



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**WHAT MARINE CORPS STAND-IN FORCES SHOULD
LEARN FROM UKRAINIAN APPLICATIONS OF
COMMERCIAL SATELLITE COMMUNICATION**

by

Dustin M. Soto

June 2023

Thesis Advisor:
Second Reader:

Michael Richardson
Aurelio Monarrez Jr.

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 2023		3. REPORT TYPE AND DATES COVERED Master's thesis
4. TITLE AND SUBTITLE WHAT MARINE CORPS STAND-IN FORCES SHOULD LEARN FROM UKRAINIAN APPLICATIONS OF COMMERCIAL SATELLITE COMMUNICATION				5. FUNDING NUMBERS
6. AUTHOR(S) Dustin M. Soto				
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 ongoing Russo-Ukrainian conflict provides a complex environment for the study of modern warfare. Surprisingly, one of the most intriguing facets of this conflict involves the melding of military operations and the commercial space industry. The Ukrainian military has made use of donated commercial satellite communications terminals with great success and devastating consequences for its Russian adversaries. The mobility, quantity, and range of these systems have aided the Ukrainians in their fight against the Russian Army in each stage of the conflict. Operating within the weapons ranges of Russian forces, the Ukrainian military has leveraged emerging commercial space technology to counter Russian aggression on the battlefield and in the information environment. Coincidentally, the fight being carried out by the Ukrainian Army at times has been similar to the proposed concept for the Marine Corps Stand-In Forces. Given the Ukrainian success in leveraging commercially owned proliferated low Earth orbit (pLEO) satellite communications, the Marine Corps should look to identify applications of their success to its own emerging warfighting concepts. The similarities in the defense of Ukraine and the future of Marine operations make it apparent that the Marine Corps should view commercial satellite communication as a viable solution for Stand-In Forces.				
14. SUBJECT TERMS Ukraine, Marine Corps, communications, PLEO, proliferated, decoys, electronic warfare, deception, expeditionary, tactics, tactical communications, EABO, advanced based operations, stand-in forces, SIF				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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**WHAT MARINE CORPS STAND-IN FORCES SHOULD LEARN FROM
UKRAINIAN APPLICATIONS OF COMMERCIAL SATELLITE
COMMUNICATION**

Dustin M. Soto
Captain, United States Marine Corps
BS, United States Naval Academy, 2017

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS
ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2023**

Approved by: Michael Richardson
Advisor

Aurelio Monarrez Jr.
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The ongoing Russo-Ukrainian conflict provides a complex environment for the study of modern warfare. Surprisingly, one of the most intriguing facets of this conflict involves the melding of military operations and the commercial space industry. The Ukrainian military has made use of donated commercial satellite communications terminals with great success and devastating consequences for its Russian adversaries. The mobility, quantity, and range of these systems have aided the Ukrainians in their fight against the Russian Army in each stage of the conflict. Operating within the weapons ranges of Russian forces, the Ukrainian military has leveraged emerging commercial space technology to counter Russian aggression on the battlefield and in the information environment. Coincidentally, the fight being carried out by the Ukrainian Army at times has been similar to the proposed concept for the Marine Corps Stand-In Forces. Given the Ukrainian success in leveraging commercially owned proliferated low Earth orbit (pLEO) satellite communications, the Marine Corps should look to identify applications of their success to its own emerging warfighting concepts. The similarities in the defense of Ukraine and the future of Marine operations make it apparent that the Marine Corps should view commercial satellite communication as a viable solution for Stand-In Forces.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	SIGNIFICANCE OF THE RESEARCH.....	2
B.	LITERATURE REVIEW	4
C.	OBSERVATIONS AND HYPOTHESIS	8
D.	RESEARCH DESIGN	9
II.	COMMERCIAL PROLIFERATED LOW EARTH ORBIT COMMUNICATIONS	11
A.	WHAT IS PLEO?	11
1.	The P in pLEO	12
2.	Technical Benefits of pLEO	12
3.	Operational Benefits of pLEO	18
B.	CHAPTER SUMMARY.....	19
III.	THE UKRAINIAN CASE STUDY	21
A.	UKRAINE CONFLICT PRE-FEBRUARY 2022	21
B.	UKRAINE CONFLICT POST FEBRUARY 2022	23
C.	ENTER STARLINK.....	24
D.	THE UKRAINIAN CONFLICT TO THE PRESENT DAY	27
E.	RUSSIAN STRUGGLES WITH ELECTRONIC WARFARE.....	30
F.	CHAPTER SUMMARY.....	33
IV.	A MARINE CORPS FOR EMERGING CHALLENGES.....	35
A.	STAND-IN FORCES	36
B.	USMC GCE NEED FOR ASSURED COMMUNICATIONS IN A CONTESTED ENVIRONMENT	38
C.	UKRAINE IN RELATION TO USMC STAND-IN FORCES.....	39
D.	CHAPTER SUMMARY.....	40
V.	APPLICATIONS OF COMMERCIAL SATCOM FROM THE UKRAINIAN CONFLICT FOR THE U.S. MARINE CORPS.....	41
A.	PLEO ARCHITECTURE FLEXIBILITY.....	41
1.	Placing the Enemy in an EW Dilemma.....	42
B.	MOBILITY	43
1.	Speed versus Security	44

