Chatzky, Anshu Siripurapu and Steven J. Markovich, "Space Exploration and U.S. Competitiveness," *Council on Foreign Relations,* updated 23 September 2021, https://www.cfr.org/backgrounder/space-exploration-and-us-competitiveness, accessed 30 August 2023.

9 Trevor Brown, "The American and Soviet Cold War Space Programs," *Comparative Strategy*, Vol. 30, no. 2: 177-185.

10 Ibid.

11 William Schauer, *The Politics of Space: A Comparison of the Soviet and American Space Programs* (New York: Holmes & Meier Publishers, 1976).

12 "CORONA: America's First Imaging Satellite Program - CIA," n.d., https://www.cia.gov/legacy/museum/exhibit/corona-americas-first-imaging-satellite-program/, accessed 30 August 2023.

13 David Nye, "This Air Force Unit Caught Spy Satellite Photos as They Fell from Space," *Business Insider*, n.d., https://www.businessinsider.com/this-air-force-unit-caught-spy-satellite-photos-as-they-fell-from-space-2015-9, accessed 30 August 2023.

14 "CORONA: America's First…"

15 Dwayne A. Day, John M. Logsdon and Brian Latell, *Eye in the Sky: The Story of the Corona Spy Satellites* (Washington D.C.: Smithsonian Institution Press, 1998).

16 Mark Amidon, "Groupthink, Politics, and the Decision to Attempt the Son Tay Rescue," *Parameters*, Vol. 35, no. 3 (Autumn 2005), https://apps.dtic.mil/sti/pdfs/ADA485587.pdf.

17 Stavros Atlamazoglou, "Son Tay Raid: One of the Most Daring Special Operations in U.S. History - Sandboxx," 25 April 2023, https://www.sandboxx.us/blog/son-tay-raid-the-massive-secret-mission-to-rescue-american-pows-that-failed/, https://www.sandboxx.us/blog/son-tay-raid-the-massive-secret-mission-to-rescue-american-pows-that-failed/, accessed 30 August 2023.

18 Benjamin F. Schemmer, *The Raid: The Son Tay Prison Rescue Mission* (New York: Ballantine Books, 2002), 77; and Amidon, "Groupthink, Politics," 119.

19 "How Satellite Military Communications Support Special Operations Forces – TS2 SPACE," n.d., https://ts2.space/en/how-satellite-military-communications-support-special-operations-forces/, accessed 30 August 2023.

20 U.S. Army Satellite Communications Agency, "History of Satellite Communications," 1992, U.S. Army Communications-Electronics Command, https://cecom.army.mil/PDF/Historian/Feature%203/Satellites/History_of_SATCOM_brief.pdf, accessed 30 August 2023.

21 Polyakov, "A Brief History."

22 "Address to Joint Session of Congress May 25, 1961," *Historic Speeches*, https://www.jfklibrary.org/learn/about-jfk/historic-speeches/address-to-joint-session-of-congress-may-25-1961#:~:text=While%20listing%20national%20goals%2C%20the,.%22%20This%20excerpt%20ends%20abruptly, accessed 30 August 2023.

23 "Intelligence Memorandum: US and Soviet Space Programs Comparative Size," *Central Intelligence Agency,* March 1966, https://irp.fas.org/cia/product/sovmim66.pdf, accessed 30 August 2023.

24 Ibid.

25 David Halberstam, *The Fifties* (New York: Villard Books, 1993).

26 "Memorandum of Conference with The President," 8 October 1957, National Security Archives, https://www.archives.gov/files/education/lessons/sputnik-memo/images/memo-page-1-l.gif, accessed 30 August 2023.

27 Director of Central Intelligence, "National Intelligence Estimate, The Soviet Space Program," 5 December 1962, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB501/docs/EBB-05.pdf, accessed 30 August 2023.

28 Slava Gerovitch, "Computing in the Soviet Space Program: An Introduction," Massachusetts Institute of Technology, April 2003, https://web.mit.edu/slava/space/introduction.htm, accessed 30 August 2023.

29 Document 18: Director of Central Intelligence National Intelligence Estimate 11-1-71, "The Soviet Space Program, July 1, 1971. Top Secret." Record Group 263, National Archives and Records Administration, College Park, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB501/docs/EBB-18.pdf, accessed 30 August 2023.

30 "50 Years Ago: Launch of Salyut, the World's First Space Station," *NASA History,* 19 April 2021. https://www.nasa.gov/feature/50-years-ago-launch-of-salyut-the-world-s-first-space-station, accessed 30 August 2023.

31 Document 22: Director of Central Intelligence, Interagency Intelligence Memorandum, "Soviet Dependence on Space Systems," November 1975. Top Secret Codeword. CIA Freedom of Information Act Release, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB501/docs/EBB-22.pdf, accessed 30 August 2023.

32 "Revelations from the Russian Archives: The Soviet Union and the United States," Exhibition at the Library of Congress, June 15–July 16, 1992. Published online in April 1996. https://www.loc.gov/exhibits/archives/index.html, accessed 29 June 2023.

33 Rafael Reuveny and Aseem Prakash, "The Afghanistan War and the Breakdown of the Soviet Union." *Review of International Studies*, Vol. 25, no. 4 (1999): 693-708.

34 Document 38b: Director of Central Intelligence, National Intelligence Estimate 11-1-83, "The Soviet Space Program," 19 July 1983. Top Secret. Record Group 263, National Archives and Records Administration, College Park, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB501/docs/EBB-38b.pdf, accessed 30 August 2023.

35 Lester W. Grau, "The Soviet-Afghan War: A Superpower Mired in the Mountains," *The Journal of Slavic Military Studies*, Vol. 17, no 1 (March 2004).

36 Ibid.

37 "NATO's approach to space." *North Atlantic Treaty Organization,* 23 May 2023, https://www.nato.int/cps/en/natohq/topics_175419.htm, accessed 30 August 2023.

38 "2022 NATO Strategic Concept." *North Atlantic Treaty Organization,* 29 June 2022, https://www.nato.int/strategic-concept/, accessed 30 August 2023.

39 Ibid.

40 Stephen McCall, "Space as a Warfighting Domain: Issues for Congress," *Congressional Research Service*, 10 August 2021, https://sgp.fas.org/crs/natsec/IF11895.pdf, accessed 30 August 2023.

