



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MILLENNIALS IN COMMAND: #INFILTRATION

by

Joseph D. Davis and William W. Bochner

June 2019

Thesis Advisor:

Robert E. Burks

Co-Advisor:

Michael E. Freeman

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2019	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE MILLENNIALS IN COMMAND: #INFILTRATION			5. FUNDING NUMBERS	
6. AUTHOR(S) Joseph D. Davis and William W. Bochner				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The relevance and best utilization of traditional SOF Infiltration methods are depicted for the battlefield of 2035. Through an analysis of trends in demographics, technology, diffusion of social media, and adversary capabilities, the study focuses on civilian population density and connectivity, and their relation to a SOF unit's ability to conduct time-sensitive, direct action operations. This study first outlines a typology for describing an operational environment, past or future, using the variables of population density and connectivity. Next, using the established typology, the study analyzes historical case studies of both military and non-military infiltration in environments that share characteristics with the proposed future environment, recognizing that no historical environments exist that simultaneously exhibit both the population density and connectivity of the future. The study then identifies among the case studies the characteristics that historically resulted in successful infiltration, with the goal of developing a heuristic approach to the problem of infiltration in a future environment. Finally, this thesis offers recommendations for the direction in which SOF capabilities (tactical, platform-based, and a planning mindset) should advance to conduct successful infiltration on the battlefields of 2035 and beyond.				
14. SUBJECT TERMS Special Operations, SOF, Infiltration, global connectivity, population density, future battlespace, 2035, technology, megacity, deception, stealth, cyber, subterranean			15. NUMBER OF PAGES 77	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

MILLENNIALS IN COMMAND: #INFILTRATION

Joseph D. Davis
Major, United States Air Force
BS, The Ohio State University, 2005
MA, American Military University, 2013

William W. Bochner
Lieutenant, United States Navy
BS, U.S. Naval Academy, 2011

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2019**

Approved by: Robert E. Burks
Advisor

Michael E. Freeman
Co-Advisor

John J. Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The relevance and best utilization of traditional SOF Infiltration methods are depicted for the battlefield of 2035. Through an analysis of trends in demographics, technology, diffusion of social media, and adversary capabilities, the study focuses on civilian population density and connectivity, and their relation to a SOF unit's ability to conduct time-sensitive, direct action operations. This study first outlines a typology for describing an operational environment, past or future, using the variables of population density and connectivity. Next, using the established typology, the study analyzes historical case studies of both military and non-military infiltration in environments that share characteristics with the proposed future environment, recognizing that no historical environments exist that simultaneously exhibit both the population density and connectivity of the future. The study then identifies among the case studies the characteristics that historically resulted in successful infiltration, with the goal of developing a heuristic approach to the problem of infiltration in a future environment. Finally, this thesis offers recommendations for the direction in which SOF capabilities (tactical, platform-based, and a planning mindset) should advance to conduct successful infiltration on the battlefields of 2035 and beyond.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	1
1.	Traditional SOF Infiltration	2
2.	Future SOF Core Tasks.....	3
3.	Why Population Density and Connectivity?	3
B.	POPULATION DENSITY	5
1.	Trends	5
2.	Consequences.....	7
C.	CONNECTIVITY	10
1.	Trends	10
2.	Consequences.....	17
II.	THEORY OF FUTURE SOF INFILTRATION.....	19
A.	DECEPTION VS. STEALTH.....	19
1.	Literature on Deception	20
2.	What Does this Mean in the Millennial Battlespace?	21
3.	Case Analysis.....	22
B.	COGNITIVE VS. PHYSICAL DEFILADE.....	24
1.	Literature on Bureaucracy and Cognition	25
2.	What Does this Mean in the Millennial Battlespace?	26
3.	Case Analysis.....	27
C.	SMALL COORDINATED UNITS.....	30
1.	Literature on Urban Warfare and Force Size.....	30
2.	What Does this Mean in the Millennial Battlespace?	32
D.	SPECIALIZED SOF CYBER.....	37
1.	Literature on Global Communications and Data Processing	37
2.	What Does this Mean in the Millennial Battlespace?	39
3.	Case Analysis.....	40
III.	RECOMMENDATIONS AND CONCLUSION.....	47
A.	TRANSFORMING SOF INFILTRATION.....	47
1.	Training	47
2.	Tactics	49
3.	Technology.....	50
B.	CONCLUSION	52
C.	AREAS OF FUTURE STUDY	53

LIST OF REFERENCES	55
INITIAL DISTRIBUTION LIST	61

LIST OF FIGURES

Figure 1.	Tweets per hour compared to flying training times in Japan on July 26, 2018.....	41
Figure 2.	Tweet examples (descriptive context)	42

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AQ	Al Qaeda
ATP	Army Technique Publication
CBP	U.S. Customs and Border Protection
CCTV	Closed-circuit television
DEA	U.S. Drug Enforcement Agency
FLN	Front Liberation Nationale
GPS	Global Positioning System
IDF	Israeli Defense Force
IED	Improvised Explosive Devices
IO	Information Operations
IRA	Irish Republican Army
ISIS	Islamic State in Iraq and Syria
IT	Information Technology
JP	Joint Publication
LeT	Lashkar-e-Taiba
LRA	Lord's Resistance Army
MILDEC	Military Deception
NPS	Naval Postgraduate School
OPSEC	Operational Security
PIRA	Provisional Irish Republican Army
PSYOP	Psychological Operations

QRF	Quick Reaction Force
RAND	Research and Development Corporation
SEAL	Sea Air Land
SOF	Special Operations Force
TTP	Tactic, Technique, and Procedure
USASOC	United States Army Special Operations Command
USSOCOM	United States Special Operations Command
UW	Unconventional Warfare
WWI	World War I
WWII	World War II

ACKNOWLEDGMENTS

We want to acknowledge and thank our advisors, Dr. Robert Burks and Dr. Michael Freeman, for their advice, guidance, and patience throughout the writing process. They helped us corral our wild visions and scope them into coherent thoughts. Without them, we would still have a pile of body parts instead of Frankenstein's monster.

Thank you to Christine Davis for putting up with the long days in the library and the occasional nights when I had to seclude myself at home. You always understood, and I could not have finished without your support. I also want to acknowledge my father, Tim Davis, for the countless hours you spent reviewing my writing and for having way better grammar than I. You still got it, Pops.

Thanks to Liz Bochner for brainstorming help, and to Eva for enthusiastically attending thesis meetings.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

The special operations community has grown accustomed to having a technological and tactical advantage over its enemies. The majority of special operations missions take place in areas that are either sparsely populated, technologically undeveloped, or both. Remote villages of Afghanistan, Iraq, and other places lacking urban infrastructure and reliable communications capability comprise the majority of locations where special operations missions take place. Correspondingly, tactics, techniques, and procedures (TTPs) leverage superior firepower and speed to overcome the effects of detection during the infiltration stage of operations. As a result, the special operations community is ill-prepared to plan and execute operations in areas where dense populations and high levels of connectivity significantly increase the likelihood and consequences of detection.¹

Recent compromises of special operations missions through ordinary citizens' reports on social media offer a glimpse into what could become the norm. One example includes the unsuccessful top-secret mission to rescue ISIS-held American hostages in 2014 after details leaked out on Syrian social media accounts.² During the mission to capture Osama bin Laden, a neighbor tweeted that he observed helicopters and explosions in his neighborhood, creating a large signature around an operation that may have been undetected otherwise.³ The situation is not likely to improve in favor of special operations forces (SOF). As population density increases and the internet becomes globally accessible within 15 years, these informal detection networks will become pervasive.⁴

¹ Todd South, "The Future Battlefield: Army, Marines Prepare for 'Massive' Fight in Megacities," *Military Times*, March 8, 2018, <https://www.militarytimes.com/news/your-army/2018/03/06/the-future-battlefield-army-marines-prepare-for-massive-fight-in-megacities/>.

² Jacob Siegel, "Could Social Media Blow Special Operations Like the Failed Foley Rescue?," *The Daily Beast*, August 22, 2014, <https://www.thedailybeast.com/could-social-media-blow-special-operations-like-the-failed-foley-rescue>.

³ Siegel.

⁴ Kieren McCarthy, "United Nations Pledges to Get Everyone Online...by 2030," *The Register*, September 8, 2015, https://www.theregister.co.uk/2015/09/08/united_nations_to_get_everyone_online_by_2030/.

By the year 2035 the “millennial generation,” loosely defined as those born between 1981 and 1996, will hold leadership positions within SOF.⁵ In this *millennial battlespace*, SOF will face threats that can potentially compromise even the most carefully planned clandestine operations. These threats have not been present in recent conflicts. Based on current technological trends, the battlefield by 2035 may present instant connectivity of a more populous and urbanized citizenry.⁶ In this scenario, every person could be a potential sensor in a new kind of early warning alert network. In spite of these conditions, it is likely that SOF will still need to conduct clandestine infiltration missions.

The question remains: How should the U.S. Special Operations community conduct SOF infiltration given increased population density and connectivity when potential targets move out of rural terrain by 2035?

1. Traditional SOF Infiltration

According to the *Joint Publication 3-05*, special operations missions are “distributed operations with small operational and logistics footprints far from major bases” which use a “broad array of infiltration, support, and exfiltration techniques to penetrate and return from hostile, denied, or politically and/or diplomatically sensitive areas.”⁷ While traditional SOF infiltration is not specifically defined, we consider it those forms of infiltration that generally utilize a variety of military vehicles, operated in a formation, avoiding population centers, and limited in timeline. Airborne assets such as fixed or rotary wing aircraft are the primary means in which to transport a special operations force but, they may use ground and sea vehicles as well. In all cases, traditional SOF infiltration seeks to move an assaulting force to at the target area within hostile or enemy controlled territory, avoid or delay contact with the enemy, complete the assigned mission, and exfiltrate the territory safely.

⁵ Michael Dimock, “Defining Generations: Where Millennials End and Generation Z Begins,” *Pew Research Center* (blog), accessed May 9, 2019, <https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/>.

⁶ McCarthy, “United Nations Pledges to Get Everyone Online...by 2030.”

⁷ Joint Chiefs of Staff, *Special Operations*, JP 3-05 (Washington, DC: Joint Chiefs of Staff, 2014), I-2.

2. Future SOF Core Tasks

SOF have a variety of mission sets or core tasks. According to the *JP 3-05*, they are “direct action, special reconnaissance, countering weapons of mass destruction, counterterrorism, unconventional warfare (UW), foreign internal defense, security force assistance, hostage rescue and recovery, counterinsurgency, foreign humanitarian assistance, military information support operations, and civil affairs operations.”⁸ The United States Army Special Operations Command’s 2016 “USASOC Strategy—2035” outlines the requirements that Army SOF may face in the future.⁹ Similarly, U.S. Special Operations Command’s “Special Operations Forces Operation Concept: A Whitepaper to Guide Future Special Operations Force Development,” provides insight into potential future mission sets.¹⁰ Each suggests that SOF will retain mission sets that involve moving small units into and out of contested areas in a short amount of time.

After considering the operating environment of the future, in which high population density and connectivity are major environmental factors, we will focus primarily on SOF infiltration for direct-action style raids. These missions may include countering weapons of mass destruction, counterterrorism, and hostage rescues.¹¹ Such operations pose the greatest challenge of moving a force quickly to and from hostile, denied, or diplomatically sensitive areas because they can take place anywhere on the globe and are time sensitive.

3. Why Population Density and Connectivity?

How SOF will operate in the future environment depends on the manner in which planners and leaders think about the problem set today. Two emergent properties of megacities that pose new challenges to SOF infiltration are *population density* and

⁸ Joint Chiefs of Staff, 3.

⁹ United States Army Special Operations Command, “USASOC Strategy—2035,” April 2016.

¹⁰ USSOCOM, “Special Operations Forces Operating Concept: A Whitepaper to Guide Future Special Operations Force Development” (USSOCOM, February 1, 2016).

¹¹ Arthur M Castiglia, “Megacities and the Role of U.S. Special Operations Forces” (Master’s thesis, United States Army War College, 2015), 3.

connectivity.¹² Therefore, our theory for future SOF infiltration and recommendations will address the environments that have both high connectivity and population density.

We use population density as a characteristic based on an analysis of global trends and the prediction that metropolitan areas will expand, eliminating what were formerly sparsely populated areas between cities.¹³ We measure *population density* quantitatively as people per square kilometer based on data from global census databases to provide accurate population densities. We will use the U.S. Census Bureau's delineation between urban and rural—of 1,000 people per square mile or roughly 385 people per square kilometer—to define high and low.¹⁴

We use *connectivity* as an environmental characteristic due to the rapid diffusion of communication technology and the projected expansion of connectivity to all persons by 2030.¹⁵ We measure connectivity as a combination of the number of connected mobile devices per capita and the estimated likelihood of reporting. Likelihood of reporting is a subjective estimation based on the population's reported use of communication technology. We will use the quantitative values of 50 mobile subscriptions per 100 people to delineate between high and low. A city below that value may actually be in the high connectivity region based on the likelihood of reporting of the population. For instance, in 2006 Israel was actively engaged in the Second Lebanon War and Lebanon only had 27 out 100 people with mobile subscriptions; however, the population was highly predisposed to report any infiltration activity by the Israeli Defense Force (IDF).¹⁶ Therefore, the connectivity in this case is high. The overall goal is to characterize the net effect of connectivity in a given operating environment.

¹² Castiglia, 3.

¹³ "Global Trends Home Page," accessed August 6, 2018, <https://www.dni.gov/index.php/global-trends-home>.

¹⁴ Louise La Caille John and Louise Reynnells, "What Is Rural?," United States Department of Agriculture, May 2016, <https://www.nal.usda.gov/ric/what-is-rural#HEALTH>.

¹⁵ McCarthy, "United Nations Pledges to Get Everyone Online...by 2030."

¹⁶ Julia Murphy and Max Roser, "Internet," OurWorldInData.org, 2018, <https://ourworldindata.org/internet>.

B. POPULATION DENSITY

1. Trends

Global urbanization results in three trends which will have an impact on SOF infiltration. First, global urbanization will increasingly concentrate the world's population into not only very large cities but dozens of megacities. Second, ungoverned spaces will exist in megacities in which both state and non-state actors will be able to find security. Third, enemy organizations will migrate out of rural areas to ungoverned urban spaces.