C.	LEVERAGING INDUSTRY RESPONSE TO ATTACKS	45
D.	MAINTAINING INFLUENCE	46
E.	ADDITIONAL CONSIDERATIONS	47
1.	Hiding in the Noise.....	48
2.	Deception	49
3.	Policy Support	50
F.	CHAPTER SUMMARY.....	50
VI.	RECOMMENDATIONS AND CONCLUSION.....	51
A.	RECOMMENDATIONS.....	51
1.	Table of Equipment Recommendation	51
2.	Training and Education	51
3.	Integration at Large Scale Exercises.....	52
B.	FUTURE RESEARCH.....	52
1.	Spectrum Evaluations.....	52
2.	Unit Evaluations.....	52
C.	CONCLUSION	53
	LIST OF REFERENCES.....	55
	INITIAL DISTRIBUTION LIST	61

LIST OF FIGURES

Figure 1.	Depiction of Jamming Concepts	17
Figure 2.	Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces.	29
Figure 3.	Russian Advances in March 2022.....	32
Figure 4.	Battlelines September 2022	32
Figure 5.	Idealized Conceptual Depiction of Stand-Off and Stand-In Engagement.....	37
Figure 6.	Starlink Data Usage in Ukraine March to May 2022	47

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C2	Command and Control
COTS	Commercial-Off-the-Shelf
CRAF	Civil Reserve Air Fleet
EMCON	Emissions Control
GEO	Geosynchronous Orbit
GCE	Ground Combat Element
HEO	High Earth Orbit
LEO	Low Earth Orbit
MOS	Military Occupational Specialty
MWX	Marine Air-Ground Task Force Warfighting Exercise
pLEO	Proliferated Low Earth Orbit
SATCOM	Satellite Communication
TCG	Tactical Cellular Gateway
TTP	Tactics, Techniques, and Procedures
USMC	United States Marine Corps
WEZ	Weapons Engagement Zone

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To the Marines of First Platoon, Lima Company and the Marines of 81mm Mortar Platoon, Weapons Company, Third Battalion, Fourth Marines, thank you for your dedication and hard work that allowed me the opportunity to be where I am today.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

There is an adage in the United States Marine Corps (USMC) combat arms military occupational specialties (MOSs) about speed being security, at times noting that the speed of unit, meaning its ability to operate in relation to the enemy, serves as a counterweight to a more aggressive force posture. As we progress into a new age of warfare, where technology and the ability to communicate lead to devastating battlefield effects, it is imperative that we continue to find ways in which to achieve greater speed than our enemies.