41 Ibid.

42 "PAROS Treaty: Proposed Prevention of an Arms Race in Space (PAROS) Treaty," *Nuclear Threat Initiative,* https://www.nti.org/education-center/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty, accessed 30 August 2023.

43 "Sending 14 Drafts to General Assembly, First Committee Defeats Motion Questioning Its Competence to Approve One Aimed at Tackling Outer Space Threats," 6 November 2020, https://press.un.org/en/2020/gadis3658.doc.htm, accessed 30 August 2023.

44 "PAROS Treaty."

45 Ricky Lee and Sarah Steele, "Military Use of Satellite Communications, Remote Sensing, and Global Positioning Systems in the War on Terror," *Journal of Air Law and Commerce* 79, no. 1 (January 1, 2014): 69.

46 R.D. Hooker, "America's Special Operations Problem," *Joint Forces Quarterly*, Vol. 108, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-108/Article/Article/3264605/americas-special-operations-problem/, accessed 30 August 2023.

47 Walter Haynes, "The Hidden Costs of Strategy by Special Operations," *War on the Rocks*, https://warontherocks.com/2019/04/the-hidden-costs-of-strategy-by-special-operations/, accessed 1 May 2023; and "U.S. Special Operations Forces (SOF): Background and Issues for Congress" (Washington D.C.: Congressional Research Service, 11 May 2022).

48 Tina Highfill and Chris Surfield. "New and Revised Statistics for the U.S. Space Economy, 2012–2021," *The Journal of the U.S. Bureau for Economic Analysis*, 27 June 2023, https://apps.bea.gov/scb/issues/2023/06-june/0623-space-economy.htm#:~:text=The%20

updated%20and%20revised%20statistics,and%20360%2C000%20private%20industry%20jobs, accessed 29 August 2023.

49 David Vergun, "Official Details Space-Based Threats and U.S. Countermeasures," *DoD News*, 26 April 2023, https://www.defense.gov/News/News-Stories/Article/Article/3375577/official-details-space-based-threats-and-us-countermeasures/, accessed 29 August 2023.

50 Kari A. Bingen, Kaitlyn Johnson, and Zhanna Malekos Smith, "Russia Threatens to Target Commercial Satellites," 10 November 2022, https://www.csis.org/analysis/russia-threatens-target-commercial-satellites.

51 Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare 2020* (New York: Hachette Books, 2020), xxviii.

52 John K. Culver and Sarah Kirchberger, *US-China lessons from Ukraine: Fueling more dangerous Taiwan tensions* (Toronto: Atlantic Council Report, 15 June 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/us-china-lessons-from-ukraine/, accessed 1 August 2023.

53 Ahmad Khan & Zulfqar Khan "Regionalism and Space Activities: China-Pakistan Economic Corridor and Space Power in South Asia" *Astropolitics*, Vol. 19, no. 1-2 (November 2021).

54 Thuy Mai, "Global Positioning System History," NASA History, updated 7 August 2017, http://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html, accessed 29 July 2023.

55 *Conduct of the Persian Gulf War*, Final Report to U.S. Congress, Pursuant to Title V of the Persian Gulf Conflict Supplemental Authorization and Personnel Benefits Act of 1991 (Public Law 102-25), April 1992, https://www.globalsecurity.org/military/library/report/1992/cpgw.pdf, accessed 30 August 2023.

56 "Other Global Navigation Satellite Systems (GNSS)," *GPS.GOV*, n.d., https://www.gps.gov/systems/gnss/#:~:text=Global%20navigation%20satellite%20system%20(GNSS,a%20global%20or%20regional%20basis.

57 "Do Winter Weather Conditions Have an Effect on the Accuracy of GNSS Devices?" *Galileo GNSS*, 11 February 2017, https://galileognss.eu/do-winter-weather-conditions-have-an-effect-on-the-accuracy-of-gnss-devices/.

58 DoD, "Space Domain Critical to Combat Operations Since Desert Storm," https://www.defense.gov/News/News-Stories/Article/Article/2543941/space-domain-critical-to-combat-operations-since-desert-storm/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F2543941%2Fspace-domain-critical-to-combat-operations-since-desert-storm%2F.

59 Stavros Atlamazoglou, "Inside the Covert Mission That Sent Delta Force and British SAS Deep behind Iraqi Lines in Search of Saddam's Missiles," *Business Insider*, n.d., https://www.businessinsider.com/delta-force-sas-hunted-iraqi-scud-missiles-during-gulf-war-2021-2.

60 "Conduct of the Persian Gulf War."

61 Ibid.

62 "Space Segment," GPS.Gov, n.d., https://www.gps.gov/systems/gps/space/, accessed 4 February 2023.

63 Alan C. O'Connor, M.P. Gallaher, K.B. Clark-Sutton, D. Lapidus, Z. Oliver, T.J. Scott, D. W. Wood and E.G. Brown, "*Economic benefits of the Global Positioning System (GPS),*" *RTI International*, 2019.

64 Phillip C. Saunders and Charles D. Lutes, "China's ASAT Test: Motivations and Implications," *Joint Force Quarterly* (2007), https://apps.dtic.mil/sti/citations/ADA517485, accessed 5 August 2023.

65 Report to the Committee on Armed Services, U.S. Senate, *GPS Alternatives - DoD Is Developing Navigation Systems but is Not Measuring Overall Progress* (Washington, D.C.: United States Government Accountability Office, August 2022), https://www.gao.gov/assets/gao-22-106010.pdf, accessed 5 August 2023.

66 F. S. Prol et al., "Position, Navigation, and Timing (PNT) Through Low Earth Orbit (LEO) Satellites: A Survey on Current Status, Challenges, and Opportunities," *IEEE Access* 10 (2022): 83971-83972, https://doi.org/10.1109/ACCESS.2022.3194050, accessed 5 August 2023; and Report to the Committee on Armed Services, U.S. Senate, *GPS Alternatives.*

67 Report to the Committee on Armed Services, U.S. Senate, *GPS Alternatives.*

68 Matt Burgess, "GPS Signals Are Being Disrupted in Russian Cities," *Wired*, https://www.wired.com/story/gps-jamming-interference-russia-ukraine/, accessed 1 May 2023.