The year 2008 marked the point at which the world's population officially became more urban than rural, and urbanization is expected to continue.¹⁷ By 2050, studies predict that 86 percent of the population in developed countries and 67 percent in less developed countries will live in urban areas.¹⁸ Currently, there are six hundred cities with a population of one million or more, and experts expect that by 2030 there will be 40 cities with a population of 10 million or more. The United Nations defines a megacity as a city with more than 10 million inhabitants; however, not all megacities are the same as each has grown to different sizes at different rates.¹⁹ There are several problems that can potentially plague all megacities. Even the best-governed megacities have the potential for massive poverty and social unrest as a result of social exclusion and informalized processes.²⁰ Additionally, infrastructure problems, transportation congestion, environmental pollution, and increased disease transmission pose a challenge to the central government and the population alike.²¹ Finally, the sheer size of megacities makes likely the existence of

¹⁷ Kees Koonings and Dirk Kruijt, *Megacities: The Politics of Urban Exclusion and Violence in the Global South* (London: Zed Books, 2009), 8.

¹⁸ Koonings and Kruijt, 8.

¹⁹ David Shunk, "Mega Cities, Ungoverned Areas, and the Challenge of Army Urban Combat Operations in 2030–2040," *Small Wars Journal*, January 23, 2014, <http://smallwarsjournal.com/jrnl/art/mega-cities-ungoverned-areas-and-the-challenge-of-army-urban-combat-operations-in-2030-2040>.

²⁰ Koonings and Kruijt, *Megacities: The Politics of Urban Exclusion and Violence in the Global South*, 8.

²¹ Shunk, "Mega Cities, Ungoverned Areas, and the Challenge of Army Urban Combat Operations in 2030–2040."

ungoverned spaces in which criminal organizations and non-state actors may find freedom of movement and a safe haven.

Ungoverned spaces exist all over the world but predominantly in weak states.²² Generally speaking, it is the territory in which a state does not have a monopoly of influence and which subversive or non-state actors may exploit to their advantage. The failure of the government to exert authority leaves a power vacuum and an opportunity for other organizations to take on the role of the state.²³ The prevalence of such spaces is of interest to SOF as the rise of violent criminal extremist organizations, such as ISIS in Syria and the Lord's Resistance Army (LRA) in Uganda, have previously taken advantage of ungoverned spaces to increase their power and influence.²⁴ In the ungoverned spaces of Karachi, Pakistan, rather than attempting to maintain order, the government acts as a mediator over the informal order between the various criminal and terrorist organizations competing for power.²⁵ Likewise, in the Latin American cities of Mexico City, and Sao Paulo, Brazil, where roughly 25 percent of the urban space is characteristically ungoverned, local chiefs and armed organizations execute a parallel law and justice system through the use of force.²⁶ In each ungoverned megacity example, the central government has little to no control over the criminal networks and insurgent groups that spread, compete with one another, and fill the power vacuum.

²² Angel Rabasa et al., *Ungoverned Territories: Understanding and Reducing Terrorism Risks* (Santa Monica, CA: RAND Corporation, 2007), 2–3, <https://www.rand.org/pubs/monographs/MG561.html>. Also available in print form.

²³ Africano Abasa, "Ungoverned Spaces and the Survival of Terrorist Groups in Africa: A Case Study of the Lord's Resistance Army" (Master's thesis, Naval Postgraduate School, 2015), 5, <https://calhoun.nps.edu/handle/10945/47802>.

²⁴ John Campbell, "Terrorists Are Not the Only Ones Exploiting Ungoverned Spaces Across Nigeria," *Council on Foreign Relations* (blog), May 15, 2018, <https://www.cfr.org/blog/terrorists-are-not-only-ones-exploiting-ungoverned-spaces-across-nigeria>.

²⁵ Nazia Hussain and Louise Shelley, "Karachi Organized Crime in a Key Megacity," *Connections* 15, no. 3 (Summer 2016): 8.

²⁶ Koonings and Kruijt, *Megacities: The Politics of Urban Exclusion and Violence in the Global South*, 14.

Rural safe havens are steadily disappearing through a combination of urbanization and counterterrorism efforts.²⁷ Traditionally, safe havens have existed primarily in the remote ungoverned spaces that offer geographic concealment, resources, and the support of a sympathetic population. For many years, al-Qaeda in Afghanistan enjoyed the freedom to hide in the remote terrain and mountain caves, had access to resources through bin Laden and other wealthy contributors, and had the support of the Afghani population. For decades, counterterrorism forces developed tactics and technologies optimized for finding and eliminating terrorist organizations in rural and less populated areas. The same is not true about urban areas. This gap in capability provides an advantage for the enemy.

Enemy organizations need money and resources to sustain the organization let alone expand it. The urban environment offers far greater access to resources than a rural one. Regardless of whether the enemy is a non-state actor or state government, urbanization provides monetary and infrastructure benefits that lend to the greater sustainment and longevity of the organization. Combined with the fact that global urbanization is feeding the growth of megacities, it is inevitable that enemy organizations will move out of the rural areas toward ungoverned urban spaces because these spaces provide concealment from adversaries, access to resources, and a sympathetic population.²⁸

2. Consequences

Conventional military forces have long avoided urban warfare. Fighting in an urban environment typically requires a great deal of manpower and poses numerous command and control challenges, while also resulting in greater collateral damage than rural combat.²⁹ While special operations forces are not concerned with capturing and holding urban terrain for extended periods of time, the characteristics that make conventional urban warfare perilous also constitute challenges to SOF missions.

²⁷ Russell W. Glenn, "Megacities: The Good, the Bad, and the Ugly," *Small Wars Journal*, no. Feb (2016), <http://smallwarsjournal.com/jrnl/art/megacities-the-good-the-bad-and-theugly>.

²⁸ Michael Freeman, "The Sources of Terrorist Financing: Theory and Typology," *Studies in Conflict & Terrorism* 34, no. 6 (2011): 463; 470.

²⁹ Koonings and Kruijt, *Megacities: The Politics of Urban Exclusion and Violence in the Global South*, 118.

The extensive concealment and cover provided by man-made structures in urban terrain make it optimal for the defender and much more difficult for the assaulting force. Locating an individual in a city can be like finding a needle in a haystack. Capturing or eliminating a target is even more difficult. The nature of urban terrain makes a surgical strike with a bomb or limited engagement with special operations forces using current tactics nearly impossible. Any conventional assault in urban terrain inevitably resembles attrition warfare with civilian casualties and escalating violence.³⁰ The physical characteristics of urban terrain allow an enemy organization to exploit both vertical and subterranean spaces, further complicating the assault and dramatically favoring the defender.³¹ Hamas has long used urban terrain to deny the Israeli Defense Force (IDF) from observing and targeting their locations.³² For example, even when the IDF knew the location of Hamas' headquarters was below a hospital in Gaza during 2014 OPERATION PROTECTIVE EDGE, the urban terrain prevented the IDF from successfully eliminating the target.³³ As population densities steadily increase due to urbanization, it will be advantageous for enemy organizations to exploit the natural defenses of urban terrain.

The terrain that makes up urban areas reduces the number of places to land aircraft, restricts movement of forces on the ground and water, and creates canalized areas which the enemy can more easily defend.³⁴ Subterranean tunnels and hidden avenues of escape further complicate the problem for the assaulting force. With limited time to conduct an operation, the infiltrating force using traditional infiltration means must rely on vastly superior firepower or numbers in order to be successful.

Another advantage for the enemy in the urban environment is that there is greater access to people sympathetic to their cause. An enemy organization will be more effective

³⁰ Peter Adey, "Vertical Security in the Megacity: Legibility, Mobility and Aerial Politics," *Theory, Culture & Society* 27, no. 6 (2010): 53; Castiglia, "Megacities and the Role of U.S. Special Operations Forces," 2.

³¹ Glenn, "Megacities: The Good, the Bad, and the Ugly."

³² Glenn.

³³ Glenn.

³⁴ Shunk, "Mega Cities, Ungoverned Areas, and the Challenge of Army Urban Combat Operations in 2030–2040."

at countering infiltration if it has the cooperation of a sympathetic population. They may be sympathetic to the organization's cause or merely willing to accept the social and economic benefits that the organization provides. For example, Hamas in Gaza and Lebanon set up schools, medical clinics and other social services for the civilian population, and they garnered legitimacy and support of the local population.³⁵ As a consequence, the population offers a means of organic early warning and defensive protections from attackers. Whether it be a single city block or an entire city, a sympathetic population helps to maximize the overall security of an enemy organization within an urban environment.

Increasing population density will have a direct effect on traditional SOF infiltration because of the inability to avoid populated areas. Historically, the avoidance of population centers was an essential risk mitigating measure and core tactic for SOF infiltrations. Regardless of whether the infiltration method is by air, land, or sea, in order to be able to arrive at a target area nested within a city, the infiltrating force will have to fly, drive, or sail through a dense population first. There certainly are instances when remaining clear of population centers is unavoidable; however, this practice is deliberately minimized. For many cases, SOF would rather abort the mission than accept the risk.

In a high population density environment, detection is essentially inevitable and, assuming that the population is sympathetic to the enemy, the infiltrating force will be at higher risk of being attacked before arriving at the target area. Additionally, an early warning from the population means little or no time on the target area before the enemy will respond. Avoiding population centers in the future will likely be impossible during SOF infiltration.

The Battle of Mogadishu in 1993 is an excellent demonstration of the challenges of high population density environment for traditional SOF infiltration. Despite superior firepower and numbers, the enemy response left eighteen dead and eighty-four wounded.³⁶

³⁵ Freeman, "The Sources of Terrorist Financing: Theory and Typology," 471.

³⁶ Shunk, "Mega Cities, Ungoverned Areas, and the Challenge of Army Urban Combat Operations in 2030–2040."

Currently, SOF forces rarely conduct an urban infiltration for these reasons; else they may encounter the same disastrous consequence. Unfortunately, these issues will be unavoidable and will likely be magnified in the future battlespace, so it is crucial that SOF planners find ways to address these issues.

C. CONNECTIVITY

1. Trends

Throughout successive periods of conflict, communication technology gives the offensive and defensive actors an advantage. Analyzing the historical relationship between communications technology and challenges to infiltration or counter-infiltration will help us identify how emerging technology will affect future SOF infiltration.

Considering the trajectory of communication technology over the last 140 years, we identify two overarching trends: First, communication is becoming faster, cheaper, more data intensive, and makes information easier to disseminate.³⁷ Second, a state or non-state organization with sufficient resources can exploit the massive amount of communications data generated by individual citizens for their own benefit.

Developments in communication technologies create opportunities and vulnerabilities for both an attacker and a defender. Because one of our goals is to suggest ways in which SOF, the offensive actor, can overcome the defensive communication technologies of future adversaries, it is valuable to consider how advancements in communications technology throughout history have affected both those staging attacks and those defending against them.

While it may seem more relevant to analyze the role of communication technology strictly in historical SOF operations, there are several advantages to studying terrorist attacks instead. First, the terrorist actions have the most significant effect when conducted in population centers, where population density is highest. Second, the operational unit size of terrorist attacks bears similarity to contemporary SOF operational unit sizes. Third,

³⁷ Christopher H. Sterling, *Military Communications from Ancient Times to the 21st Century* (Santa Barbara, CA: ABC-CLIO, 2008).

terrorist actions do not necessarily take place in entirely hostile environments, which is analogous to SOF operations into neutral and densely populated areas.

Using the periods proposed in David Rapoport's "Four Waves of Terrorism," we examine how offensive and defensive capabilities fluctuated with advances in communications technology.³⁸ David Rapoport suggests that terrorism has existed in four waves, each occupying a specific time-period. A particular wave, he argues, is exemplified by groups sharing ideology and tactics. The First Wave, defined by anarchism, lasted from around the 1880s to the 1920s. Anti-colonial terrorist groups pervaded from the conclusion of WWI through the 1960s, making up the Second Wave. The Third Wave consisted of what Rapoport termed "The New Left" and lasted from the 1960s into the 1990s. Finally, the Fourth Wave, characterized by religious zealotry, began with the 1979 Iranian Revolution and persists today.³⁹ With successive waves, advances in communication technology resulted in variations in the tactics, organization, and vulnerabilities of terrorist groups and those defending against them. The following groups and their respective counterterrorist adversaries serve to provide insight into the relationship of communication technology to terrorism over time: Narodnaya Volya and the Russian government, the Algerian Front Liberation Nationale (FLN) and the French government, the IRA (Irish Republican Army) and the British government, and Al Qaeda (AQ) and the U.S.-led Coalition.

One of the earliest established terrorist organizations during the First Wave was the Russian anarchist group, "The People's Will," also known as Narodnaya Volya, which holds the credit of being the "first organization in history dedicated to systematic political terrorism."⁴⁰ At the time of Narodnaya Volya's emergence in 1879, the technology of "electrotyping" and the telegraph impacted both the group's ability to spread its beliefs and coordinate attacks. Electrotyping, created in 1839 by a German inventor temporarily living

³⁸ Audrey Kurth Cronin and James M. Ludes, *Attacking Terrorism: Elements of a Grand Strategy* (Washington, DC: Georgetown University Press, 2004).

³⁹ Cronin and Ludes.

⁴⁰ Richard Pipes, *The Degaev Affair: Terror and Treason in Tsarist Russia* (New Haven, CT: Yale University Press, 2003), 10.

in Russia, made the duplication of metal printing plates faster and more accurate than the previous method.⁴¹ The technology made it viable for Narodnaya Volya to disseminate its underground newspaper, “The People’s Gazette,” which spread the group’s anti-autocratic message. Additionally, the introduction of the telegraph to Russia allowed Narodnaya Volya to coordinate its unprecedented 1879 train bombing over vast distances. In preparation for the group’s 1879 attack on Tsar Alexander II’s train, informants for Narodnaya Volya reportedly telegraphed coded details about the Tsar’s train schedule to fellow terrorists in Moscow.⁴²

Both the telegraph and electrotyping technologies allowed Narodnaya Volya to communicate beyond the restrictions of physical meetings and overcome geographic dispersion when conducting attacks. As early as the 1870s, the paradox of technology as both a force of peace and an enabler of terrorism was evident. No longer was it necessary to have a massive army to conduct significant acts of violence; the ability to communicate widely and in real-time was critical to this change.

Telegraph and electrotyping had a force multiplying effect on Russian revolutionaries, but did little for the Tsarist counterterrorism forces. Tsar Alexander II’s Secret Police, tasked with countering revolutionary assassins and terrorists, was known as the “Third Section.”⁴³ With assassination attempts increasing in the 1870s, an investigation into the Third Section in 1880 found the organization grossly lacking in its ability to coordinate between geographically and bureaucratically dispersed offices. Administrative records of political exiles and terrorist suspects were disorganized and not shared among counter-terrorism units. As a result, Narodnaya Volya members and others frequently moved around the country with impunity and escaped police surveillance when it was present.⁴⁴ The electrotypes and telegraph may have been quite beneficial to revolutionary

⁴¹ Harris Hatch and Stewart Alexander, *Electrotyping and Stereotyping* (Chicago: United Typothetae of America, 1918): 4.