The Marine Corps continues to redefine itself. Based on the Commandants' Planning Guidance, it is imperative that the Marine Corps reassesses and redefines its ability to operate in distributed, maritime environments within the weapons engagement zones (WEZ) of potential adversaries.¹ The Marine Corps must recognize that this is uncharted waters, both figuratively and literally. The United States' armed forces may not be able to rely upon all domain dominance when it goes into its next fight. Incomplete dominance in the operating environment calls for a reevaluation of current tactics, techniques, and procedures in preparation for an environment of the unknown. In doing so, the Marine Corps must weigh the costs of traditional operating procedures versus riskier tactics that may go against recognized norms, with the ultimate goal being that the fighting force is able to gain operational speed to action over the enemy.

This thesis evaluates the Marine Corps current tactics and technical procedures (TTPs) towards commercial communication architectures, specifically proliferated low earth orbit (pLEO) satellites, and provide evidence as to the efficacy of their use on the battlefield. The ongoing war in Ukraine, offers a revealing case study of the potential significance of pLEO on tomorrow's battlefield. Operating much like the Commandant's Planning Guidance envisions the future Marine Corps, the Ukrainian Armed Forces have been able to grind the Russian bear to a standstill, thanks in part to the interconnected targeting networks their army established blending a mix of commercial-off-the-shelf

¹ U.S. Marine Corps, *Commandant's Planning Guidance* (Arlington, VA: U.S. Marine Corps, 2019).

(COTS) capabilities and devastating fire support.² Furthermore, the same conflict demonstrated how commercial satellite communication (SATCOM) architectures have stymied traditional superpowers due to their expansive size, responsiveness, and adaptability. Finally, the invasion of Ukraine demonstrates that these communications architectures have served as an undeniable tool for fighting on the frontlines of the information war.

A. SIGNIFICANCE OF THE RESEARCH

While the United States enjoys a period of relative peace after the end to the global war on terror, countries across the world continue to prepare and increase their prospects of success against the United States given a large-scale conflict. Many envision that the first phases of a potential future conflict among peer adversaries would involve the significant degradation of command-and-control networks.³ Specifically, this refers to the current SATCOM architecture that provides coverage for all facets of the U.S. military.⁴ If this future conflict were to continue as predicted, thousands of U.S. troops would be left without the ability to communicate across the various levels of command as military and civilian leadership struggled to coordinate operations with limited remaining military SATCOM. This lapse in control potentially gives the enemy a relative speed advantage to strike while U.S. forces are disoriented and without guidance. As such, there is an obvious need for a more robust communication architecture that fills an immediate gap if traditional SATCOM providers are targeted.

My background as an infantry officer, drives me to focus on the men and women who remain on the frontlines of battlefields. To prepare for future conflicts, the Marine infantry units who operate at the forward edge of the battlefield are training continually for

² Seth G. Jones, Riley McCabe, and Alexander Palmer. “Ukrainian Innovation in a War of Attrition,” Center for Strategic and International Studies, February 27, 2023. <https://www.csis.org/analysis/ukrainian-innovation-war-attribution>.

³ Mark K. Jbeilly “Satellites in the Crosshairs,” *Proceedings* 147, no. 6 (June 2021). <https://www.usni.org/magazines/proceedings/2021/june/satellites-crosshairs>.

⁴ Stephen Losey. “Military Must Train to Fight When Communications Break Down: Experts.” *Defense News*, April 24, 2023. <https://www.defensenews.com/battlefield-tech/2023/04/26/experts-military-must-train-to-fight-through-communications-breakdown/>.

operating in heavily contested environments. A reemphasis on camouflage and emissions control (EMCON) has made its way throughout the operating forces. Despite these unit's best efforts, they are still tethered to large communication nodes in order to receive tasking and guidance. Units are warned in large scale training exercises that the enemy is all seeing and all sensing, capable of quickly finding and targeting friendly forces based on their dominance of the electromagnetic spectrum. At the same time, an ocean away, our Ukrainian allies are progressively modeling themselves more and more after the United States military, including synchronizing complex weapon systems as part of kill webs even while remaining elusive to their Russian counterparts. Time and again we read or hear of frontline Ukrainian infantry units successfully integrating unmanned aerial systems with long range fires to support conventional combat units in both offensive and defensive operations. Even more remarkable, during the initial phases of the invasion, Ukrainian infantry, special operations, and territorial defense units masterfully demonstrated skill in conducting distributed operations in defending key cities from the Russian invaders.⁵ To any observer, the Ukrainian military is beginning to look more and more like its counterparts in the United States in both appearance and practice. Yet, for as much emphasis placed on enemy electronic and information warfare in the United States, the Ukrainian military has not appeared to be greatly hindered by these capabilities.