69 David Hambling, "Ukraine Is Spoofing Russian Drones Out of The Sky," *Forbes*, https://www.forbes.com/sites/davidhambling/2023/04/21/ukraine-is-spoofing-russian-drones-out-of-the-sky/, accessed 1 May 2023.

70 Elizabeth Howell, "Russia Is Jamming GPS Satellite Signals in Ukraine, US Space Force Says," *Space.com*, 12 April 2022, https://www.space.com/russia-jamming-gps-signals-ukraine.

71 U.S. Space Force, "GPS Control Segments," *Global Positioning System (GPS).org*, https://www.gps.gov/systems/gps/control/#:~:text=The%20GPS%20control%20segment%20consists,and%20data%20to%20the%20constellation, accessed 3 August 2023.

72 Patrick Smith, "Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy," American Security Project, 2020, https://www.jstor.org/stable/resrep24679.

73 "GNSS Signal - Navipedia," https://gssc.esa.int/navipedia/index.php/GNSS_signal, accessed 1 May 2023.

74 Captain Brian C. Barker et al., "Overview of the GPS M Code Signal," n.d., https://www.mitre.org/sites/default/files/pdf/betz_overview.pdf, accessed 7 September 2023.

75 Peter A. Iannucci and Todd E. Humphreys, "Fused Low-Earth-Orbit GNSS," *ArXiv: Signal Processing*, 2020.

76 Prol et al., "Position, Navigation, and Timing."

77 Muhammad Yeasir Arafat, Muhammad Morshed Alam, and Sangman Moh, "Vision-Based Navigation Techniques for Unmanned Aerial Vehicles: Review and Challenges," *Drones*, Vol. 7, no. 2 (February 2023): 89, https://doi.org/10.3390/drones7020089, accessed 20 June 2023.

78 This mantra is key to SEALs thinking. It simply emphasizes the importance of a backup plan. The concept is that "having one of something is like having none at all and that having two of anything is the same as what you think having one is. This concept is applied to everything in the sphere of a SEAL's world from supplies to weapons to gear and even clothing (…) It most importantly applies to mission planning. One plan means no plan. Two plans? Well that's as good as one." Matt Given, "This Navy SEAL Hack for Planning is a Game Changer," *Inc.com*, n.d., https://www.inc.com/matt-given/this-1-lesson-from-how-the-navy-seals-plan-their-m.html, accessed 25 June 2023.

79 Vivienne Machi, "US Military Places a Bet on LEO for Space Security," *Space Development Agency*, June 2021. https://www.sda.mil/us-military-places-a-bet-on-leo-for-space-security/, accessed 19 May 2023.

80 Ibid.

81 "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine." *Royal United Services Institute*, 19 May 2023, https://rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine, accessed 23 June 2023.

82 A. Datta, "NRO Announces Billion-Dollar Historic Commercial Imagery Contracts to Maxar, Planet and BlackSky," *Geospatial World*, 26 May 2022, https:// www.geospatialworld.net/blogs/nro-announces-billion-dollar-historic-commercial-imagery-contracts-to-maxar-planet-and-blacksky/, accessed 7 September 2022.

83 Kate Duffy, "Elon Musk says SpaceX has sent 15000 Starlink internet kits to Ukraine over the past 3 months," *Business Insider*, 6 June 2022, https://www.businessinsider.com/elon-musk-spacex-sent-starlink-satellite-internet-terminals-ukraine-2022-6.

84 John M. Olson et al., "State of the Space Industrial Base 2022," Defense Innovation Unit, August 2022, 51, https://www.diu.mil/latest/state-of-the-space-industrial-base-2022, accessed 23 June 2023.

85 Ibid.

86 Emily Harding and Harshana Ghoorhoo, "Seven Critical Technologies for Winning the Next War: A Report of the CSIS International Security Program," *Center for Strategic & International Studies*, April 2023, 10, https://www.csis.org/.

87 Theresa Hitchens. "Space Force Eyes Commercial P-LEO SATCOM." *Breaking Defense,* 5 October 2021. https://breakingdefense.com/2021/10/space-force-eyes-commercial-p-leo-satcom/, accessed 10 July 2023.

88 U.S. Space Force, "United States Space Force Vision for Satellite Communications (SATCOM)," 23 January 2020, https://www.spaceforce.mil/Portals/1/SATCOM%20Vision%20Paper.pdf, accessed 29 June 2023.

89 *DoD Strategic Management Plan FY22-FY26* (updated), 6 March 2023. https://media.defense.gov/2023/Mar/13/2003178168/-1/-1/1/DOD-STRATEGIC-MGMT-PLAN-2023.PDF, accessed 02 August 2023.

90 Harding and Ghoorhoo, "Seven Critical Technologies, 14.

91 "Initial contracts for Hybrid Space Architecture Program," *Defense Innovation Unit* 6 July 2022, https://www.diu.mil/latest/developing-the-internet-of-space, accessed 29 June 2023.

92 Courtney Albon, "Defense Innovation Unit Teams with Companies on Space-Based Internet." C4ISRNet, 10 July 2023, https://www.c4isrnet.com/battlefield-tech/space/2023/07/10/defense-innovation-unit-teams-with-companies-on-space-based-internet/, accessed 30 August 2023.

93 Olson et al., "State of the Space Industrial Base."

94 Ibid.

95 Rachael Zisk, "The Proliferated Warfighter Space Architecture (PWSA): An Explainer," *Payload*, 23 January 2023, https://payloadspace.com/ndsa-explainer/, accessed 29 June 2023.

96 Ibid.

97 C. Todd Lopez. "Agency Director Discusses Multi-Pronged Approach to Resiliency in Space." *U.S. Department of Defense,* 4 April 2023, https://www.defense.gov/News/News-Stories/Article/Article/3351552/agency-director-discusses-multi-pronged-approach-to-resiliency-in-space/, accessed 29 June 2023.

98 John R. Hoehn, "Joint All-Domain Command and Control (JADC2)," *Congressional Research Service*, 21 January 2022, https://sgp.fas.org/crs/natsec/IF11493.pdf, accessed 30 August 2023.