⁴² Frithjof Benjamin Schenk, “Attacking the Empire’s Achilles Heels: Railroads and Terrorism in Tsarist Russia,” *Jahrbucher Fur Geschichte Osteuropas* 58 (2010): 232–53: 237.

⁴³ Richard Deacon, *A History of the Russian Secret Service* (New York: Taplinger Pub. Co., 1972).

⁴⁴ Richard Deacon, *A History of the Russian Secret Service* (New York: Taplinger Pub. Co., 1972): 65.

groups trying to spread their message and conduct point-to-point attack coordination, yet it did little to assist the Tsarist forces from coordinating their security efforts on the massive scale required.

The net effect of communication technology during this First Wave favored the small unit attacker. Given the high cost of transmitting each package of information from one point to another high, the defender was unable to share the necessary amount of data to keep a dispersed network of security offices informed of suspected individuals and head-off potential attacks.

A terrorist group representative of the Second Wave is Le Front de Liberation Nationale (FLN) in Algeria, formed in November 1954 to oppose French colonial rule.⁴⁵ A critical military technological development during the Second Wave (1920s-1960s) was the radio. Advancements with the use of quartz as a frequency controller allowed for the installation of radios in mobile air and ground platforms, where previously radios were strictly stationary.⁴⁶ Radios, which were becoming increasingly mobile and capable, were the primary means of communication between geographically dispersed forces during WWII.⁴⁷ The portable radio was a vital tool in the French military's fight against the FLN.

The French military's strategy to counter the FLN relied on accurate intelligence and the ability to quickly disseminate enemy locations to tactical units. France's use of helicopters, aerial surveillance, and an "abundance of radio equipment," allowed them maximum mobility and flexibility, which denied the FLN freedom of movement to coordinate attacks.⁴⁸

While the fight to establish Algerian independence from France included non-terrorist efforts, the terrorist component of the FLN remained active throughout, despite significant setbacks. Under the tactically effective opposition of the French military

⁴⁵ Henry F. Jackson, *The FLN in Algeria: Party Development in a Revolutionary Society*, Contributions in Afro-American and African Studies ; No. 30 (Westport, Conn: Greenwood Press, 1977).

⁴⁶ Sterling, *Military Communications from Ancient Times to the 21st Century*.

⁴⁷ *Military Communications from Ancient Times to the 21st Century*: 373.

⁴⁸ Constantin Melnik, "The French Campaign Against the FLN" (Santa Monica, CA: RAND Corporation, 1967).

enabled by their synchronization of radio communication and mobility, communication among FLN members was difficult and entailed high risk. As such, the FLN relied heavily on children as messengers and women as combatants.⁴⁹ With intense pressure on the FLN organization, its members were forced to meet in person to coordinate attacks, establish a strategy, and nominate leaders. As a result, the FLN adopted an organization that was a combination of a hierarchy and the star/hub model, which is a structure that suits environments in which communication is costly.⁵⁰

The FLN and other anti-colonial terrorist groups seem to be the victims rather than beneficiaries of technological advances. Narodnaya Volya capitalized on developments in printing and the telegraph to gain the upper hand on the state. For the FLN, on the other hand, the French military's effective use of technology forced the terrorists to use costly, inefficient means of communication. There were many factors that contributed to the FLN's inability to progress beyond a terrorist group into a legitimate military. Significantly, physical barriers like the Meurice-Challe Line, which physically isolated FLN fighters in neighboring Tunisia and Morocco, was an effective impediment to communication.⁵¹

The Provisional Irish Republican Army (PIRA) was prominent during the Third Wave, despite the fact that it shared ideology with earlier, Second Wave, groups. The PIRA was an anti-colonial terrorist group rather than "New Left" like other Third Wave groups. Forming out of a split with the Official IRA in 1970, the PIRA became the more violent, less political, of the groups that posed a security threat to Britain.⁵² The PIRA employed car bombs and Improvised Explosive Devices (IEDs) frequently in its campaign of

⁴⁹ Jackson, *The FLN in Algeria: Party Development in a Revolutionary Society*.

⁵⁰ "The *hub*, star, or wheel network, as in a franchise or a cartel where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other." Quoted in: John. Arquilla and David F. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, MR / Rand Corporation; MR-1382-OSD (Santa Monica, CA: Rand, 2001).

⁵¹ Jackson, *The FLN in Algeria: Party Development in a Revolutionary Society*.

⁵² James. Dingley, *Combating Terrorism in Northern Ireland*, Cass Series on Political Violence (London: Routledge, 2009).

violence. A particular spike in attacks famously occurred on “Bloody Friday,” during which the PIRA detonated 22 IEDs within two hours.⁵³

Communication technology available to the PIRA was significantly more advanced than that available to terrorist groups of the Second Wave. The PIRA still had to primarily use point-to-point communication rather than the network structure seen in the Fourth Wave. Telephones allowed the PIRA to be geographically dispersed across Northern Ireland and the globe while maintaining overall control through its hierarchical structure.⁵⁴

The effect of communication technology on the PIRA’s tactics and organization demonstrates the trend that as communication becomes cheaper and more accessible, attacks become more complex, and the organization can become more dispersed. In their study on network connections within the PIRA, Paul Gill et al. conclude that tactics which involve greater transfers of knowledge, synchronization, and levels of complexity demand a higher degree of interconnectivity and communication.⁵⁵ Such tactics include IED emplacement and simultaneous vehicle bombs. The increases in communication among PIRA members was possible only with innovations such as the telephone.

Technologically, the Fourth Wave of Terrorism represents a departure from the previous three waves. The global spread of Information Technology (IT) negates many of the challenges that groups like Narodnaya Volya, the FLN, and the IRA faced when trying to communicate internally. While those groups relied heavily on personal meetings and point-to-point messaging, modern groups like Al Qaeda have access to cheap and difficult to intercept communication methods that can reach many nodes for no additional cost. Technologies including cellular phones, fax machines, electronic mail, websites, and

⁵³ Paul Gill et al., “Lethal Connections: The Determinants of Network Connections in the Provisional Irish Republican Army, 1970–1998,” *International Interactions: Empirical and Theoretical Research in International Relations*, 2014.

⁵⁴ Sean Boyne, “Uncovering the Irish Republican Army,” News, PBS Online, August 1, 1996, <https://www.pbs.org/wgbh/pages/frontline/shows/ira/inside/org.html>.

⁵⁵ Gill et al., “Lethal Connections: The Determinants of Network Connections in the Provisional Irish Republican Army, 1970–1998.” 73.

computer conferencing led to a massive reduction in cost and effort required to communicate and facilitates a different organizational structure altogether, the network.⁵⁶

In their book *Networks and Netwars*, Dr. Arquilla and Dr. Ronfeldt discuss the impacts of the information revolution on non-state actors. Describing the relationship of communication technology to organizational structure, they argue:

“Of the three network types, the all-channel has been the most difficult to organize and sustain, partly because it may require dense communications. But it is the type that gives the network form its new, high potential for collaborative undertakings and that is gaining new strength from the information revolution.”⁵⁷

AQ is a Fourth Wave terrorist group that made use of these new IT capabilities and demonstrates what is possible using the “all-channel” network. Osama bin Laden reportedly had a contemporary suite of IT equipment at his rural headquarters in Afghanistan from which he directed the globally dispersed network of AQ affiliates and cells in the 1990s.⁵⁸ AQ and other Fourth Wave groups are known to have used floppy discs and compact discs to transmit large files on bomb-making instructions, recruiting material, and tactics.⁵⁹ While the telephone did allow real-time coordination and geographic dispersion for Third Wave groups, transfers of large amounts of data only became possible during the Fourth Wave.

With counterterrorist forces having access to the same, if not superior, IT capabilities as terrorists, the contest over who benefits more comes down to organizational limitations. The technology which enables a dispersed network structure is useful only if tactical decision-making authority rests at lower levels. The dispersed structure of terrorist organizations requires less hierarchical communication as cells execute pre-planned attacks, which leverages the capabilities of IT well. Counterterrorism forces like the U.S. military, on the other hand, are organized into hierarchies intended to fight a centralized

⁵⁶ Arquilla and Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*.

⁵⁷ Arquilla and Ronfeldt, 8.

⁵⁸ Arquilla and Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*.

⁵⁹ Arquilla and Ronfeldt, 36.

enemy like the Soviet Union.⁶⁰ Therefore, recent developments in communication technology favor the flexible and dispersed small-unit attacker over a hierarchically structured defender.

In recent years, computing technology enabled a new defensive capability to enter the arena. In its effort to control unrest in the remote Xinjiang Province, the Chinese government implemented regulations which force the transmission of all personal communications between its citizens through data processing hubs.⁶¹ From this aggregated data, computers employing Artificial Intelligence (AI) can rapidly identify potential security threats within the population. Consequently, we conclude that just as individual communication capability increases, the capacity of centralized entities to effectively monitor interpersonal communication will also expand.

2. Consequences

Based on trends in communication, advantages and disadvantages emerge for both the defender and attacker (infiltrator). Due to a higher number of communication devices, combined with increased data collection and processing power, the defender will be able to identify security threats much more rapidly than we have seen throughout history. Additionally, because of the potential for AI empowered computers to associate social media communications with geographic locations, the defender's response time to threats will significantly decrease.

While increased technological capability will aide both the infiltrator and defender, each will be vulnerable to attacks against its respective IT networks. For the infiltrator relying on advanced communication within the unit and back to headquarters, this vulnerability would take the form of communication disruption by the defender, cutting the unit off from required supporting assets and inhibiting internal synchronization. The

⁶⁰ Sterling, *Military Communications from Ancient Times to the 21st Century*.

⁶¹ Jerome Doyon, "Counter-Extremism' in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics," *War on the Rocks*, January 14, 2019, <https://warontherocks.com/2019/01/counter-extremism-in-xinjiang-understanding-chinas-community-focused-counter-terrorism-tactics/>.

defender will similarly be susceptible to cyber-attacks against its alert networks, which could create blind spots through which a SOF unit could infiltrate.

With more effective alert networks and precise locating of infiltrating forces, the likelihood that a SOF unit would arrive on target with enough time to conduct its operation before an enemy reaction force contacts them would significantly decrease. On the other hand, the need for an infiltrating force to move in a formation, whether by aircraft, ground vehicles, or maritime vessels, will diminish as technology allows units to disperse, infiltrate, then concentrate at a specific location and time.

As communication technology improves, situational awareness of the infiltrating unit will also increase, enabling increasingly complex tactics. Just as the telegraph allowed “The Peoples’ Will” to synchronize attacks across vast distances, improvements in communication technology will facilitate SOF infiltration that requires more complex timing and spatial orientation. Infiltrating units will no longer need to be within physical proximity to maintain situational awareness and synchronize their arrival on target. With this capability, a 16-man unit could split its force into smaller, less detectable elements, each using different modes of travel during infiltration but concentrating on the target location with precise timing.

As both offensive and defensive actors place more reliance on IT systems, the infiltrating unit must be prepared to leverage these advanced capabilities when they are available, but also to operate in a communication-denied environment. Some of the advanced technologies that facilitate complex infiltration tactics also represent a vulnerability which the defender can target. This aspect of the future operating environment differs significantly from that of the last decades, in which SOF maintained overwhelming technological superiority over its enemies. In the future, SOF will find its technologies equaled and sometimes surpassed by the enemy’s. Therefore, SOF must possess a range of infiltration practices that can achieve success while wielding superior technology but also minimize risk when faced with it.

II. THEORY OF FUTURE SOF INFILTRATION

In the previous chapter, we presented two trends that will likely shape the future battlespace and impact how special operations forces will have to conduct infiltrations. *Population density* and *connectivity* trends foretell that highly connected megacities will be where the enemy finds a safe haven and where SOF must learn to infiltrate. In this chapter, we will present our theory of what the future of SOF infiltration will likely need to embody. The basis for this theory has foundation in concepts found in literature and supported by both historical and current cases. While not all encompassing, the theory instead encapsulates four critical areas where we observe that traditional SOF infiltration needs reform and innovation. Our theory is that deception will be more important than stealth technology, cognitive defilade will be more effective than physical defilade, the unit size must reduce to smaller coordinated elements, and organic SOF cyber capability will be as vital as physical actions for infiltration in the millennial battlespace environment.⁶²

A. DECEPTION VS. STEALTH

In the high population density, highly connected environment of the future, remaining unseen during infiltration will be nearly impossible. Stealth technology, which renders a vehicle invisible to RADAR sensors, does not conceal it from millions of passive observers in a megacity. Therefore, with the understanding that detection is likely, achieving stealth becomes less possible and less relevant; SOF must craft infiltration platforms and tactics to achieve deception instead.

⁶² “Defilade”- 1. Protection from hostile observation and fire provided by an obstacle such as a hill, ridge, or bank. Quoted in Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Defense Technical Information Center, 2019).

1. Literature on Deception

Military theorists throughout history have examined deception from debating its relevancy to analyzing how a successful deception functions.⁶³ Even in the era of medieval warfare, scholars emphasized the centrality of deception to a battle plan. Specifically, they declared the importance of signaling to the enemy the opposite of what was the reality with regards to one's own forces.⁶⁴ Moving beyond the question of deception's relevance in warfare, an examination of how to employ deception with the greatest chance of success suggests that a particular deception should amplify the enemy's preconceived notions rather than challenge them. Thus, a deception effort builds credibility among the enemy based on biases and oversights they already possessed.⁶⁵ Rothstein and Whaley further this concept by dividing deception into two components: dissimulation, or hiding what is true, and simulation, which is the affirmation of what is false.⁶⁶

While some modern warfighters hold the perception that deception is a "weapon of the weak," this idea is especially misguided when it comes to special operations.⁶⁷ Describing the importance of the principle of *Surprise* in special operations, William McRaven suggests that the role of deception is to delay the enemy's response to the SOF unit, thereby allowing the SOF unit to surprise the enemy and achieve relative

⁶³ Sunzi, *The Art of War*, UNESCO Collection of Representative Works: Chinese Series (London: Oxford University Press, 1963); Hy S. Rothstein, *The Art and Science of Military Deception* (London: Artech House, 2013); James F. Dunnigan, *Victory and Deceit: Dirty Tricks at War*, 1st ed. (New York: W. Morrow, 1995).

⁶⁴ Sun Tzu discusses deception in *The Art of War*. He states: "All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near." Quoted in Sunzi. *The Art of War*. UNESCO Collection of Representative Works: Chinese Series. London: Oxford University Press, 1963.