For all intents and purposes, prior to February 2022, Russia was seen as a preeminent competitor to the United States, capable of matching many of the capabilities the United States could bring to bear militarily. Nonetheless, an army that was predicted to be defeated in three days has fought effectively and valiantly for more than a year in the defense of their homeland. As of May 2023, the Ukrainian military stands poised to take back more of their subjugated country. In my opinion, besides stalwart bravery and tenacious patriotism, the United States Marine Corps can take many lessons from the Ukrainian Conflict specifically in regard to the Ukrainian military's creativity and willingness to assume risk.

⁵ Michael G. Anderson, "How Ukraine's Roving Teams of Light Infantry Helped Win the Battle of Sumy: Lessons for the U.S. Army." Modern War Institute, August 17, 2022. <https://mwi.usma.edu/how-ukraines-roving-teams-of-light-infantry-helped-win-the-battle-of-sumy-lessons-for-the-us-army/>.

Given the interconnectedness of the world in 2022 and overall shock of the Russian invasion, the Ukrainian government was able to acquire hundreds of Starlink satellite terminals in the opening days of the conflict and rapidly integrate them into their military command and control (C2) structure. Overnight, Russian attempts at isolating Ukraine from the global community and limiting their military's control of forces crumbled. The Ukrainian capacity to mesh the capabilities of high-end commercial SATCOM equipment into their military system offers many avenues for the Marine Corps to explore. It does not take much imagination to see the similarities in the efforts of the Ukrainian Army in the early days of the war with the mission of the Marine Corps Stand-In Forces (SIFs) as described by the Commandant of the Marine Corps, General James Berger in his *Force Design 2030*⁶ and *A Concept for Stand-In Forces*.⁷ It is imperative that the Marine Corps take the appropriate lessons from ongoing conflicts and encourage creativity among Marines to adapt those lessons learned in the current operating forces. This thesis explores the positives and negatives of the Ukrainian case study through the lens of a Marine Corps prepared to serve as SIFs and conduct highly distributed operations as envisioned by the current force design guidance.

B. LITERATURE REVIEW

Prior to the Russian invasion of Ukraine, much of the work written regarding communications and their employment for the next war was purely theoretical. Even in the early stages of the conflict, many observers did not expect to glean much from ongoing battles. It was expected that Ukraine would be defeated in a matter of days. Yet, overnight, on the whim of a tweet, Ukraine was rapidly equipped with the capability of conducting communication via space systems, a luxury previously reserved for world powers. Because of the ongoing nature of the conflict, little has been written academically in regard to communications on the front lines. At the same time, however, the conflict has been heavily documented due to the implementation of social media and messaging campaigns by the

⁶ U.S. Marine Corps, *Force Design 2030* (Arlington, VA: U.S. Marine Corps, March 2020)

⁷ U.S. Marine Corps, *A Concept for Stand-In Forces* (Arlington, VA: U.S. Marine Corps, December 2021).

Ukrainian government.⁸ While specifics have not yet been written for the Ukrainian implementation of pLEO SATCOM, much has been written describing the factors that facilitate the use of commercial satellite internet providers at a tactical level.

Starting in the early 2000s, militaries followed global trends and became more and more networked; identifying a need to link warfighters to increased combat power through information technologies. Scholars began to approach the concept of merging civilian capabilities with military requirements. In the books *Tactical Communications for the Digitized Battlefield* by Michael Ryan and Michael Frater, and *Tactical Wireless Communications Networks* by George Elmasry, the authors identify benefits in the use of both cellular networks and satellite communications. However, when these books were published, for the tactical user, these were seen as completely different entities. Today, humans have achieved the ability to combine personal communication devices with satellite provided internet services through the use of internet service providing pLEO satellite constellations. The trend towards pLEO is something of a new idea in and of itself. For example, Ryan and Frater discuss the disadvantages that LEO constellations inherently have in their book, claiming that “an increased requirement for handover and the large number of satellites required [to operate a LEO constellation]” are detrimental to their military application.⁹ This way of thinking has in fact reversed almost completely. As technology has progressed and costs have decreased, the military has consistently looked to pLEO as the future of military SATCOM.¹⁰