99 U.S. Army Weapons Command, Directorate of R&D, Future Weapons Office, "The Meanderings of a Weapon Oriented Mind When Applied in a Vacuum Such as the Moon," June 1965, https://www.documentcloud.org/documents/3038458-The-Meanderings-of-a-Weapon-Oriented-Mind-When.html, accessed 7 September 2023; and Joseph Trevithick, "The U.S. Army's Gun-Toting Space Soldiers," *War is Boring*, 9 November 2015, https://warisboring.com/the-u-s-army-had-plans-for-gun-toting-space-soldiers/, accessed 30 June 2023.

100 Bruce W. MacDonald, Carla P. Freeman, and Alison McFarland. "China and Strategic Instability in Space: Pathways to Peace in an Era of US-China Strategic Competition," Special Report No. 515, *United States Institute of Peace,* February 2023, https://www.usip.org/sites/default/files/2023-02/20230209-sr-515-china-strategic-instability-space.pdf.

101 Ibid., 19.

102 J. Michael Dahm, "Electronic Warfare and Signals Intelligence," *South China Sea Military Capabilities Series: A Survey of Technologies and Capabilities on China's Military Outposts on the South China Sea,*" Johns Hopkins Applied Physics Laboratory, 2020, https://www.jhuapl.edu/work/publications/south-china-sea-military-capabilities-series, accessed 8 September 2023.

103 D.J. Kessler and B.G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research*, Vol. 83, no. A6 (1 June 1978): 2637-2646.

104 Donald Kessler, Nicholas Johnson, Nicholas, J.C. Liou and Mark Matney, "The Kessler Syndrome: Implications to Future Space operations," *Advances in the Astronautical Sciences*, 2010, 137, https://aquarid.physics.uwo.ca/kessler/Kessler%20Syndrome-AAS%20Paper.pdf, accessed 29 August 2023.

105 MacDonald et al, "China and Strategic Instability in Space"; Irina Liu et al., *Evaluation of China's Commercial Space Sector* (Alexandria, VA: Institute for Defense Analyses, 2019), 11-26, https//www.jstor.org/stable/resrep22872.5; and Matthew Daniels, "The History and Future of US–China Competition and Cooperation in Space," Johns Hopkins Applied Physics Laboratory, 2020, 4-5, https://www.jhuapl.edu/Content/documents/Daniels-Space.pdf; and Namrata Goswami, "China in Space: Ambitions and Possible Conflict," *Strategic Studies Quarterly*, Vol. 12, no. 1 (Spring 2018): 76.

106 Michael Sheetz, "In race to provide internet from space, companies ask FCC for about 38,000 new broadband satellites," *CNBC*, 5 November 2021, https://www.cnbc.com/2021/11/05/space-companies-ask-fcc-to-approve-38000-broadband-satellites.html, accessed 4 August 2023.

107 Michael Bennett and Corinne Kramer, "Large Constellations of Low-Altitude Satellites: A Primer," *Congressional Budget Office,* May 2023, https://www.cbo.gov/publication/59175#"_idTextAnchor073, accessed 30 August 2023.

108 Rachel S. Cohen, "Space Force Boss Signs 'Fighting SATCOM' Strategy," *Air and Space Forces Magazine,* 20 February 2020, https://www.airandspaceforces.com/space-force-boss-signs-fighting-satcom-strategy/, accessed 29 August 2023.

109 "Defense Space Strategy Summary," U.S. DoD, June 2020, https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF, accessed 29 August 2023.

110 "Space Threat Assessment 2023," *Aerospace Security Project at the Center for Strategic and International Studies* (CSIS), 6th Edition, 14 April 2023, https://www.csis.org/analysis/space-threat-assessment-2023, accessed 29 August 2023.

111 China Power Team, "What's Driving China's Race to Build a Space Station?" *China Power*, 7 December 2016, https://chinapower.csis.org/chinese-space-station/, accessed 3 July 2023.

112 Sandra Erwin. "Hyten blasts 'unbelievably' slow DoD bureaucracy as China advances space weapons," *Space News,* 28 October 2021, https://spacenews.com/hyten-blasts-unbelievably-slow-dod-bureaucracy-as-china-advances-space-weapons/, accessed 30 August 2023.

CHAPTER 16

1 Edward N. Luttwak, "Notes on Low-Intensity Warfare," *Parameters*, Vol. 13, no. 4 (December 1983): 17.

2 Michael P. Noonan, *Irregular Soldiers and Rebellious States: Small-Scale U.S. Interventions Abroad* (Lanham, MD: Rowman & Littlefield Publishing Group, 2021), 41.

3 Fernando M. Luján, *Light Footprints: The Future of American Military Intervention* (Washington, D.C.: Center for a New American Security, 2013).

4 Rob Newson, "Adapting for the 'Other War,'" *Small Wars Journal*, 18 October 2013. https://smallwarsjournal.com/jrnl/art/adapting-for-the-%e2%80%9cother%e2%80%9d-war.

5 Luján, *Light Footprints*, 5.

6 David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2009), 283.

7 Colin S. Gray, *Explorations in Strategy* (Westport, CT: Greenwood Press, 1996), 168.

8 Luján, *Light Footprints*, 10.

9 Ibid., 5.

10 Abigail Watson and Alasdair McKay, "Remote Warfare: A Critical Introduction," *E-International Relations*, 11 February 2021, 17.

11 Jolle Demmers and Lauren Gould, "The Remote Warfare Paradox: Democracies, Risk Aversion and Military Engagement," *E-International Relations*, 20 June 2020, 1.

12 Jolle Demmers and Lauren Gould, "An Assemblage Approach to Liquid Warfare: AFRICOM and the 'Hunt' for Joseph Kony," *Security Dialogue*, Vol. 49, no. 5 (October 2018): 364.

13 Source: Abigail Watson, "The Perils of Remote Warfare: Finding a Political Settlement with Counter-Terrorism in the Driving Seat," *The Strategy Bridge*, December 5, 2018, https://thestrategybridge.org/the-bridge/2018/12/5/the-perils-of-remote-warfare-finding-a-political-settlement-with-counter-terrorism-in-the-driving-seat.

14 Tom Watts and Rubrick Biegon, *Defining Remote Warfare: Security Cooperation* (London: Remote Control, 2017); Demmers and Gould, "An Assemblage Approach to Liquid Warfare"; and Watson and McKay, "Remote Warfare," 1.