⁶⁵ In their work, "Multidisciplinary Perspectives on Military Deception," Katherine Herbig and Donald Daniel reach a single overwhelming conclusion: "It is far easier to lead a target astray by reinforcing the target's existing beliefs, thus causing the target to ignore the contrary evidence of one's true intent, than it is to persuade a target to change his or her mind." Donald C. Daniel et al., "Multidisciplinary Perspectives on Military Deception," Technical Report (Monterey, CA: Naval Postgraduate School, 1980), 60.

⁶⁶ Hy S. Rothstein, *The Art and Science of Military Deception* (London: Artech House, 2013): 20.

⁶⁷ Dunnigan, *Victory and Deceit: Dirty Tricks at War*.

superiority.⁶⁸ Considering the fact that the U.S. Department of Defense publishes its Joint Publication on the principles of deception, it is evident that deception is still considered a central component of warfare. The vague nature of the principles outlined in official military instructions, however, leads us to conclude that there is a substantial gap in knowledge of what deception looks like in the current and future SOF operating environment.⁶⁹

2. What Does this Mean in the Millennial Battlespace?

Considering what theorists and military experts have said about deception on current and past battlefields, let us contemplate what it will mean in the millennial battlespace. Deceptions will need to not only delay the enemy's discovery of the assault force, but hide the fact that there is an assault force at all.

A key consideration when executing a deception effort in the millennial battlespace is the fact that the assault force will be near the civilian populace throughout the infiltration. Therefore, we need to accept and embrace the fact that the population will see the force. For the same reason that this dense population makes remaining unseen difficult, it provides an opportunity to SOF; there is indigenous activity within which to hide. The right deception plan allows a small SOF team to blend more easily into the crowded and noisy megacity environment compared to a barren desert.

To enact effective deceptions, we must analyze the future environment and predict what the enemy and civilian populace expects to see. In a megacity, they will likely expect to see heavy commercial traffic to include sea, air, and land modes of transport. The enemy security forces will expect to see the vehicles and personnel that accompany such commerce. A proper deception for infiltration in the future environment need only confirm this expectation by mimicking the pattern of life of the local populous.

⁶⁸ In his compilation of historical case studies, *Spec Ops*, William McRaven offers six principles of special operations: Purpose, Simplicity, Speed, Security, Repetition, and Surprise. He writes, "Deception when it works, either directs the enemy's attention away from the attacking force or delays his response long enough for surprise to be gained at the crucial moment." Quoted in William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice* (Novato, CA: Presidio, 1995).

⁶⁹ Joint Chiefs of Staff, *Special Operations*, II-3.

3. Case Analysis

On the night of November 23, 2008, ten Lashkar-e-Taiba (LeT) terrorists and their handlers boarded a rented vessel in Karachi, Pakistan, and began their journey toward Mumbai. After entering Indian territorial waters, they seized an Indian fishing vessel, the *MV Kuber*, and transferred the ten attackers to the hijacked ship while moving the *Kuber's* crew, except its captain, to their rented vessel. Forcing the captain's cooperation, the *Kuber* then made the 550 nautical mile trip back toward Mumbai. Four miles outside Mumbai, the terrorist killed the *Kuber's* captain and deployed their inflatable dinghy. After abandoning the *Kuber* under cover of darkness on 26 November, the ten terrorists transited to the Badhwar Park Jetty in Mumbai, where four of five two-man teams went ashore. The remaining team used the dinghy to approach their first target from the water. Once ashore, the pairs used local taxis to move to their primary targets.⁷⁰

Until they drew their weapons at the first set of targets, the LeT attackers remained unnoticed. Starting at the port of Karachi, they had clandestinely transited roughly 600 miles and infiltrated the densely populated, urban center of Mumbai. After indiscriminately killing and wounding scores of people during three near-simultaneous attacks at a train station, a café, and the famous Taj Mahal Hotel, the attackers were able to move to additional targets. Sieges ensued at a Jewish center, the Trident-Oberoi Hotel, and the Taj Mahal Hotel, with the terrorists taking hostages and barricading themselves within the respective structures while Indian security forces responded. For nearly three days, Indian security forces struggled to apprehend the ten LeT attackers. With no exfiltration plan, the terrorists eventually followed through on their intended "martyrdom." The security forces killed all but one by the end of the day on November 29th.⁷¹

Mumbai is a high population density environment. Based on censuses in 2001 and 2011, the population in 2008 was approximately 3.2 million. This population is spread over 157 square kilometers, giving Mumbai a very high population density of 20,400 people per

⁷⁰ Stephen Tankel, *Storming the World Stage: The Story of Lashkar-e-Taiba* (Oxford: Oxford University Press, 2013).

⁷¹ Tankel: 219.

square kilometer.⁷² For comparison, the population density of New York City, New York, was reported at 11,000 people per square kilometer in 2019.⁷³ Of note, Mumbai is listed among the top ten most densely populated cities in the world.⁷⁴

Mumbai residents had recent exposure to anti-Indian terrorists. Just two years prior, in 2006, LeT members placed bombs on Mumbai commuter trains, killing more than 180 people. Therefore, we can presume that Mumbai residents would be unlikely to ignore evidence of an imminent or ongoing attack and would consequently alert authorities and other civilians with any mobile devices they had available. Despite a relatively low per capita number of mobile subscriptions (29 per 100 people), Twitter reported that during the attack there were 70 tweets every five seconds describing the events.⁷⁵ Therefore, we assess a very high likelihood of reporting, which compensates for the lower number of devices. Thus, Mumbai was a high population density and high connectivity environment.

LeT used multiple physical deceptions throughout their infiltration in order to blend into the Mumbai pattern of life. The first level was their use of the *MV Kuber*, a Mumbai based vessel with its original captain piloting it. To pass a potential secondary inspection by Indian navy or coast guard, the attackers had fake Indian ID cards, had taken Hindi language lessons, and even wore the symbolic thread around their wrists common among Hindus.⁷⁶

Not only is Mumbai densely populated on land, but everything from container ships to a vast fleet of small fishing boats crowd its harbor. LeT's use of both a fishing boat to make the long transit from Karachi to Mumbai and the insertion via dinghy took maximum

⁷² "City Population—Population Statistics in Maps and Charts for Cities, Agglomerations and Administrative Divisions of All Countries of the World." Accessed December 2, 2018. <https://www.citypopulation.de/>.

⁷³ "U.S. City Populations 2019," accessed April 29, 2019, <http://worldpopulationreview.com/us-cities/>.

⁷⁴ "The World's Most Densely Populated Cities," WorldAtlas, accessed May 9, 2019, <https://www.worldatlas.com/articles/the-world-s-most-densely-populated-cities.html>.

⁷⁵ Claudine Beaumont, "Mumbai Attacks: Twitter and Flickr Used to Break News," November 27, 2008, sec. World, <https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html>; Murphy and Roser, "Internet."

⁷⁶ Tankel, *Storming the World Stage : The Story of Lashkar-e-Taiba: 209*.

advantage of this difficult-to-police domain. Maritime patrolling is a resource-demanding task. Maharashtra State, which governs Mumbai, had turned down an additional 26 patrol craft from the Indian government because the state could not afford to maintain them.⁷⁷ Additionally, the use of local taxis to approach their initial targets enabled the attackers to remain unnoticed despite being in an urban metropolis.

One could argue that the operation was unsuccessful because the terrorists were eventually all killed or captured. Debriefs with the sole surviving attacker, David Headley (born Daood Gilani), however, indicate that the operation's planners initially contemplated having an exfiltration plan but shifted to an intentional "martyrdom" operation to garner more public attention.⁷⁸ Had the attackers only struck their initial three targets of the train station, café, and Taj Mahal Hotel then commenced an exfiltration, it is imaginable that they could have escaped death or capture. Instead, they deliberately hunkered down and awaited the slow response of India's security forces.

LeT's 2008 attack on Mumbai presents a valuable case of a small unit successfully infiltrating a densely populated environment undetected through the use of several deceptions. Physical disguise and indigenous vehicles constituted multiple layers of deception that allowed the LeT attackers to transit through the high population density and high connectivity environment of Mumbai. Acknowledging that contact with the population was certain, LeT prioritized deception over stealth with great effect.

B. COGNITIVE VS. PHYSICAL DEFILADE

In the rural environment, infiltration routes use physical defilade provided by natural features to mask the sight, sound, and electronic signature of SOF units. Though these routes do not exist in the same manner in the millennial battlespace, new defensive vulnerabilities arise that SOF can exploit, which constitute *cognitive defilade*. The

⁷⁷ Ayesha. Jalal, *Partisans of Allah: Jihad in South Asia* (Cambridge, Mass: Harvard University Press, 2008), 25.

⁷⁸ Taniel, *Storming the World Stage: The Story of Lashkar-e-Taiba*, 228.

complexities of a megacity demand the existence of governing bureaucracies that can provide general services and security to the population. Even so-called ungoverned spaces may have an informal governing body. These bureaucracies may be state or non-state actors with legal or illegal authorities, yet they play a role in the security. Vulnerabilities of security bureaucracies like shortfalls of imagination and failures to cooperate between jurisdictions will likely result in physical avenues of approach that SOF can utilize.

1. Literature on Bureaucracy and Cognition

A core competency of a successful military commander is the ability to withhold from the opponent the precise location of an attack, thereby forcing the opponent to disperse its defensive forces.⁷⁹ Considering the nature of the high population density, high connectivity future operating environment, we find that this principle of warfare will only become more relevant. For instance, when attacks can come from the maritime, ground, aerial, space, and cyber domains, the defender will have to allocate finite defensive resources across this broad spectrum of vulnerabilities.

As these potential points of vulnerability multiply in the future, the bureaucratic structure of security organizations will likely prove to be incapable of preparing for innovative and previously unused methods of infiltration. A bureaucracy, when functioning properly, excels at executing routine protocols based on procedure, individual expertise, and formal responsibility. The same reasons a bureaucracy follows established procedures well, make the bureaucracy generally very poor at innovation and imagination.⁸⁰ When it comes to future SOF infiltration, this weakness of security bureaucracies to imagine their own vulnerabilities offers an advantage to the infiltrating force.

There is a vulnerability of security bureaucracies that is not universally true, but bears consideration when assessing infiltration routes and tactics: specifically, the geographical borders dictating where one security force's jurisdiction stops and another's begins. In his study on the potential cooperation between terrorist groups and international

⁷⁹ Sunzi, *The Art of War*.

⁸⁰ Philip D. Bougen and Pat O'Malley, "Bureaucracy, Imagination and U.S. Domestic Security Policy," *Security Journal* 22, no. 2 (2009): 101, <https://doi.org/10.1057/palgrave.sj.8350078>.

organized criminal groups, Gernot Morbach identifies some of the reasons why the international community struggles to apprehend transnational criminals. Specifically, he argues that states consistently want to fight crime under their own laws, and therefore are biased against international cooperation. As a result, international crime goes unpunished in exchange for states maintaining their desired law enforcement sovereignty.⁸¹ This pattern serves as an example of how crowding of the security domain, as one would likely see in the future operating environment, can result in an opportunity for the infiltrating force. The study of how jurisdictions impact security operations typically relates to countering organized crime and terrorism, but it offers a fresh perspective on how an infiltrating force can leverage cognitive defilade to achieve its goals. The same reluctance of security forces to cooperate at the international level is possible at provincial and regional levels, as evidenced by the second case study in this section.

2. What Does this Mean in the Millennial Battlespace?

Security forces operate under some form of bureaucracy. Bureaucracies are good at dealing with the expected.⁸² Natural disasters and terrorist attacks have shown us that bureaucracies are terrible at dealing with the unexpected.⁸³ What this means for an enemy defensive system is that in the future, military defenses against SOF infiltration will be geared to counter the most likely traditional infiltration methods. After all, every potential adversary is limited to some extent by resources and must, therefore, accept compromises in certain areas to bolster others. Consequently, we should recognize what these expected deterrents to infiltration are and then alter our methods accordingly.

Much can be learned about defeating a security bureaucracy by understanding the tactics of high-value heists, drug traffickers, and terrorists. Each of these criminal types must rapidly adapt to capable and well-funded adversaries in harsh, unforgiving

⁸¹ Gernot W. Morbach, "Terrorism and Organized Crime: The Alliance of Tomorrow? How to Counter a Possible Future Threat." (Master's thesis, Naval Postgraduate School, 1998).

⁸² Bougen and O'Malley, "Bureaucracy, Imagination and U.S. Domestic Security Policy."

⁸³ Bougen and O'Malley.

environments. Successful criminals know how to identify the vulnerable points in what may, at first consideration, appear to be a thorough defense.

3. Case Analysis

We will analyze three cases that illuminate aspects of our theory. A helpful lens through which to consider the security vulnerabilities stemming from cognitive oversight and bureaucratic shortfalls is the way in which thieves operate. Thieves intending to steal high-value prizes are up against robust security countermeasures. Modern perpetrators of bank and jewelry heists face advanced alarm systems, reinforced buildings or vehicles, short police response times, and the fact that so many methods of entry have been tried and are well defended. As a result, to succeed, thieves must strive to use “outside the box” thinking to achieve their end goal. An excellent example of creative thinking to overcome bureaucratic constraints and cognitive oversight is the 2009 robbery of the G4S Cash Depot in Sweden. An account of the heist follows:

“At 5:15 AM on September 23, 2009, four thieves landed a stolen Bell 206 Jet Ranger helicopter on the roof of the G4S Cash Depot in Västberga, Sweden. Breaking into the depot through a large pyramid-shaped skylight, the thieves descended via custom-length ladders to the depot’s counting room. Breaking through the door using custom-fit explosives, the thieves opened the depot’s cash cages with the assistance of a circulating saw. Twenty minutes after they landed, the thieves ascended to the roof and took off with \$6.1 million (FY12) in cash. Thanks to a tip-off from the Serbian foreign ministry, Swedish police had been expecting a helicopter assault on a large cash depot in September, but they were not expecting that the thieves would actively hinder a police response by spreading caltrops across roads near the depot and placing packages resembling bombs outside the police heliport.”⁸⁴

The G4S robbery highlights a number of the concepts contained in our theory of future SOF infiltration. First, their use of a helicopter for a vertical approach to the bank demonstrates a *cognitive shortfall* by the bank’s security team, which had fortified ground level entrances but had not conceived of an airborne entry into the vault. Secondly, the thieves played off *bureaucratic protocols* of the responding security units by placing fake

⁸⁴ Jarret Lafleur et al., “The Perfect Heist: Recipes from Around the World” (Albuquerque, NM: Sandia National Laboratories, March 2015).

bombs on the building's roof. As members of a protocol driven organization, the Swedish police were forced to stop and deal with the potential bombs before pursuing the criminals. Lastly, while the Swedish police did receive the tip-off from the Serbian government, it occurred just before the robbery and left little time for the Swedes to emplace defensive measures. As such, it demonstrates how the thieves benefited from the *bureaucratic delay* between the two governments' security organizations.