In contrast, Elmasry’s work on wireless communications provides an in-depth discussion on the implementation of tactical cellular networks for frontline troops. He addresses the concerns and vulnerabilities of implementing COTS cellular technologies in a tactical environment, elaborating on the needs for security while advocating for

⁸ Stephen Fidler and Thomas Grove. “Smartphones Are Changing the War in Ukraine.” *Wall Street Journal*, February 16, 2023. <https://www.wsj.com/articles/smartphones-are-changing-the-war-in-ukraine-adb37ba1>.

⁹ Michael J. Ryan and Michael R. Frater. *Tactical Communications for the Digitized Battlefield*. (Boston, MA: Artech House, 2002), 79.

¹⁰ “US Military Places a Bet on LEO.” *Satellite Today* (June 3, 2021). ProQuest.

distributed operations.¹¹ He proposes a Tactical Cellular Gateway (TCG) to address some of the security concerns while also allowing for flexibility in implementation. In a generic ground combat unit, Elmasry envisions the TCGs at the company level, reaching back to a TCG at the battalion level, and subsequently the brigade level until it finally reaches the root service provider.¹² At the surface level, this sounds similar to what has been seen in Ukraine. However, due to the available technology at the time of writing, his models require significant reach back to the core 3G/4G/LTE service providers.¹³ As will be discussed later in this thesis, the benefits of modern pLEO technology eliminate much of this reach back, rendering the models obsolete by allowing frontline units a much shorter link between forward and rear units. Given the progression in commercial and military SATCOM technology, frontline troops on modern battlefields have the root service provider on the frontline which ultimately increases flexibility and decreases the architecture size required for robust, persistent communications.

While these two books provide insight into the technical specifications required to maintain a network-based military, a study titled *Army Network-Enabled Operations* published by RAND addresses the fact that network-based military communications are here to stay. This study addresses the efficacy of these networks in the wars in Iraq and Afghanistan.¹⁴ One of the recommendations in the RAND study was to “continue to expand efforts to extend the network to lower echelons.”¹⁵ The author explains that given the resources and natures of those conflicts, frontline forces often experienced limited network capabilities or network access.¹⁶ Because of the deployments of platoons in remote combat outposts, units often lacked the direct access to intelligence, surveillance,

¹¹ George F. Elmasry, *Tactical Wireless Communications and Networks*. (Hoboken, NJ: John Wiley and Sons, Ltd. 2012.), 261–274.

¹² Elmasry, *Tactical Wireless Communications and Networks*, 265.

¹³ Elmasry, *Tactical Wireless Communications and Networks*, 264.

¹⁴ Timothy M. Bonds et al., *Army Network Enabled Operations*. (Santa Monica, CA: RAND Corporation, 2012).

¹⁵ Bonds et al., *Army Network Enabled Operations*, 119.

¹⁶ Bonds et al., *Army Network Enabled Operations*, 119–120.

and reconnaissance data they sought for mission accomplishment.¹⁷ They also explain how due to accessibility and availability issues, soldiers and leaders often made informal networks to share information across units and commands given the resources that they were able to access from their remote positions, thus circumventing formal military information networks in order to achieve mission success.¹⁸ From personal experience, I can attest to the use of informal networks to achieve success in Afghanistan. My unit used civilian satellite imagery to provide maps on the tablet devices used for tactical planning and C2 because we did not have access to government procured imagery. The lessons learned in this RAND study, along with personal experience, identifies a shortfall in the ability to provide frontline units with real time data and network integration. In the coming chapters it will become apparent how the Ukrainian military identified a solution to this issue using commercially available network providers. This is something that the Marine Corps should take note of as it continues to shift focus towards operating in remote environments.