15 Watson and McKay, "Remote Warfare," 1.

16 Watts and Biegon, *Defining Remote Warfare*, 1.

17 James Rogers and Delina Goxho, "Light Footprint—Heavy Destabilising Impact in Niger: Why the Western Understanding of Remote Warfare Needs to Be Reconsidered," *International Politics*, 11 January 2022, 1-28.

18 Demmers and Gould, "The Remote Warfare Paradox," 1.

19 Ibid., 1.

20 Watson and McKay, "Remote Warfare."

21 Michael P. Mahaney, *Striking a Balance: Force Protection and Military Presence, Beirut, October 1983* (Fort Leavenworth, KS: Army Command and General Staff College, 2001).

22 Gordon H. McCormick, "Guerilla Warfare Seminar" (Lecture, Naval Postgraduate School, Monterey, CA, January 4, 2023).

23 Ibid.

24 Gordon H. McCormick and Frank Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," *Third World Quarterly*, Vol. 28, no. 2 (2007): 295-320; Gordon H. McCormick, Steven B. Horton, and Lauren A. Harrison, "Things Fall Apart: The Endgame Dynamics of Internal Wars," *Third World Quarterly*, Vol. 28, no. 2 (2007): 321-367; and Moshe Kress and Roberto Szechtman, "Why Defeating Insurgencies Is Hard: The Effect of Intelligence in Counterinsurgency Operations--A Best-Case Scenario," *Operations Research*, Vol. 57, no. 3 (2009): 578-585.

25 Nathan Constantine Leites and Charles Wolf, *Rebellion and Authority; an Analytic Essay on Insurgent Conflicts* (Chicago: Markham Pub. Co., 1970), 147; McCormick, Horton, and Harrison, "Things Fall Apart"; and Kress and Szechtman, "Why Defeating Insurgencies Is Hard."

26 Kress and Szechtman, "Why Defeating Insurgencies Is Hard."

27 Gordon H. McCormick, "The Complete Win" (RAND-CIA Insurgency Board Quarterly Conference, 14 February 2011).

28 McCormick, Horton, and Harrison, "Things Fall Apart"; McCormick and Giordano, "Things Come Together"; and Kress and Szechtman, "Why Defeating Insurgencies Is Hard."

29 Emily Harding et al., "Sparking a Revolution in Open Source Intelligence [Transcript]," Online Event (Washington, DC: Center for Strategic and International Studies, 3 December 2021), 9, https://www.csis.org/events/sparking-revolution-open-source-intelligence.

30 Harding et al., "Sparking a Revolution in Open Source Intelligence [Transcript]."

31 Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 9th ed. (Thousand Oaks, CA: CQ Press, 2023), 112.

32 Robert Hight, "Principles of Joint Operational Intelligence - Session 14: Geospatial Intelligence (GEOINT)" (Lecture, Naval Postgraduate School, Monterey, CA, 23 February 2023).

33 Lowenthal, *Intelligence*, 119.

34 Ibid., 119.

35 Jeff Giesea, "Hybrid Intelligence As A Response to Hybrid Warfare? How To Make Intelligence Collection & Verification Cheaper, Faster, and Better Using New Technologies," *Small Wars Journal*, 7 February 2023, https://smallwarsjournal.com/jrnl/art/hybrid-intelligence-response-hybrid-warfare.

36 Lowenthal, *Intelligence*, 119.

37 David P. Oakley, *Partners or Competitors? The Evolution of the Department of Defense/ Central Intelligence Agency Relationship since Desert Storm and Its Prospects for the Future:* (MacDill AFB, FL: Joint Special Operations University, 2014).

38 William Burke, "Security Cooperation: Constraints and Opportunities in Operationalizing Resilience and Resistance" (Lecture, Naval Postgraduate School, Monterey, CA, 1 May 2023).

39 Rogers and Goxho, "Light Footprint—Heavy Destabilising Impact in Niger," 10.

40 Ibid., 10.

41 Ibid.

42 Ibid.

43 Ibid.

44 Adapted from: Rogers and Goxho, "Light Footprint—Heavy Destabilising Impact in Niger."

45 NATO, "Three Allies Establish Special Forces Command," 7 June 2018, http://www.nato.int/cps/en/natohq/news_155347.htm.

CHAPTER 17

1 For example, see Bernd Horn and Emily Spencer, "Force of Choice: SOF as a Foreign Policy Enabler," in Emily Spencer, ed., *Special Operations Forces: Building Global Partnerships* (Kingston: CDA Press, 2012), 1-28.

2 See Colonel Bernd Horn, "When Cultures Collide: The Conventional Military / SOF Chasm," *Canadian Military Journal*, Vol. 5, no. 3 (Autumn 2004): 3-16; and Colonel Bernd Horn, "Love 'Em or Hate 'Em: Learning to Live with Elites," *Canadian Military Journal*, Vol. 8, no. 4 (Winter 2007-2008): 32-43.

3 Canada, *Canadian Special Operation Forces Command. An Overview* (DND: Ottawa, 2008), 7.

4 Colin Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1996), 149.

5 SOF characteristics include:

1. Small footprint / small team deployments;
2. SOF can operate clandestinely, covertly or overtly;
3. Operations are often conducted at great distances from a supporting operational base;
4. SOF utilize sophisticated means of insertion, support, and extraction to penetrate and successfully return from hostile, denied, or politically sensitive areas;
5. SOF employ sophisticated communications systems;
6. SOF are proficient with, and enabled by, application of advanced technologies;
7. SOF utilize unorthodox tactics;
8. SOF often require development, acquisition, and employment of equipment that are not standard for others;
9. SOF normally conduct operations "General Purpose Forces" cannot perform;
10. SOF are well-suited for operations in denied and politically sensitive environments;
11. SOF conduct operations not only against military objectives, but also to support the application of the diplomatic, informational, and economic instruments of national power;
12. SOF are capable of working independently or in conjunction with conventional forces or other government agencies, or host nations/partner nations;
13. SOF are proficient at inter-organizational coordination; and
14. SOF missions are differentiated by physical and political risk, operational techniques, modes of employment, and dependence on detailed operational intelligence and indigenous assets.