We propose that the problem-solving approach used by the thieves is one that SOF planners might benefit from when infiltrating the millennial battlespace. The thieves' recognition of both the physical vulnerability of the bank's rooftop paired with the fact that information transmission from the Serbian to Swedish government would have some sort of delay and distortion would aide SOF in successfully infiltrating a high population density, highly connected future environment.

During a deployment to the U.S. Central Command in 2017, this thesis' author observed that Islamic State in Iraq and Syria (ISIS) supply routes and bases of operations frequently lay along national and provincial borders. After further investigation, it appeared that the local military commanders assigned to secure their respective provinces were extremely reluctant to conduct operations near the borders of their jurisdictions. This tendency was due to the fact that the commanders had finite resources, and if the enemy was located on the border of their jurisdiction and another commander's, they would much rather the other expend his resources to solve the problem. As a result, often neither would launch operations along these jurisdictional borders and the enemy's activities would continue unhindered. The fact that ISIS' final major territorial strongholds were on the border of Iraq and Syria in the city of Baghouz, Syria, suggests that this pattern can exist at an international level as well.⁸⁵

It is not the case that jurisdictional borders are entirely open for infiltration. However, we propose that there is an incentive for those in charge of securing the areas on either side to withhold from responding to threats in the hopes that the other commander

⁸⁵ "Coalition Warplanes Hit Last ISIS Enclave in Eastern Syria | CBC News," accessed April 26, 2019, <https://www.cbc.ca/news/world/syrian-democratic-forces-fight-isis-baghouz-1.5013866>.

will expend his own resources to do so. This jurisdictional rivalry creates a delay in reaction that would otherwise not exist. Incorporating this understanding into SOF infiltration planning can aid in identifying potentially vulnerable points in the enemy's defense.

Smugglers' along the U.S. and Mexican border demonstrate an infiltration method that combines cognitive oversight and jurisdictional gaps. With increasing pressure on drug cartels by U.S. Customs and Border Protection (CBP) and the Drug Enforcement Agency (DEA), smugglers turned to a subterranean network of both pre-existing and newly constructed tunnels to move illicit goods across the U.S./Mexico border. U.S. law enforcement identified the highest concentration of tunnels in Nogales, Arizona, which lies across the border from Nogales, Mexico. From the first tunnel discovery in 1990 through 2014, CPB located 102 tunnels dug by criminals.⁸⁶ CBP classifies tunnels in three categories: rudimentary, interconnecting, and sophisticated.⁸⁷ While rudimentary and sophisticated are independent of existing infrastructure, interconnecting tunnels exploit cognitive oversight. Interconnecting tunnels are short spans that breach existing drainage networks, allowing criminals to tap into the elaborate and largely unmapped system of storm drains on both sides of the border. Once inside the system of subterranean pathways on the U.S. side, smugglers can move drugs, people, and terrorist materials further North and away from the heavily monitored border.⁸⁸ Because the bureaucracies on either side of the border did not consider the drainage system as a potential infiltration avenue due to a lack of imagination, smugglers were able to effectively circumvent robust defenses above ground.

Smugglers use of tunnels not only exploits the fact that CBP and DEA until recently did not think to fortify underground access points against infiltration, but it also takes advantage of the jurisdictional gap along the border. In order to identify potential tunnel

⁸⁶ Jason McCammack, "What Lies Beneath | U.S. Customs and Border Protection," accessed May 8, 2019, <https://www.cbp.gov/frontline/what-lies-beneath>.

⁸⁷ McCammack.

⁸⁸ McCammack.

entries on the Mexico side, U.S. authorities must cooperate with Mexican authorities.⁸⁹ Regardless of how smooth this cooperation is, it inevitably contains friction points with regards to sharing of intelligence and physical access for U.S. personnel to investigate on Mexican soil.⁹⁰ As a result, those defenders against subterranean infiltration must overcome both the lack of information on the location of tunnels and jurisdictional gaps that arise when cooperating with Mexican authorities.

C. SMALL COORDINATED UNITS

Decades of urban fighting and the occasional attempt at SOF infiltration into high population density environments has revealed several lessons learned with regard to large force concentrations. Infiltration in the millennial battlespace cannot rely on superior numbers and overwhelming firepower to be successful. A large infiltration force will undoubtedly be immediately detected and will encounter a reduced enemy response time in a highly connected and densely populated environment. Instead, a SOF force divided into smaller units, synchronized and coordinated toward the same objective, will be necessary.

1. Literature on Urban Warfare and Force Size

Lessons learned from U.S. and non-U.S. campaigns in the urban environment from 1980 to 2015 indicate that units must not only be smaller but also be able to move independently at a tactical level.⁹¹ Regardless of whether the force is conventional military or special operations, complexity increases in urban warfare due to the physical

⁸⁹ “Nogales Tunnel Task Force, Mexican Authorities Shut down Incomplete Drug Tunnel,” accessed May 8, 2019, <https://www.ice.gov/news/releases/nogales-tunnel-task-force-mexican-authorities-shut-down-incomplete-drug-tunnel>.

⁹⁰ Sigrid Arzt, “US-Mexico Security Collaboration: Intelligence Sharing and Law Enforcement Cooperation,” *Shared Responsibility. US-Mexico Policy Options for Confronting Organized Crime*, 2010, 351–69.

⁹¹ The Asymmetric Warfare Group states in their report, “Modern Urban Operations,” illustrated that urban warfare “necessitates decentralized, small-unit operations at the tactical level” in which “small-unit commanders must be resourced and empowered to operate independently based on mission command.” Quoted in “Modern Urban Operations: Lessons Learned from Urban Operations from 1980 to the Present” (Asymmetric Warfare Group, November 2016), 2.

characteristics of the environment that greatly favor the defender and increase the resource demand of the attacker.⁹² The concept of shrinking the problem is one that is applied as a means of countering the complexity of the urban environment by reducing the size and thus the complexity of the assaulting force.⁹³ This idea is executable by reducing the physical size of the unit to shape it to the problem and by employing tactics which minimize the effects of the environment on the mission.

While Clausewitz spoke simply of superior numbers as an advantage, the concept of relative superiority offers the counter-argument in which small numbers of special operations forces can achieve tactical advantage by employing the six principles of special operations.⁹⁴ The concept of relative superiority has already been engrained into special operations forces as a tenant of successful operations and must continue to be as the environment increasingly favors the defender.

Doctrinal references for optimal unit size for an infiltration echo those for urban operations. Simplicity is an essential principle for successful special operations as it is for an infiltration. As the force size and number of units involved increases, so do the complexity and risk level of the mission.⁹⁵ The risk mitigation measures required to plan an infiltration mission do not lend themselves to a large force, as additional operators

⁹² “Modern Urban Operations: Lessons Learned from Urban Operations from 1980 to the Present” (Asymmetric Warfare Group, November 2016), 2.

⁹³ In the work *Reimagining the Character of Urban Operations for the U.S. Army*, RAND presents the concept of “shrinking the problem” of urban operations by developing a “conceptually appropriate way to reduce the magnitude of an urban environment to the point where military forces can exploit localized nuances to operational effect.” Quoted in Gian Gentile et al., “Reimagining the Character of Urban Operations for the U.S. Army” (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1602.html.

⁹⁴ McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice*.

⁹⁵ The United States Army and Marine Corps technique publication, *ATP 3-06: Urban Operations* discusses the force size for infiltration in that, “the difficulty of infiltration attacks increases with the size and number of units involved.” Quoted in Department of the Army, *Urban Operations*, ATP 3-06 (Washington, DC: Army Publishing Directorate, 2017), 4-6.

increase contact with a potentially hostile population.⁹⁶ Ultimately, special operations infiltration into the millennial battlespace necessitates a smaller, dispersed force that can consolidate at a single specified target objective.⁹⁷

2. What Does this Mean in the Millennial Battlespace?

The concepts and theory presented above are founded on experiences of traditional and special operations forces in the urban environment over the last several decades. As it stands, they suggest that small, coordinated units are a more effective infiltrating force in an urban environment. As the net effect of connectivity trends equate to a highly connected population that magnifies the enemy's ability to detect and respond to an infiltrating SOF force, tactics and methods of infiltration must adapt and find ways to exploit these conditions.

A pivotal modification to traditional SOF infiltration is that units must learn to move in even smaller force sizes than they currently do and without overwhelming firepower. Several teams using different routes and modes of transportation to approach the target will reduce the overall signature and likelihood of detection. SOF must rely on McRaven's principles of speed, stealth, and surprise to compensate for their reduced numbers until the entire force consolidates at the objective.⁹⁸ The enemy and sympathetic population, likely conditioned to a traditional SOF infiltration, will not be prepared to detect a well disguised small force that better blends into the pattern of life of a megacity.

Case Analysis

Revisiting the 2008 Lashkar-e-Taiba case as a non-military example of infiltration, the decision by LeT planners to split the force into multiple small teams capitalized on slow communication throughout the Indian security forces and the increased mobility inherent

⁹⁶ *Joint Publication JP 3-06: Joint Urban Operations*, states that "Infiltration depends on situational awareness and understanding of the urban area, careful selection of objectives, detailed planning, and efficient support and deception. Infiltration is not likely to be attempted by large conventional forces, but rather small units. A hostile civilian population reduces the prospects for success." Quoted in Joint Chiefs of Staff, *Joint Urban Operations*, JP 3-06 (Washington, DC: Joint Chiefs of Staff, 2013).

⁹⁷ Department of the Army, *Urban Operations*, 4–18.

⁹⁸ McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice*, 8.

to the smaller units.⁹⁹ Due to the speed with which the five two-man teams of terrorists moved from target to target, and because the multitude of reports reached authorities with varying speed and accuracy, the Indian authorities believed that there was a much larger attacking force than merely ten men.¹⁰⁰ Along with the element of surprise and convincing disguise, the decision to shrink the problem by splitting into small coordinated groups contributed significantly to LeT's disproportionate effects. SOF forces will have to adopt a similar distribution of forces to infiltrate the millennial battlespace, especially considering the defender's detection capabilities will improve, and SOF is subject to ethical and legal constraints which terrorists are not.

Alternatively, the case of OPERATION NEPTUNE SPEAR in 2011 represents a successful SOF infiltration by "shrinking the problem" with an uncharacteristically small force in a highly connected urban environment. At approximately eleven o'clock in the evening on May 1, 2011, a small assault team of 23 Navy SEALs departed Jalalabad Air Field, Afghanistan on two specially modified MH-60 Black Hawk helicopters and headed East toward Pakistan.¹⁰¹ The helicopters had exotic emulsions designed to evade radar, gave off a low heat signature, and had tail rotors designed to reduce noise and radar detection.¹⁰² Pakistan, perpetually in conflict with India on its eastern border, has a sophisticated radar warning system. The majority of the system, however, points toward India, with few systems monitoring the border with Afghanistan where the helicopters would enter the airspace. To avoid detection, they flew nap of the earth, very low, very fast, and hugging riverbeds and valleys that penetrate the foothills of the Hindu Kush mountain range.¹⁰³ Flying low and fast made them harder to be detected by radar and from visual observers. Their flight path skirted north of Peshawar, Pakistan and its millions of

⁹⁹ Tankel, *Storming the World Stage: The Story of Lashkar-e-Taiba*, 215.

¹⁰⁰ Tankel, 215.

¹⁰¹ Kevin Govern, "Operation Neptune Spear: Was Killing Bin Laden a Legitimate Military Objective?," in *Targeted Killings: Law and Morality in an Asymmetrical World* (Oxford University Press, 2012), 355.

¹⁰² Peter L. Bergen, *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*, 1st ed. (New York: Crown Publishers, 2012), 215.

¹⁰³ Bergen, 215.

residents. After about an hour and a half, the helicopters arrived at Abbottabad from the northwest. They avoided the population to the north before hugging the sparsely populated foothills to the east of the city and ultimately turning on the shortest path directly to the compound.¹⁰⁴ Bin Laden's compound was a one-acre complex with a three-story building surrounded by twenty-foot walls at the end of a dirt road in the middle of Bilal Town.¹⁰⁵ Bilal Town is an affluent Abbottabad, Pakistan, suburb surrounded by golf courses and the Pakistani Military Academy.¹⁰⁶

We assess that the population density is high in this case. The city of Abbottabad is a suburban mountain retreat for wealthy individuals to escape from the heat of Islamabad.¹⁰⁷ The population of Abbottabad in 2011 was approximately 150,000 people, based on census interpolation, and the urbanized area was 89 square kilometers.¹⁰⁸ As a result, the population density was 1685 people per square kilometer.¹⁰⁹ By comparison, Abbottabad in 2011 had approximately the same population density as Grand Junction, Colorado or Tuscaloosa, Alabama today.¹¹⁰

The connectivity level for Pakistan and Abbottabad was high. Penetration of broadband internet access, let alone access to land connected internet network, paled in comparison to the rest of the world at the time; however, mobile cellular subscriptions were

¹⁰⁴ Bergen, 215.

¹⁰⁵ Mark Bowden, *The Finish: The Killing of Osama Bin Laden* (London: Grove Press, 2012), 134.

¹⁰⁶ Bowden, 134.

¹⁰⁷ Nicholas Schmidle, "Getting Bin Laden: What Happened That Night in Abbottabad," *The New Yorker*, August 8, 2011, https://www.thomasweibel.ch/artikel/110808_new_yorker_getting_bin_laden.pdf.

¹⁰⁸ Thomas Brinkhoff, "City Population—Population Statistics in Maps and Charts for Cities, Agglomerations and Administrative Divisions of All Countries of the World," City Population, accessed September 2, 2018, <https://www.citypopulation.de/>.

¹⁰⁹ The population size and density of Pakistan and, more specifically Abbottabad, in 2011 cannot be precisely measured because census data is only available from 1998 and 2017. However, we can interpolate between the two censuses to get an approximate value. These databases are available at www.citypopulation.de/ and the Pakistan Bureau of Statistics at United Nations, *Pakistan: Population Density (as of 26 August 2013)* (United Nations Office for the Coordination of Humanitarian Affairs, August 26, 2013), <https://reliefweb.int/map/pakistan/pakistan-population-density-26-august-2013>.

¹¹⁰ "Population Density for U.S. Cities Statistics," Governing, accessed November 15, 2018, <http://www.governing.com/gov-data/population-density-land-area-cities-map.html>.

very prevalent. The Pakistani population had 62 mobile subscriptions for every 100 people in 2011.¹¹¹

Additionally, the likelihood of reporting among the Pakistani population was high as evidenced by the activity of Sohaib Athar on his Twitter account @ReallyVirtual during the raid and the fact that at the time roughly one billion people had access to social media worldwide.¹¹² Even though the Pakistani population was not hostile toward the United States, nor would they have anticipated an infiltration and reported it to bin Laden, they were always on alert from a possible invasion by India. Also, it was not uncommon for helicopters to fly over Abbottabad during the daytime, but it was rare for one to fly over at night.¹¹³ Despite the fact that the Black Hawk helicopters were modified to reduce their noise signature, they were not completely silent; observers during mission rehearsals noticed that they could detect the inbound helicopters about two minutes before their arrival.¹¹⁴ Therefore, the connectivity for OPERATION NEPTUNE SPEAR was high due to the access to a communications network and the population's likelihood of reporting.