Current literature on military use of pLEO satellites focuses mostly on the shift from large, highly capable satellites in geosynchronous orbit (GEO) to the more modular pLEO satellites.¹⁹ The Department of Defense (DOD) has taken note that Low-Earth Orbit offers advantages in communications, missile warning, and other missions. It appears that a joint commercial space industry-DOD path forward is a way to successfully create a pLEO infrastructure capable of meeting future SATCOM challenges. At the same time, at the tactical level, the understanding of the benefits of commercial SATCOM remains limited. A previous Naval Postgraduate School thesis titled “Using Commercial 5G and LEO Technologies to Enhance Navy-Army Sensor-to-Shooter Networks” is one of the few discussing the tactical employment of commercial SATCOM. In the thesis, the authors made clear the speed of LEO communication outweighed other variables found in current options available for linking sensors and shooters. From a data rate perspective, the thesis

¹⁷ Bonds et al., *Army Network Enabled Operations*, 117.

¹⁸ Bonds et al., *Army Network Enabled Operations*, 117.

¹⁹ *Satellite Today*, “US Military Places a Bet on LEO.”

validated that LEO has higher speeds than traditional military communications.²⁰ With that being said, there is little available that validates the potential implementation of commercial pLEO SATCOM at a tactical level. In order for ground combat elements to employ these emerging assets to their full potential, an in-depth evaluation of current best practices is needed.

It is apparent that there are gaps at the tactical level when it comes to truly integrating units into the network centric operating environment. With an understanding of the current capabilities of satellite provided internet and an evaluation of the Ukrainian employment of the pLEO Starlink constellation, this thesis will offer a potential solution for these gaps in communications capabilities. Furthermore, it will identify benefits of the use of commercial capabilities while also addressing some of the vulnerabilities of commercial services.

C. OBSERVATIONS AND HYPOTHESIS

The ongoing conflict in Ukraine demonstrates a unique hybridization of traditional warfare and information warfare. One of the immediate priorities of the Ukrainian government was maintenance of their connections to the outside world via the internet. One can presume that this will remain the norm for any future conflict. Maintenance of connectivity via the internet was twofold; it not only allowed for command and control of distributed Ukrainian units, at the same time by giving the Ukrainian government a lifeline to the outside world, it prevented the Russians from dictating the narrative of the conflict.²¹ This aided the Ukrainian government in rallying allies to its cause and gave civilians the ability to aid in intelligence gathering and information sharing. The Ukrainians should be applauded for identifying the need for persistent internet access early and seeking creative ways to use this tool in the defense of their country on these two fronts.

²⁰ Jonathan S. Dodge, and James G. Carlton. "Using Commercial 5G And LEO Technologies To Enhance Navy-Army Sensor-To-Shooter Networks." (Master's Thesis, Naval Postgraduate School, December 2022), <https://hdl.handle.net/10945/71449>.

²¹ Hope Hodge Seck. "Ukraine Lessons Take Center Stage in Marines' New Information Warfare Plan." *Marine Corps Times*, June 29, 2022. <https://www.marinecorpstimes.com/news/your-marine-corps/2022/06/29/ukraine-lessons-take-center-stage-in-marines-corps-new-information-warfare-plan/>.

While it is true that communications by commercial communications satellites do not offer the same assuredness and integrity of military grade systems, the flexibility provided by their physical architecture and the regular improvements driven by consumer demand is astounding. The continued growth of commercial SATCOM has applications that could enhance military capabilities. As the Marine Corps sifts through an era of experimentation and redesign, commercial SATCOM is a technology that should be further explored. By comparing the Marine Corps' potential employment of stand-in forces, with the early stages of the Russian invasion of Ukraine, it can be readily seen that the use of commercial pLEO systems offer successful implementation that could be replicable in combat situations.