6 For example, trends in military spending that are arguably indicative of effectiveness highlight the growth of SOF. The US Special Operations Command budget has been increased from $3.8 billion to almost $10 billion over the last decade. Quoted in Aki Peritz & Eric Rosenbach, *Find, Fix Finish. Inside the Counterterrorism Campaigns that Killed Bin Laden and Devastated Al-Qaeda* (New York: Public Affairs, 2012), 232. In addition, the U.S. military newspaper *Stars and Stripes* publicly reported that the Pentagon is preparing to "unleash special operations troops worldwide as traditional operations are cut back." Cited in Julie Levesque, "US Army Goes Underground: Special Ops Deployed Worldwide," *Global Research*, 27 January 2012.

7 The author of the five SOF Truths is American Colonel John M. Collins. The "Truths" are:

1. *Humans are more important than hardware;*
2. *Quality is better than quantity:*
3. *SOF cannot be mass produced;*
4. *Competent SOF cannot be rapidly created after emergencies occur; and*
5. *Most Special Operations require non-SOF assistance.*

CONTRIBUTORS

ARQUILLA – Dr. John Arquilla is Distinguished Professor Emeritus of Defense Analysis at the U.S. Naval Postgraduate School (NPS) at Monterey. He is the author or co-author of over a dozen books covering a range of topics, from irregular warfare (e.g., *Insurgents, Raiders, and Bandits,* Rowman 2011; and *Afghan Endgames,* Georgetown 2012) to cybersecurity *(Bitskrieg,* Polity 2021). Dr. Arquilla is best known for pioneering the concepts of cyberwar and swarm tactics, and is currently pursuing an effort to encourage the application of design thinking to the realm of military strategy.

BIBBS – Lieutenant (JAG) Charles Bibbs is a member of the U.S. Navy and a student at NPS.

BLOCKSOME – Dr. Patricia J. Blocksome's research focuses on special operations, unconventional/proxy warfare, and rebel group operations and strategy. Her most recent publication is the chapter "Conceptualizing Strategic Sabotage" in the book *The (In)Visible Hand: Strategic Sabotage Case Studies*. She is the co-editor of the book *Special Operations: Out of the Shadows* and the author of numerous journal articles. She serves as the vice president for research at the Special Operations Research Association, the managing editor for *Special Operations Journal*, an associate editor on the *Journal of Interdisciplinary Conflict Science*, and as a member of the JSOU Press Editorial Board. Prior to joining Joint Special Operations University as an associate professor, she taught at the U.S. Naval War College and at the U.S. Army School of Advanced Military Studies. She received her PhD in Security Studies from Kansas State University.

BOSCH – Major Ruud van den Bosch is an officer in the Royal Netherlands Marine Corps. He holds a Master's degree in Military History from the University of Amsterdam. He is currently assigned to NPS as a student of the Defense Analysis M.Sc. program and the U.S. Marine Corps Command and Staff College.

BOSS – Major Christopher M. Boss is a Special Forces officer in the U.S. Army, who is currently pursuing an additional Master's degree in the "Applied Design for Innovation" program within the esteemed Defense Analysis Department at NPS. Previously, he taught at the U.S. Army John F. Kennedy Special Warfare Center and School. During this time, he attended Harvard University and graduated from their "Essential Skills for Innovation" professional development program. In his operational capacity, Major Boss has garnered rich experience through several deployments to Africa, most recently as a Special Forces Detachment Commander.

COUILLARD – Lieutenant-Colonel Mathieu Couillard is a Signals Officer in the Canadian Army. He has served in a variety of command and staff roles within the Canadian Armed Forces (CAF) domestically and abroad. He holds a Bachelor of Engineering in Computer Engineering from Université Laval, and Master of Science degrees in Defense Analysis (Irregular Warfare & Special Operations) and Computer Science (Cyber Operations) from NPS. At NPS, he graduated with distinction and received the Rear Admiral Grace Murray Hopper Computer Science Award and the Gary Kildall Award for Computing Innovation. Lieutenant-Colonel Couillard is currently employed as J6 of the Canadian Special Operations Forces Command (CANSOFCOM).

CRANINX – Major Cedric Craninx is an Army Special Operations Officer in the Belgian Defence Forces. He holds a Master of Science degree from the Belgian Royal Military Academy and a Master of Science degree in Defense Analysis from NPS. He has held command and staff appointments in the Belgian SOF community, including Platoon Commander in the 1st Para Bn, Coy 2nd in Command in the 2nd Bn Commando, and Team Leader, Troop Commander, and Operations & Training (S3) Officer in the Belgian Special Forces Group.

CUNNINGHAM – Major Patrick Cunningham is an U.S. Army officer pursuing his Master of Science degree at NPS. He maintains a broad range of operational experiences across multiple domains in multiple AORs.

DUMAS – Lieutenant (Navy) Austin Dumas is a member of the U.S. Navy and a student at NPS.

FAUKSTAD – Commander Senior Grade (Navy) Nikolai Faukstad is an officer in the Norwegian Armed Forces. He has served in the Norwegian Special Forces (MJK) for most of his career and held multiple command and staff positions. Throughout his career, Faukstad has served in various domestic and international assignments, including squadron commander and task group commander. He is currently serving as a senior staff officer in the Norwegian Ministry of Defence, in the department of defence policy and long-term planning. He obtained a Master of Business and Administration degree from the University of Tromsø, Norway, in 2020, and subsequently completed a Master of Science in Defense Analysis at NPS in 2023.

GANS – Lieutenant-Colonel Ben Gans is a military officer in the Netherlands Armed Forces and currently assigned to NPS where he serves as visiting professor in the Defense Analysis Department. He holds a PhD in business administration and has authored work on civil-military relations, military strategy, and stabilization operations. Currently he is working on a forthcoming book titled *Special Operations in Strategic Competition: Policies, Strategies, and Tactics* (Routledge).

HANSEN – Lieutenant (Navy) Lloyd (Forrest) Hansen is a member of the U.S. Navy and a student at NPS.

HORN – Colonel (retired) Bernd Horn, PhD is a former infantry officer who has held key command and staff appointments in the CAF, including Deputy Commander of 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. He has authored, co-authored, edited or co-edited 50 books and numerous monographs/chapters/articles on military history, SOF, leadership and military affairs.

LAUZEN – Lieutenant Commander Hans Lauzen is a member of the U.S. Navy and a student at NPS.

MEARS – Lieutenant (Navy) Christopher Mears is a member of the U.S. Navy and a student at NPS.