The infiltration force arrived on the target at one o'clock in the morning, when they would have the longest period of darkness during which to conduct the assault. The SEALs had planned and rehearsed their actions to allow for no more than 30 minutes on the ground, which they assessed to be the response time of an alerted Pakistani military. There was no planned air superiority nor any close air support aircraft. This decision was intended to prevent the Pakistani air forces from being alerted to the presence of the infiltration force and reduce the overall signature of the infiltration. The only additional forces were a quick

¹¹¹ Murphy and Roser, "Internet."

¹¹² Cathy Scott-Clark, *The Exile: The Stunning inside Story of Osama Bin Laden and Al Qaeda in Flight* (New York: Bloomsbury, 2017), 420–25; Oriana Pawlyk, "The Days of Secret Military Operations May Soon Be Over. Does That Matter?," *Military.com*, December 1, 2018, <https://www.military.com/daily-news/2018/12/01/days-secret-military-operations-may-soon-be-over-does-matter.html>.

¹¹³ Schmidle, "Getting Bin Laden: What Happened That Night in Abbottabad."

¹¹⁴ Bergen, *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*, 183.

reaction force (QRF) that followed on three MH-47 Chinooks and were waiting outside the city limits in the event that the assault force became overwhelmed.¹¹⁵

The helicopters successfully arrived at the target compound without alerting the occupants or the Pakistani military. The plan was to fast-rope the force onto the roof and inside the internal walls. However, one of the helicopters lost control and managed to execute a controlled crash into an animal pen outside of the interior walls.¹¹⁶ Fortunately, no one was injured, so the assault force exited the aircraft and proceeded on the mission.

For the next 38 minutes, the SEALs cleared the three-story building room by room in search of bin Laden. Meanwhile, the noise of the crash, explosions, and gunfire alerted the civilian neighbors who began to investigate after about 15 minutes.¹¹⁷ One citizen, Sohaib Athar, live-tweeted the incident, commenting that “Helicopter hovering above Abbottabad at 1 AM (is a rare event).”¹¹⁸ At this point, the connectivity of the local population compromised the mission. The interpreter with the assault force managed to control the crowd long enough for the SEALs to finish the operation, destroy the damaged helicopter, and extract via one of the waiting Chinooks.¹¹⁹ The U.S. forces sustained no casualties throughout the mission, and the Pakistani army did not respond. Only after the helicopters departed the area did the Pakistani military respond with two F-16s, but the helicopters were never detected or under threat.

The mission was deemed a success because it resulted in Osama bin Laden’s death and the collection of a large amount of intelligence. It was, however, marred by the loss of the stealth helicopter and compromised by a civilian bystander who revealed information about the mission to approximately one billion people with access to social media.¹²⁰

¹¹⁵ Bergen, 215.

¹¹⁶ Schmidle, “Getting Bin Laden: What Happened That Night in Abbottabad.”

¹¹⁷ Mark. Owen, *No Easy Day: The Autobiography of a Navy SEAL: The Firsthand Account of the Mission That Killed Osama Bin Laden* (New York, N.Y.: Dutton, 2012), 250.

¹¹⁸ Pawlyk, “The Days of Secret Military Operations May Soon Be Over. Does That Matter?”

¹¹⁹ Schmidle, “Getting Bin Laden: What Happened That Night in Abbottabad.”

¹²⁰ Pawlyk, “The Days of Secret Military Operations May Soon Be Over. Does That Matter?”

The case of OPERATION NEPTUNE SPEAR exemplifies a small unit special operations infiltration into an urbanized, high connectivity environment. The infiltration force knew that they would face a variety of challenges that increased the risk of being detected by the Pakistani military and population. There was serious risk that Pakistan's robust air defense system would detect the helicopters and launch fighters to intercept them. By shrinking the problem, the small size of the infiltration force helped to reduce the risk of detection because there was less chance that they would be picked up on radar or be seen or heard by the population during the infiltration. These risk mitigation measures enabled the assault force to reach the target undetected. Only after several minutes in the target area and one of the helicopters crashing did civilians in the area detect the assault force. Fortunately, the surrounding population was not particularly hostile, or it may have overwhelmed the small force. This case demonstrates how a small force size reduces the chance that a passive observer will have an opportunity to detect an infiltration.

D. SPECIALIZED SOF CYBER

Trends in communication and data processing have the potential to level the proverbial playing field in the cyber domain between SOF and enemy adversaries. The enemy will have increased situational awareness of an infiltrating SOF unit, and therefore SOF forces must have specialized cyber warriors with the necessary resources and skills to ensure the success of the infiltration. These cyber specialists should be able to manage the friendly cyber signature, support deceptions with cyber based information operations, exploit the enemy's cyber signature, and monitor online reflections about operations in real-time.

1. Literature on Global Communications and Data Processing

The global trends in communication point toward a worldwide network of interconnected individuals. As of 2019, only 58 percent of the world's population has internet access.¹²¹ The United Nations, however, has pledged to bring affordable internet

¹²¹ Miniwatts Marketing Group, "World Internet Users Statistics and 2019 World Population Stats," March 2019, <https://www.internetworldstats.com/stats.htm>.

to the entire population by 2030 through sustainable development.¹²² While globalization and advances in technology will certainly help to improve living conditions and reduce poverty, it will paradoxically result in emboldening and empowering anti-establishment groups, potentially leading to greater conflict.¹²³ The paradox is both promising and ominous as special operations forces may find themselves facing numerous, highly-connected groups in unfamiliar environments.

Moving beyond the question of how much of the population will be interconnected, we must consider the effects of this connectivity on SOF operations. Adversaries large and small can take advantage of the affordability of sophisticated cyber systems to have an asymmetric impact in cyberspace.¹²⁴ Enemy militaries and governments can economically and effectively analyze social media data to build intelligence on their opponents' movements.¹²⁵ Additionally, while it is possible for real-time tweet classification, the rate of collection and amount of the data requires multiple processors and advanced algorithms to be successful.¹²⁶ This is certainly not an insurmountable hindrance as publicly accessible social media networks can diffuse information at near real-time, and algorithms are increasingly able to detect emerging patterns, shape information flows, and make predictions based on the observed trends.¹²⁷ The application of analysis algorithms with machine learning artificial intelligence (AI) will eventually facilitate data analysis of audio and video-based information as well.¹²⁸ Ultimately, emerging technology will soon allow

¹²² McCarthy, "United Nations Pledges to Get Everyone Online...by 2030."

¹²³ "Global Trends Home Page."

¹²⁴ Eric Leonhardi, Mark Murphy, and Hannah Kim explore this subject in their NPS thesis, "Analysis of Department of Defense Social Media Policy and its Impact on Operational Security" specifically concerning Operational Security (OPSEC) for military operations. Quoted in Eric V. Leonhardi, Mark Murphy, and Hannah Kim, "Analysis of Department of Defense Social Media Policy and Its Impact on Operational Security" (Master's thesis, Naval Postgraduate School, 2015), 15.

¹²⁵ Patrick M. Gillen, "Real-Time Detection of Operational Military Information in Social Media" (Master's thesis, Naval Postgraduate School, 2015).

¹²⁶ Gillen, 52.

¹²⁷ Karthik Kambatla et al., "Trends in Big Data Analytics," *Journal of Parallel and Distributed Computing* 74, no. 7 (2014): 2570, <https://doi.org/10.1016/j.jpdc.2014.01.003>.

¹²⁸ Daniel O'Leary, "Artificial Intelligence and Big Data," *IEEE Intelligent Systems* 28, no. 2 (April 2013): 99, <https://doi.org/10.1109/MIS.2013.39>.

an adversary to collect, aggregate, and interpret enormous amounts of real-time data and pose a credible threat to SOF infiltration.

2. What Does this Mean in the Millennial Battlespace?

The concepts presented above illustrate an environment in which the ability to collect, analyze, and interpret data obtained from a plethora of sources is becoming more attainable by potential adversaries. The enemy can exploit the connectedness of the population to gather information in real-time. No longer is it necessary to possess state-level resources to have a robust cyber capability. Non-state actors can also obtain the technology required to leverage an asymmetric threat against SOF infiltration.

In the millennial battlespace, integrated air defense systems will not be the only means of detecting an airborne infiltration, nor will closed-circuit televisions (CCTV)—like in Beijing, China or London, England—be the only way to monitor ground movements in urban areas.¹²⁹ Instead, a population connected through personal devices, social media, and other means will create a network of passive and active sensors which can be exploited by both defender and attacker. A simple Twitter post of an aircraft flying overhead from a casual observer or a photograph of a suspicious looking vehicle driving in a neighborhood could compromise a SOF infiltration. In states with fewer privacy laws than the U.S., personal devices may have software forcibly installed which allows the state to monitor the microphone, camera, and location at all times, providing a steady stream of observational data. Doing so would turn both witting and unwitting civilians into sensors feeding a central processing node. In an era when data-processing capabilities are rapidly expanding through machine learning and AI, this metadata could potentially enable a rapid response to a security threat.

SOF must evolve its employment of cyber forces to be effective in the millennial battlespace. While cyber forces currently support SOF operations in a complementary

¹²⁹ “Top 5 Cities with the Largest Surveillance Camera Networks,” [vintechnology.com](https://vintechnology.com/2011/05/04/top-5-cities-with-the-largest-surveillance-camera-networks/), May 4, 2011, <https://vintechnology.com/2011/05/04/top-5-cities-with-the-largest-surveillance-camera-networks/>.

capacity, their integration and role are insufficient and generally reactionary.¹³⁰ A SOF infiltration in the millennial battlespace will require a more robust and dedicated cyber element embedded into the unit, directly supporting and even accompanying the assault force. The cyber operator must be specially trained in the nuances of SOF operations and play an offensive and defensive role by facilitating both deception and physical disruption of the network of passive sensors embedded in the population. SOF will require the ability to monitor and disrupt friendly and enemy social media activity for specific signatures that may compromise the mission.

3. Case Analysis

A current case that illuminates the challenges of conducting a traditional SOF infiltration in both a high population density and high connectivity environment is that of U.S. Air Force CV-22 Osprey operations in Japan. Air Force Detachment 353 is the unit that currently flies the CV-22 Osprey at Yokota Air Base in Tokyo, Japan. The population of Tokyo in 2018 was approximately 9.5 million people based on 2018 census, and the urbanized area was 627 square kilometers.¹³¹ As a result, the population density was 15,248 people per square kilometer. Additionally, the Japanese population has 133 mobile subscriptions for every 100 people compared to the world average of 104 for every 100 in 2017.¹³² The Ospreys arrived in 2018 with a fair amount of controversy due to the Japanese citizens' concerns regarding safety and noise-level. Not only is the environment highly dense and highly connected, but due to the resistance to the aircraft's presence, Japan could be considered a semi-permissive or even hostile environment.

Twitter is one of the most popular social media platforms in the region, and it also has a program that can "scrape" past tweets, searching for specific hashtag phrases.¹³³

¹³⁰ Clint Tracy, "Operationalizing Cyber, Electronic Warfare, Space, Special Technical Operations for Decisive Action," *Fires*, 2018, 11.

¹³¹ Brinkhoff, "City Population—Population Statistics in Maps and Charts for Cities, Agglomerations and Administrative Divisions of All Countries of the World."

¹³² Murphy and Roser, "Internet."

¹³³ "Japan: Social Network Audience Reach 2017 | Statistic," Statista, accessed September 10, 2018, <https://www.statista.com/statistics/258849/most-popular-social-networks-in-japan-ranked-by-reach/>.

Comparison of tweets to actual flight data from Detachment 353 reveals correlation that an adversary could exploit. We observe that there is a distinct spike in Twitter posts during flying periods on a given day. Notably, on July 26, 2018, Figure 1 shows this correlation.



Figure 1. Tweets per hour compared to flying training times in Japan on July 26, 2018

Analysis of the tweets reveals that posts consisted of photographs, videos, and comments concerning the Osprey during its flying period (Figure 2); posts during the non-flying period show non-specific posts and retweets regarding the presence of the Osprey in Japan. The concentration in Twitter activity that occurs spatially during the flying period correlates to the spike in activity temporally. In conjunction with the content from the actual posts during the flying period, there is evidence that social media activity could function as an early warning system to locate a SOF infiltration force in a similar environment.



Figure 2. Tweet examples (descriptive context)

This example is not applicable to every environment and threat; however, the findings reveal some essential indicators about the challenges traditional SOF infiltration will face in the millennial battlespace. A highly connected population, with a predisposition to report activity, could compromise security and the ability to maintain surprise during an infiltration mission. Regardless of whether the population is friendly or hostile, this brief but powerful example demonstrates that a SOF aircraft could be detected and located both temporally and spatially with enough accuracy that an opposing force could be alerted to their arrival well in advance. The Twitter activity would need to be able to be monitored in real time, and analyzed for key terms that would signal special operations activity. Additionally, the population would have to be active enough on social media to post at a frequency necessary to provide a spike in activity. Ultimately, as Twitter and other social media scrubbing algorithms learn how to better “read” the context of tweets, and adversaries can process more social media data from decentralized sources faster, it will likely become easier to spatially and temporally detect where SOF aircraft are operating using this method.

A state that closely monitors its citizens' communications could detect, coordinate, and react against an infiltration. While this notion may seem far-fetched, there is at least one contemporary example of such a system already in place. The Chinese government has constructed a multi-faceted surveillance apparatus in its Xinjiang province that resembles a dystopian science fiction society.

Xinjiang Province is roughly 1500 miles west of Beijing and borders Tibet, India, Mongolia, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Afghanistan, and Pakistan. It is home to the Uyghur ethnic group, a Turkic people who follow Islam. China has historically struggled to maintain control in this vast region.¹³⁴ After a series of fatal riots in 2009 and bombings in 2014 attributed to Xinjiang-based militants, the Chinese government launched an internal security campaign called, "The Strike Hard Campaign Against Violent Terrorism."¹³⁵ This effort entailed a massive increase in surveillance and population coercion measures. According to a Chinese human rights lawyer, the cutting-edge technologies used in Xinjiang will appear soon in other parts of China.¹³⁶

Following terrorist bombings in 2014 that the Chinese government attributed to Xinjiang based Uyghurs, the government appointed Chen Quanguo as Party Secretary for Xinjiang. Known for his harsh methods of suppressing dissent in Tibet, Quanguo drastically ramped up surveillance and population control measures in Xinjiang beginning in 2016.¹³⁷

Quanguo began by creating 7,500 "convenience police stations" in Xinjiang, essentially placing police on every street corner. Additionally, the government rolled out a surveillance network incorporating facial recognition, the collection of biometric data, GPS

¹³⁴ Elizabeth Van Wie Davis, "Uyghur Muslim Ethnic Separatism in Xinjiang, China," *Asian Affairs: An American Review* 35, no. 1 (2008): 15–30, <https://doi.org/10.3200/AAFS.35.1.15-30>.