MORRIS – Major Reuben Morris is an active-duty Army Civil Affairs officer who has served in Special Operations for the last eight years. He has numerous operational deployments supporting resistance and resilience efforts in the European theatre of operations. He is currently studying the tactics and strategies of maximalist social movements at NPS.

PANELLA – Cecilia Panella is a Faculty Associate-Research in the Defense Analysis Department at NPS. She works primarily with the Applied Design for Innovation program and the Naval Warfare Studies Institute. She holds a graduate degree in American Foreign Policy and International Economics from Johns Hopkins SAIS.

SCHWARZBAUER – Lieutenant-Colonel Matthias Schwarzbauer is an infantry officer in the German Armed Forces. He holds a Master of Science degree in economics and organizational sciences from the German Armed Forces University Munich and a Master of Science degree in Defense Analysis from NPS. He is also a graduate of the U.S. Marine Corps Command and Staff College (CDET).

SOULES – Michael J. Soules, Ph.D., is an Assistant Professor of Political Science at the University of Houston. He was previously a Donald R. Beall Defense Fellow at NPS. His research focuses on terrorism and civil wars. His research has appeared in journals including *International Studies Quarterly, Journal of Conflict Resolution, Security Studies* and *Conflict Management and Peace Science,* among others.

TAILLON – Colonel (retired) J. Paul de B. Taillon, PhD, served in the Canadian intelligence community for 30 years. During this period, he has served as a reserve army officer in numerous command and staff positions on reserve/active duty. A graduate of the USMC Amphibious Warfare School,

USMC Command and Staff College and the U.S. Army War College he completed his doctorate at the London School of Economics and Political Science. He has served with Canadian, American and British special forces and has deployed to Bosnia, Croatia, Kosovo, Afghanistan and the Ukraine. From 2006-2014 he was the Strategic/Counter-insurgency Advisor to the Commander the Canadian Army and took part in 22 mobile training teams under the auspices of USSOCOM. Dr. Taillon is an Adjunct Fellow at the Joint Special Operations University and has taught at the Royal Military College of Canada, Canadian Forces Command and Staff College, Toronto, United States Marine Corps Command and Staff College, Quantico, Virginia, as well as NPS. He was also instructional staff at the NATO Special Operations School at Chièvres, Belgium. He has authored numerous books and articles and was appointed as the Honourary Colonel of the Canadian Grenadier Guards.

GLOSSARY OF ABBREVIATIONS

160th SOAR	160th Special Operations Aviation Regiment
427 SOAS	427 Special Operations Aviation Squadron
9/11	11 September 2001
A2/AD	Anti-Access / Area Denial
ABI	Activity-Based Intelligence
AFRICOM	United States African Command
AI	Artificial Intelligence
AO	Area of Operation
AOR	Area of Responsibility
AQ	al-Qaeda
AQI	al-Qaeda in Iraq
AQIM	al-Qaeda in the Islamic Maghreb
ARSOF	Army Special Operations Forces
ASAT	Anti-Satellite
ASEAN	Association of Southeast Asian Nations
BMV	Bergen Mekaniske Verksted
BPC	Building Partner Capacity
BRI	Belt and Road Initiative
C2	Command and Control
C3	Command, Control and Communications
C5ISRT	Command, Control, Computing, Communications, Cyber, Intelligence, Surveillance, Reconnaissance, and Targeting
CAR	Central African Republic
CCG	Civilian Coast Guard
CCP	Chinese Communist Party

CCRAK	Covert, Clandestine, and Related Activities – Korea
CCTV	Closed-Circuit Television
Cdr	Commander
CENTCOM	Central Command
CIA	Central Intelligence Agency
CIDG	Civilian Irregular Defense Group
CIGS	Chief of the Imperial General Staff
CITES	Convention on International Trade in Endangered Species
CJADC2	Combined Joint All-Domain Command and Control
CMPR	China Military Power Report
CMS	Chinese Marine Surveillance
CNO	Chief of Naval Operations
CNOOC	China National Offshore Oil Corporation
CNSA	China National Space Administration
COIN	Counter-insurgency
COMSAT	Communications Satellite Corporation
COTS	Commercial Off-the-Shelf
CPEC	China-Pakistan Economic Corridor
CSIS	Canadian Security Intelligence Service
CSOCC	Composite Special Operations Component Command
CT	Counterterrorism
C-VEO	Counter-Violent Extremist Organizations
DA	Direct Action
DA-ASAT	Direct Ascent Anti-satellite
DARPA	Defense Advanced Research Projects Agency
DDMA	Defence, Diplomacy and Military Assistance
DEVGRU	Naval Special Warfare Development Group
DIA	Defense Intelligence Agency
DIU	Defense Innovation Unit
DMO	Distributed Maritime Operations
DoD	Department of Defense
DPP	Democratic Progressive Party

DSCS	Defense Satellite Communications System
DSU	Directorate of Special Units
EEZ	Exclusive Economic Zone
ELINT	Electronic Intelligence
EMCON	Electromagnetic Control
ESI	*Escadron spécial d'intervention*
EU	European Union
EW	Electronic Warfare
FDR	Federal Republic of Germany
FEC	Far East Command
FFI	French Forces of the Interior
FID	Foreign Internal Defense
FLEC	Fisheries Law Enforcement Command
FLIR	Forward Looking Infrared
FLQ	*Front de Libération du Québec*
FoA	Freedom of Action
GEO	Geostationary-Earth Orbit
GEOINT	Geospatial Intelligence
GGF	Great Green Fleet
GHQHF	General Headquarters Home Forces
GIGN	*Groupe d'intervention de la Gendarmerie nationale*
GIS	*Gruppo di Intervento Speciale*
GLONASS	*Globalnaya Navigatsionnaya Sputnikovaya Sistema*
GNSS	global navigation satellite system
GPC	Great Power Competition
GPS	Global Positioning System
GRU	*Glavnoye Razvedyvatelnoye Upravlenie* – Foreign Military Intelligence Agency (Russian Federation)
GSG 9	*Grenzschutzgruppe* 9
GWOT	Global War on Terror

HSA	Hybrid Space Architecture
HUMINT	Human Intelligence
HVT	High Value Target or High Value [depending on context]
IC	Intelligence Community
IMSI	International Mobile Subscriber Identity Number
INDOPACOM	Indo-Pacific Command
INT	Intelligence (Collection Disciplines)
IO	Information Operations
IORG	Information Operations Research Group
IP	Internet Protocol
IR	Irregular Warfare
IRA	Irish Republican Army
IS	Islamic State
ISAF	International Security Assistance Force
ISIS	Islamic State of Iraq and Syria
ISR	Intelligence, Reconnaissance, and Surveillance
JADC2	Joint All-Domain Command and Control
JIIM	Joint, Interagency, Intergovernmental, and Multinational
JNIM	Jama'at Nusrat al-Islam wal-Muslimin
JSOC	Joint Special Operations Command
KKV	Kinetic Kill Vehicle
KMT	Kuomintang
LEA	Law Enforcement Agency
LEO	Low Earth Orbit
LLM	Large Language Models
LRPA	Long Range Patrol Aircraft
LRRP	Long Range Reconnaissance Patrols
MA	Military Assistance
MACV	Military Assistance Command Vietnam
MAVNI	Military Accessions Vital to National Interests

MCF	Military-Civil Fusion
MDAS	Multi-Domain Autonomous Systems
MI6	Special Intelligence Service
MILSATCOM	Military-specific SATCOM
MISO	Military Information Support Operations
ML	Machine Learning
MoD	Russian Ministry of Defense
MoE	Measures of Effectiveness
MSKIs	Noncombat Musculoskeletal Injuries
MSS	Ministry of State Security
NAF	Norwegian Armed Forces
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCTV	National Coordinator for Security and Counterterrorism
NDS	National Defense Strategy
NGO	Non-Governmental Organization
NIS	Norwegian Intelligence Service
NRF	NATO Response Force
NSS	Network Systems Department
NSW	Naval Special Warfare
NVA	North Vietnamese Army
OCS	Operational Control Segment
ODA	Operational Detachment Alpha
OGD	Other Government Department
OIE	Operations in the Information Environment
OIR	Operation Inherent Resolve
OPCOM	Operational Command
OPEC	Organization of the Petroleum Exporting Countries
OPFOR	Opposing Force
OPSEC	Operational Security

OSCE	Organization for Security and Co-operation in Europe
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
PACE	Primary, Alternate, Contingency, and Emergency
PAFMM	People's Armed Forces Maritime Militia
PAP	People's Armed Police
PFLP	Liberation of Palestine
PIFWC	Persons Indicted for War Crimes
PLA	People's Liberation Army
PLAN	People's Liberation Army Navy
PLASSF	People's Liberation Army Strategic Support Force
PLEO	Proliferated Low-Earth-Orbit
PLO	Palestinian Liberation Organization
PMC	Private Military Company
PNT	Position, Navigation, and Timing
PPD	Payload Delivery Systems
PRC	People's Republic of China
PSYOP	Psychological Operations
PWSA	Proliferated Warfighter Space Architecture
R&D	Research and Development
RAF	Royal Air Force
RCAF	Royal Canadian Air Force
RF	Russian Federation
RIMPAC	Rim of The Pacific
RM	Resource Mobilization
ROC	*Resistance Operating Concept*
RSF	Rapid Support Forces
SACEUR	Supreme Allied Commander Europe
SAS	Special Air Service
SASC	Senate Committee on Armed Services

SASR	Special Air Service Regiment (Australia)
SATCOM	Satellite Communications
SATCOMA	Satellite Communications Agency
SBIR	Small Business Innovation Research
SBS	Special Boat Service
SCS	South China Sea
SDA	Space Development Agency
SEAL	Sea, Air, Land
SF	Special Forces
SFG	Special Forces Group
SFHQ	Special Forces Headquarters
SHAEF	Supreme Headquarters Allied Expeditionary Force
SIGINT	Signals Intelligence
SIS	Special Intelligence Service
SISMI	*Servizio per le Informazioni e la Sicurezza Militare* – Military Intelligence and Security Service (Italy)
SMT	Social Movement Theory
SO	Special Operations or Stability Operations [depending on context]
SOCAFRICA	U.S. Special Operations Command Africa
SOE	Special Operations Executive
SOF	Special Operations Forces
SOG	Studies and Observation Group
SOTG	Special Operations Task Group
SR	Special Reconnaissance
SSD	Space Systems Department
SSRF	Scale Raiding Force
STR	Support to Resistance
SW	Special Warfare
TC	Theatre Command
TMH	Transmashholding Group
TTP	Tactics, Techniques and Procedures

U.S.	United States of America
UAV	Unmanned Aerial Vehicles
UDT	Underwater Demolition Team
UFWD	United Front Work Department
UK	United Kingdom
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
USC	United Shipbuilding Corporation
USD	U.S. Dollars
USNS	U.S. Navy Ship
USSF	United States Special Forces
USSOCOM	U.S. Special Operations Command
USV	Unmanned Surface Vehicles
UW	Unconventional Warfare
UXS	Unmanned System
VPN	Virtual Private Network
WGS	Wideband Global SATCOM
WMD	Weapons of Mass Destruction
WS	Weapon System
WWII	World War II

INDEX

CANSOFCOM EDUCATION & RESEARCH CENTRE (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, eds., 2021.

A Perilous Future: High Intensity Conflict and the Implications for SOF
Lieutenant-Colonel Andrew L. Brown, PhD, ed., 2022.

Strategic Competition: Implications for SOF
Colonel (retired) Bernd Horn, PhD, 2022.

Operating on the Margins: SOF in the Gray Zone
Dr. Howard G. Coombs with Dr. Christopher Marsh, eds., 2023.

Force Multiplier: Utilization of SOF from a Small State Perspective
Colonel (Retired) Bernd Horn and Colonel (Retired) Hans Ilis-Alm, 2024.

Threat in the national security context can be defined as state or non-state actor actions that can cause disruption, damage and potential ruin of another state's national security, economic, defence and political stability and/or sovereignty. Threats must be assessed against an adversary's intent, opportunity and capability. Clearly assessment is as much art as it is science and must be considered within the context of an ambiguous, dynamic and extremely complex security environment. Response to threat(s) must be calibrated accordingly. This volume examines threat through three different lenses: historical, from a macro perspective of "below the threshold of armed conflict" to more specific threats, and finally, potential SOF/SO responses to the myriad of existing and emerging threats that face partner nations.