¹³⁵ Doyon, "Counter-Extremism' in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics."

¹³⁶ Josh Chin and Clement Burge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal Eastern Edition*, December 20, 2017.

¹³⁷ "Eradicating Ideological Viruses: China's Campaign of Repression Against Xinjiang's Muslims" (Human Rights Watch, September 2018), 12, https://www.hrw.org/sites/default/files/report_pdf/china0918_web.pdf.

tracking of private vehicles, and spyware in Uyghurs' smartphones.¹³⁸ Though it is unclear if the entire system is in place currently, China's stated goal of consolidating the information from the various sources and processing it with AI would enable personnel at its "convenience police stations" to rapidly interdict individuals suspected of "extremism."¹³⁹

A central component of China's surveillance network in Xinjiang is the implementation of mandatory monitoring apps on internet devices. These applications send records of all calls and messages made on the individuals' devices to a central processing hub in real-time. This element of the surveillance network essentially turns every connected device into an observation tool for the state. In the case of Xinjiang, the state is using the data from personal devices to hone in on perceived internal threats. The state could just as easily use this same capability to monitor for external threats observed by individual citizens.

Although China's surveillance system in Xinjiang targets Chinese citizens rather than foreign intruders, one can readily imagine how such an environment could pose enormous challenges to SOF called upon to infiltrate an environment with similar technology. The networked approach to internal security that connects cameras, drones, human observers, civilian cell phones, and vehicle/body scanners to an AI empowered hub would make the likelihood of detection extraordinarily high and the efficiency with which that information reaches a central command center equally high.

As population density and rates of connectivity increase, an adversary with the ability to tap into interpersonal communication and sort the massive amount of data in real-time could have a considerable advantage in detecting security threats, both internal and external. The contemporary example of China's surveillance in Xinjiang combined with the example of the civilian reports of special operations activity in Japan demonstrate that such a capability is no longer mere science fiction. These examples are isolated, but they

¹³⁸ Doyon, "Counter-Extremism' in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics."

¹³⁹ Doyon.

paint a vivid picture of the millennial battlespace. To infiltrate this environment, SOF will need specialized cyber forces that can anticipate, neutralize, and leverage this massive network of sensors upon which a defender relies.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RECOMMENDATIONS AND CONCLUSION

A. TRANSFORMING SOF INFILTRATION

The time to transform our SOF units to infiltrate the future environment is now. Using our theory to guide our recommendations, we will suggest concrete steps that SOF must take today to adapt to the changing requirements of the high population density, high connectivity environment. Simply making small tweaks to decades-old training, tactics, and technology does not address the rapidly changing nature of the future battlefield. Our recommendations stem from the theory of infiltration and our study of the future battlefield.

1. Training

SOF training is a feedback loop. Traditionally, deployed units report lessons-learned back to training commands, who then update their curriculums accordingly for the next unit to deploy. This method fits well with periods of sustained conflict where the enemy's actions and the operating environment remain consistent. This method is reactive, however, and will not prepare SOF for a rapid transition from infiltrating sparsely populated deserts and mountains to expansive megacities. To do so, we must be proactive in our training regime in anticipation of an increasingly unforgiving and lethal operating environment. Based on our theory of SOF infiltration, we propose the following five changes to SOF training: operation of indigenous mobility platforms, navigation of underground urban infrastructure, use of cutting-edge disguise techniques, the creation of an organic SOF cyber warfare capability, and social media signature training.

To improve SOF's ability to remain undetected during infiltration in urban environments, they should train on indigenous mobility platforms that will easily blend in with the pattern of life in target environments. The emphasis should be placed not on indigenous military platforms, but primarily on indigenous commercial platforms. For example, SOF small boat operators should gain proficiency operating fishing and merchant type vessels in the same manner that professional fisherman and merchants would. Doing so with maritime, ground, and aerial platforms will enable SOF to delay detection and increase the enemy's reaction time.

Part of neutralizing the defender's advantage in an urban environment will be the use of above—and below—ground infrastructure to travel. To do so, SOF must train at underground navigation. This training will depend on available navigation technology that is not reliant on the global position system (GPS). To start, however, SOF units should merely begin by practicing moving through the underground infrastructure of cities in controlled training environments.

The apparent difference in physical appearance between most SOF members and the populace in the areas SOF will operate poses a severe risk of detection. As such, SOF should treat physical disguise as a core skill set, like shooting and combat medicine. There is no reason that SOF should not be employing the techniques of cinematic make-up artists to change members' appearances to match those of the operating environment. Like the use of indigenous vehicles, expert physical disguises can delay detection enough to prevent an effective enemy reaction at a very low cost.

To take on the myriad of cyber impediments to infiltration, SOF needs to develop an organic cyber capability. Specifically, SOF units will need to collectively understand and account for how their physical movements and actions will reflect across networks of highly connected civilians as well as enemy military cyber defenses. Rather than training a cyber-specialist to accompany SOF units, we should train a SOF member to plan and execute the cyber component of an infiltration. Placing the cyber skills in the hands of SOF members would likely result in a better understanding among the unit of how to offensively employ cyber to enable infiltration and increase awareness of vulnerabilities to enemy cyber operations.

SOF must adopt a new perspective on the social media signature of its members to facilitate infiltration. Historically, social media use is tolerated in SOF but viewed as a nuisance to be constrained and ideally eliminated due to the amount of compromising personal and unit information that an adversary could glean from it. Attempting to curb that use is not only an uphill battle for SOF leaders but potentially counterproductive. With the prevalence of social media use today, a sudden lack of activity by a SOF member that is normally very active is also a data point for the enemy. SOF must not only train members to restrict the accurate information they publicize; with a studied understanding of how

social media activity informs the enemy, SOF can then deliberately manipulate its online signature to support deception and aide in infiltration.

2. Tactics

Multimode, dispersed infiltration will be the key to infiltrating future urban environments. Avoiding a concentration of SOF members while transiting through urban environments will decrease the likelihood of detection and hamper enemy interdiction efforts. Rather than numerous vehicles moving together with the entire SOF unit concentrated, we must work toward individuals using different modes of transportation but synchronized through the use of advanced communication technology. The advantages of concentrating the force during infiltration (i.e., the ability to bring greater firepower to an enemy engagement), are outweighed in the millennial battlespace by the much higher likelihood of detection when infiltrating as an entire unit.

Historically, SOF has sought infiltration routes that avoid high concentrations of traffic. In the future environment, it must do the opposite. Using indigenous infiltration platforms along the paths of high traffic concentration gives the advantage to the SOF unit over the enemy security forces trying to find the “needle in the haystack.” LeT’s maritime infiltration of Mumbai harbor by blending in with the mass of small fishing boats exemplifies this tactic.

Just as we must train SOF members on how social media use influences the enemy’s intelligence, tactically leveraging this understanding is critical to conducting infiltration. After acknowledging the enemy’s capability to identify patterns among SOF social media accounts that forewarn of an infiltration, the next step is to incorporate this understanding into Information Operations (IO) and Psychological Operations (PSYOP). Doing so would turn a vulnerability into an asset to use in support of SOF operations. Essentially, if we know what patterns the enemy looks for to identify an imminent operation, we can either artificially create the impression of a diversionary operation or deliberately refrain from sending such signals.

3. Technology

The United States military has a long-standing reputation for investing in technological and other innovations for overt and clandestine purposes. SOF often modifies existing technologies for specific purposes rather than originating them from scratch. Our recommended technological focus areas are intended to meet the inevitable needs of the infiltrating SOF force in the future battlespace. The requirements for greater deception, use of cognitive defilade, and small coordinated units will be possible with the use of communications improvements, faster, smaller, non-traditional vehicles, and subterranean mapping and navigation technologies.

The United States military has often been at the forefront of communications technology. Some of the most sophisticated and secure communication and data systems completely changed how we conduct warfare. Data links between air, ground, sea, and spaceborne assets aid in synchronization and coordination of the battlespace on a grand scale. Advancements are leveling the proverbial playing field with the enemy, which means that SOF must adapt. Currently, data link and high bandwidth voice and video communication are only available through equipment mounted in vehicles. Once the ground force leaves the vehicle, their access to information is usually limited to only voice. As tactics adapt to address the new environment, units will need to be divided into smaller teams and utilize multiple modes of transportation. This shift will require more coordination between the mission commander and individual elements. SOF units must take advantage of the rapid advancements in communication technology by scaling the data link down to the single soldier. This capability will allow the SOF unit to simplify the problem by having a smaller force but also maintain relative superiority with unparalleled situational awareness during the mission. While the technology may not yet exist, it could take the form of a helmet integrated heads up display, goggles, or another wearable device. SOF units should leverage advanced communications technology and the high connectivity environment to maintain situational awareness, coordinate movements, and precisely time assaults.

As mentioned earlier, a combination of modes of transit will be vital to infiltration in the future battlespace. SOF's incorporation of high speed vehicles, deceptive indigenous

vehicles, and small, maneuverable aerial platforms will satisfy mobility capability requirements of future infiltration. Considering that SOF will likely not avoid detection, they must strive to delay it. Increased speed of travel is essential to stalling the enemy's response. As such, SOF units must invest in vehicles capable of higher speeds to increase the time from detection to enemy reaction.

Additionally, current SOF vehicles have a particular signature and performance that are immediately recognizable as distinctly military. The sound and performance of a Black Hawk helicopter or Humvee stand out from commercial aircraft and trucks. LeT utilized common indigenous vehicles to blend into the environment and facilitate deception as well as exploit the cognitive defilade with success. Similarly, traditional SOF infiltration will have to evolve away from the strict use of military vehicles and explore non-traditional vehicles with more speed and adaptability for use in the environment of a megacity.

The tight physical spaces and vertical development of a megacity are not conducive to the traditional SOF infiltration aerial vehicle. Transmission lines, antennas, spires, traffic lights, etc., all pose a hazard for helicopters in the urban environment. Even though SOF units currently train for urban infiltrations, an enemy can easily protect their structure from traditional platforms with simple homemade defenses. In the millennial battlespace, the enemy will leverage the defensive advantages inherent to the urban environment wherever they can. Consequently, SOF must adopt aerial vehicles that are small and maneuverable enough to negotiate the three-dimensional space of a city with the ability to fly in between structures and light enough to land nearly anywhere. These smaller aircraft will naturally facilitate division into smaller, more maneuverable and coordinated elements necessary for infiltration.

SOF units will need a technology that facilitates navigation of the subterranean infrastructure in megacities. To maximize the potential of a multimode dispersed infiltration in the megacity environment, SOF must use all avenues of approach, including underground spaces. The subterranean environment poses limitations in that GPS does not work, and a compass may be inaccurate due to influences from urban infrastructure. Additionally, the availability of up-to-date and accurate diagrams of this domain is unlikely. Therefore, future SOF infiltration will hinge on advances not yet conceived or

developed in navigation equipment that functions underground so forces can synchronize movements, avoid enemy detection networks, and effectively launch attacks against enemy utilizing subterranean spaces for defense.

B. CONCLUSION

The challenges SOF will face when conducting infiltration in millennial battlespace are numerous. Our analysis of current global trends indicates that the population density and connectivity will continue to increase over the next 15 years. Consequently, we focused on several key trends. Global urbanization will concentrate the world's population into geographically larger, denser cities and megacities. Ungoverned spaces will exist in these urban zones in which both state and non-state actors can find security. Enemy organizations will migrate out of rural areas to ungoverned urban spaces. Communication is becoming faster, cheaper, more data intensive, and easier to disseminate widely. An organization with sufficient resources can exploit the massive amount of communications data generated by individual citizens for its benefit. In sum, SOF's ability to reach a specific target using traditional means of infiltration with sufficient time to conduct its operation will be in jeopardy.

Based on the trends above, we predict that by 2035 the battlespace will change in several ways that affect SOF infiltration. Extensive concealment and cover provided by human-made structures in urban terrain will overwhelmingly favor the defender over the assaulting force. An enemy organization's ability to counter SOF infiltration will be tied even more closely to whether or not it has the cooperation of the local population. Increases in population density will mean that infiltration routes through populated areas are unavoidable. The defender will be able to identify security threats much more rapidly than we have seen throughout history with an increase in sensors and computing capability. The defenders' response time to threats will significantly decrease with the greater situational awareness that communication technology will allow. Both infiltrator and defender will be vulnerable to attacks against their respective IT networks. Finally, the infiltrating unit's situational awareness will increase through the use of emerging communication technology, enabling more sophisticated tactics to meet the rising threat.

The success of SOF infiltration will depend on how well planners prepare today to address our findings. First, SOF infiltration should focus on deception over stealth. Second, SOF infiltration must employ routes that use cognitive rather than physical defilade. Third, infiltration will require smaller, better-coordinated units. Finally, infiltration will require specialized SOF cyber to counter enemy capabilities. Ultimately, success will depend on the willingness of today's leaders to take risks and experiment with new methods of infiltration.

C. AREAS OF FUTURE STUDY

The adage from World War II propaganda “loose lips sink ships” holds relevance in the current and future battlespace. In the past, discussion of classified operations was limited to anyone within earshot; now, an errant post on social media is visible to billions of people. While some studies exist that explore the impacts of military members posting information about operations, enemy forces are now able to aggregate seemingly innocuous social media data from service members to build a detailed picture of our operations. For instance, account activity patterns, location data from fitness devices, or a sudden lack of activity can signal to the enemy that a unit may be deploying or conducting an operation. Further work correlating SOF's use of social media to operations would allow us to turn a vulnerability into a flexible tool for deception and greater operational security.

Infiltration in the future battlespace will require the use of non-traditional vehicles. We cannot predict what specific technologies will make it through the rigors of development and acquisitions. The vehicles required will not be new variants of current military platforms, however. Instead, we should consider vehicles that are capable of exceptional agility in confined spaces while not discounting the value of common commercial vehicles as effective infiltration platforms. For instance, there have been recent breakthroughs in jetpacks that could facilitate the dispersed infiltration tactics and the small, light, and maneuverability demands of the urban environment mentioned earlier. Similarly, there is a company developing a flying motorcycle which may be ideal for maneuvering through the urban environment. Other technologies like wingsuits and powered body armor bring capabilities previously seen only in large platforms to an

individual level. While these vehicles may not meet all the demands and may even stand out more than a traditional military vehicle in some instances, they offer SOF a means to conceive of new ways with which to conduct infiltration in the millennial battlespace. It will be the development and adaptation of some of these technologies which will increase the mobility of the individual SOF member, allowing them to disperse or concentrate with greater maneuverability, that will facilitate successful infiltration.

LIST OF REFERENCES

- Abasa, Africano. "Ungoverned Spaces and the Survival of Terrorist Groups in Africa: A Case Study of the Lord's Resistance Army." Master's thesis, Naval Postgraduate School, 2015. <https://calhoun.nps.edu/handle/10945/47802>.
- Adey, Peter. "Vertical Security in the Megacity: Legibility, Mobility and Aerial Politics." *Theory, Culture & Society* 27, no. 6 (2010): 51–67.
- Arquilla, John, and David F. Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. MR / Rand Corporation; MR-1382-OSD. Santa Monica, CA: Rand, 2001.
- Arzt, Sigrid. "US-Mexico Security Collaboration: Intelligence Sharing and Law Enforcement Cooperation." *Shared Responsibility. US-Mexico Policy Options for Confronting Organized Crime*, 2010, 351–69.
- Beaumont, Claudine. "Mumbai Attacks: Twitter and Flickr Used to Break News," November 27, 2008, sec. World. <https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html>.
- Bergen, Peter L. *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*. 1st ed. New York: Crown Publishers, 2012.
- Bougen, Philip D., and Pat O'Malley. "Bureaucracy, Imagination and U.S. Domestic Security Policy." *Security Journal* 22, no. 2 (2009): 101. <https://doi.org/10.1057/palgrave.sj.8350078>.
- Bowden, Mark. *The Finish: The Killing of Osama Bin Laden*. London: Grove Press, 2012.
- Boyne, Sean. "Uncovering the Irish Republican Army." News. PBS Online, August 1, 1996. <https://www.pbs.org/wgbh/pages/frontline/shows/ira/inside/org.html>.
- Brinkhoff, Thomas. "City Population—Population Statistics in Maps and Charts for Cities, Agglomerations and Administrative Divisions of All Countries of the World." City Population. Accessed September 2, 2018. <https://www.citypopulation.de/>.
- Campbell, John. "Terrorists Are Not the Only Ones Exploiting Ungoverned Spaces Across Nigeria." *Council on Foreign Relations* (blog), May 15, 2018. <https://www.cfr.org/blog/terrorists-are-not-only-ones-exploiting-ungoverned-spaces-across-nigeria>.

- Castiglia, Arthur M. "Megacities and the Role of U.S. Special Operations Forces." Master's thesis, United States Army War College, 2015.
- Chin, Josh, and Clement Burge. "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life." *The Wall Street Journal Eastern Edition*, December 20, 2017.
- "Coalition Warplanes Hit Last ISIS Enclave in Eastern Syria | CBC News." Accessed April 26, 2019. <https://www.cbc.ca/news/world/syrian-democratic-forces-fight-isis-baghoub-1.5013866>.
- Cronin, Audrey Kurth, and James M. Ludes. *Attacking Terrorism: Elements of a Grand Strategy*. Washington, D.C: Georgetown University Press, 2004.
- Daniel, Donald C., Katherine L. Herbig, William Reese, Richards J. Heuer, Theodore R. Sarbin, Paul H. Moose, and Ronald G. Sherwin. "Multidisciplinary Perspectives on Military Deception." Technical Report. Monterey, CA: Naval Postgraduate School, 1980.
- Daniel O'Leary. "Artificial Intelligence and Big Data." *IEEE Intelligent Systems* 28, no. 2 (April 2013): 96–99. <https://doi.org/10.1109/MIS.2013.39>.
- Davis, Elizabeth Van Wie. "Uyghur Muslim Ethnic Separatism in Xinjiang, China." *Asian Affairs: An American Review* 35, no. 1 (2008): 15–30. <https://doi.org/10.3200/AAFS.35.1.15-30>.
- Deacon, Richard. *A History of the Russian Secret Service*. New York: Taplinger Pub. Co., 1972.
- Department of the Army. *Urban Operations*. ATP 3–06. Washington, D.C.: Army Publishing Directorate, 2017.
- Dimock, Michael. "Defining Generations: Where Millennials End and Generation Z Begins." *Pew Research Center* (blog). Accessed May 9, 2019. <https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/>.
- Dingley, James. *Combating Terrorism in Northern Ireland*. Cass Series on Political Violence. London: Routledge, 2009.
- Doyon, Jerome. "Counter-Extremism' in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics." *War on the Rocks*, January 14, 2019. <https://warontherocks.com/2019/01/counter-extremism-in-xinjiang-understanding-chinas-community-focused-counter-terrorism-tactics/>.
- Dunnigan, James F. *Victory and Deceit: Dirty Tricks at War*. 1st ed. New York: W. Morrow, 1995.

- Freeman, Michael. "The Sources of Terrorist Financing: Theory and Typology." *Studies in Conflict & Terrorism* 34, no. 6 (2011): 461–75.
- Gentile, Gian, David E. Johnson, Lisa Saum-Manning, Raphael S. Cohen, Shara Williams, Carrie Lee, Michael Shurkin, Brenna Allen, Sarah Soliman, and James L. III Doty. "Reimagining the Character of Urban Operations for the U.S. Army." Santa Monica, CA: RAND Corporation, 2017.
https://www.rand.org/pubs/research_reports/RR1602.html.
- Gill, Paul, J. Lee, K. Rethemeyer, J. Horgan, and V. Asal. "Lethal Connections: The Determinants of Network Connections in the Provisional Irish Republican Army, 1970–1998." *International Interactions: Empirical and Theoretical Research in International Relations*, 2014.
- Gillen, Patrick M. "Real-Time Detection of Operational Military Information in Social Media." Master's thesis, Naval Postgraduate School, 2015.
- Glenn, Russell W. "Megacities: The Good, the Bad, and the Ugly"." *Small Wars Journal*, no. Feb (2016). <http://smallwarsjournal.com/jrnl/art/megacities-the-good-the-bad-and-theugly>.
- "Global Trends Home Page." Accessed August 6, 2018.
<https://www.dni.gov/index.php/global-trends-home>.
- Govern, Kevin. "Operation Neptune Spear: Was Killing Bin Laden a Legitimate Military Objective?" In *Targeted Killings: Law and Morality in an Asymmetrical World*, 347–73. Oxford University Press, 2012.
- Hatch, Harris, and Stewart Alexander. *Electrotyping and Stereotyping*. Chicago: United Typothetae of America, 1918.
- Hussain, Nazia, and Louise Shelley. "Karachi Organized Crime in a Key Megacity." *Connections* 15, no. 3 (Summer 2016): 5–16.
- Jackson, Henry F. *The FLN in Algeria: Party Development in a Revolutionary Society*. Contributions in Afro-American and African Studies ; No. 30. Westport, Conn: Greenwood Press, 1977.
- Jalal, Ayesha. *Partisans of Allah: Jihad in South Asia*. Cambridge, Mass: Harvard University Press, 2008.
- "Japan: Social Network Audience Reach 2017 | Statistic." Statista. Accessed September 10, 2018. <https://www.statista.com/statistics/258849/most-popular-social-networks-in-japan-ranked-by-reach/>.
- Joint Chiefs of Staff. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*. Defense Technical Information Center, 2019.

- . *Joint Urban Operations*. JP 3-06. Washington, D.C.: Joint Chiefs of Staff, 2013.
- . *Special Operations*. JP 3-05. Washington, D.C.: Joint Chiefs of Staff, 2014.
- Kambatla, Karthik, Giorgos Kollias, Vipin Kumar, and Ananth Grama. “Trends in Big Data Analytics.” *Journal of Parallel and Distributed Computing* 74, no. 7 (2014): 2561–73. <https://doi.org/10.1016/j.jpdc.2014.01.003>.
- Koonings, Kees, and Dirk Kruijt. *Megacities: The Politics of Urban Exclusion and Violence in the Global South*. London: Zed Books, 2009.
- La Caille John, Louise, and Louise Reynnells. “What Is Rural?” United States Department of Agriculture, May 2016. <https://www.nal.usda.gov/ric/what-is-rural#HEALTH>.
- Lafleur, Jarret, Liston Purvis, Alex Roesler, and Paul Westland. “The Perfect Heist: Recipes from Around the World.” Albuquerque, NM: Sandia National Laboratories, March 2015.
- Leonhardi, Eric V., Mark Murphy, and Hannah Kim. “Analysis of Department of Defense Social Media Policy and Its Impact on Operational Security.” Master’s thesis, Naval Postgraduate School, 2015.
- McCammack, Jason. “What Lies Beneath | U.S. Customs and Border Protection.” Accessed May 8, 2019. <https://www.cbp.gov/frontline/what-lies-beneath>.
- McCarthy, Kieren. “United Nations Pledges to Get Everyone Online...by 2030.” *The Register*, September 8, 2015. https://www.theregister.co.uk/2015/09/08/united_nations_to_get_everyone_online_by_2030/.
- McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice*. Novato, CA: Presidio, 1995.
- Melnik, Constantin. “The French Campaign Against the FLN.” Santa Monica, CA: RAND Corporation, 1967.
- Miniwatts Marketing Group. “World Internet Users Statistics and 2019 World Population Stats,” March 2019. <https://www.internetworldstats.com/stats.htm>.
- “Modern Urban Operations: Lessons Learned from Urban Operations from 1980 to the Present.” Asymmetric Warfare Group, November 2016.
- “Modern Urban Operations: Lessons Learned from Urban Operations from 1980 to the Present.” Asymmetric Warfare Group, November 2016.

- Morbach, Gernot W. "Terrorism and Organized Crime: The Alliance of Tomorrow? How to Counter a Possible Future Threat." Master's thesis, Naval Postgraduate School, 1998.
- Murphy, Julia, and Max Roser. "Internet." OurWorldInData.org, 2018. <https://ourworldindata.org/internet>.
- "Nogales Tunnel Task Force, Mexican Authorities Shut down Incomplete Drug Tunnel." Accessed May 8, 2019. <https://www.ice.gov/news/releases/nogales-tunnel-task-force-mexican-authorities-shut-down-incomplete-drug-tunnel>.
- Owen, Mark. *No Easy Day: The Autobiography of a Navy SEAL: The Firsthand Account of the Mission That Killed Osama Bin Laden*. New York, N.Y.: Dutton, 2012.
- Pawlyk, Oriana. "The Days of Secret Military Operations May Soon Be Over. Does That Matter?" Military.com, December 1, 2018. <https://www.military.com/daily-news/2018/12/01/days-secret-military-operations-may-soon-be-over-does-matter.html>.
- Pipes, Richard. *The Degaev Affair: Terror and Treason in Tsarist Russia*. New Haven, CT: Yale University Press, 2003.
- "Population Density for U.S. Cities Statistics." Governing. Accessed November 15, 2018. <http://www.governing.com/gov-data/population-density-land-area-cities-map.html>.
- Rabasa, Angel, Steven Boraz, Peter Chalk, Kim Cragin, Theodore Karasik, Jennifer Moroney, Kevin O'Brien, and John Peters. *Ungoverned Territories: Understanding and Reducing Terrorism Risks*. Santa Monica, CA: RAND Corporation, 2007. <https://www.rand.org/pubs/monographs/MG561.html>. Also available in print form.
- Rothstein, Hy S. *The Art and Science of Military Deception*. London: Artech House, 2013.
- Schenk, Frithjof Benjamin. "Attacking the Empire's Achilles Heels: Railroads and Terrorism in Tsarist Russia." *Jahrbucher Fur Geschichte Osteuropas* 58 (2010): 232–53.
- Schmidle, Nicholas. "Getting Bin Laden: What Happened That Night in Abbottabad." *The New Yorker*, August 8, 2011. https://www.thomasweibel.ch/artikel/110808_new_yorker_getting_bin_laden.pdf.
- Scott-Clark, Cathy. *The Exile: The Stunning inside Story of Osama Bin Laden and Al Qaeda in Flight*. New York: Bloomsbury, 2017.

- Shunk, David. "Mega Cities, Ungoverned Areas, and the Challenge of Army Urban Combat Operations in 2030–2040." *Small Wars Journal*, January 23, 2014. <http://smallwarsjournal.com/jrnl/art/mega-cities-ungoverned-areas-and-the-challenge-of-army-urban-combat-operations-in-2030-2040>.
- Siegel, Jacob. "Could Social Media Blow Special Operations Like the Failed Foley Rescue?" *The Daily Beast*, August 22, 2014. <https://www.thedailybeast.com/could-social-media-blow-special-operations-like-the-failed-foley-rescue>.
- South, Todd. "The Future Battlefield: Army, Marines Prepare for 'Massive' Fight in Megacities." *Military Times*, March 8, 2018. <https://www.militarytimes.com/news/your-army/2018/03/06/the-future-battlefield-army-marines-prepare-for-massive-fight-in-megacities/>.
- Sterling, Christopher H. *Military Communications from Ancient Times to the 21st Century*. Santa Barbara, CA: ABC-CLIO, 2008.
- Sunzi. *The Art of War*. UNESCO Collection of Representative Works: Chinese Series. London: Oxford University Press, 1963.
- Tankel, Stephen. *Storming the World Stage: The Story of Lashkar-e-Taiba*. Oxford: Oxford University Press, 2013.
- "The World's Most Densely Populated Cities." WorldAtlas. Accessed May 9, 2019. <https://www.worldatlas.com/articles/the-world-s-most-densely-populated-cities.html>.
- "Top 5 Cities with the Largest Surveillance Camera Networks." vintechology.com, May 4, 2011. <https://vintechology.com/2011/05/04/top-5-cities-with-the-largest-surveillance-camera-networks/>.
- Tracy, Clint. "Operationalizing Cyber, Electronic Warfare, Space, Special Technical Operations for Decisive Action." *Fires*, 2018, 11–14.
- United Nations. "Pakistan: Population Density (as of 26 August 2013)." United Nations Office for the Coordination of Humanitarian Affairs, August 26, 2013. <https://reliefweb.int/map/pakistan/pakistan-population-density-26-august-2013>.
- United States Army Special Operations Command. "USASOC Strategy—2035," April 2016.
- "US City Populations 2019." Accessed April 29, 2019. <http://worldpopulationreview.com/us-cities/>.
- USSOCOM. "Special Operations Forces Operating Concept: A Whitepaper to Guide Future Special Operations Force Development." USSOCOM, February 1, 2016.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California