Given a proper understanding of the risks and benefits of commercial pLEO communications, the sky is the limit for the capabilities that they can provide. While there are inherent risks to using commercial capabilities for military operations, it is imperative to understand that given the shifting thresholds of violence and gray zone conflicts, a reevaluation of the Marine Corps potential utilization of commercial communications is required. The ability to have assured communications among distributed units is a must for the types of complex kill chains and kill webs expected on tomorrow's battlefield. Given their robust worldwide networks, commercial communications do just that. Furthermore, because of their presence worldwide, commercial communications offer an opportunity to "hide in the noise," using indigenous networks and civilian signals emissions as cover for military communications in environments where Marines are tasked with minimizing their signals emissions profile. Finally, the simplicity and availability of commercial communication equipment provides an ample opportunity for the implementation of tactical electronic warfare deception, a capability that is currently lacking.

D. RESEARCH DESIGN

In conducting my research, I chose to do a comparative analysis of the ongoing Ukrainian conflict and the future operating concepts as explained in *Force Design 2030* and a *Concept for Stand in Forces*. The Ukrainian conflict is one of the most well documented of all time, thanks in part to social media and internet connectivity. Moreover,

the operating models described in *Force Design 2030* and *A Concept for Stand in Forces* are still in their experimentation and validation phases with the United States Marine Corps. Because of the active, well documented aspects of both cases, I was able to draw conclusions between the two situations. By analyzing the conclusions from Ukraine and comparing them to the Marine Corps Stand-In Force model, I was able to come up with the pros and cons of commercial SATCOM use for within Marine Corps formations. Finally, I provide recommendations and potential employment opportunities for commercial satellite usage based on lessons drawn from the Russian invasion of Ukraine and the inherent characteristics of satellite provided internet services.

II. COMMERCIAL PROLIFERATED LOW EARTH ORBIT COMMUNICATIONS

Satellite communications are not a new concept. The first communications satellite broadcast a message from President Eisenhower in 1958 and the United States has remained a leading figure in this field since its inception.²² However, as technology continues to outpace military procurement, newer and more complete options for SATCOM have permeated the atmosphere from out of the commercial sector. Leading tech companies are looking to provide satellite-based internet and other communications around the globe by leveraging creative solutions, lower costs, and government cooperation. The goal of communication providers remains the same: provide affordable, quality coverage to the greatest number of people. Since the first satellites, design and functionality of satellites has remained relatively the same; large, expensive satellites are designed to provide a robust spectrum of capabilities. These systems are usually designed to work in small constellations made up of highly complex satellites in order to provide the necessary coverage. Until recently, this has been the prevailing practice and has worked quite well. However, with the increase of technology and the growing commercialization of space, novel approaches have been taken to reassess how we view space-based communications.

A. WHAT IS PLEO?

In order to describe pLEO, it is important to first differentiate between the existing orbits utilized by current manmade objects in space. Most orbits generally fall into three categories: high earth orbit (HEO), low earth orbit (LEO), and geosynchronous orbits (GEO). Usually, a satellite's orbit is determined by its mission set, with each orbit offering distinct characteristics and benefits. Current communication providing satellites tend to use GEO and HEO orbits because they offer more ground coverage. While coverage is greater, the cost to place a satellite in HEO and subsequently run it for the remainder of its mission is highly expensive. This has resulted in few, highly expensive satellites providing large

²² Gary D. Gordon. *Principles of Communications Satellites*. (New York, NY: John Wiley and Sons, Inc., 1993).

amounts of coverage. Recently, however, this practice has changed. LEO has quickly become the direction in which many companies and space agencies are narrowing their focus. By limiting the altitude at which the satellites orbit, companies are able to save money on the cost of launches and maintenance. This results in money for more satellites, providing more opportunities to provide the same coverage as a HEO satellite.

1. The P in pLEO

Within the last 10 years, the concept of Proliferated Low Earth Orbit has grown exponentially. Eschewing traditional concepts of satellite employment, pLEO looks to leverage an increasingly more accessible space domain and continually decreasing costs to saturate LEO with thousands of small, specially designed satellites that can execute specifically tailored missions. One benefit of pLEO constellations is the almost assured capability to provide truly global coverage at any given time. Because of the large constellations, satellites can provide redundant service meaning if one satellite fails to operate properly, another satellite can take its place in providing the necessary signal.²³ This redundancy is extremely beneficial by expanding the resiliency and assuredness of the service provided. The large number of satellites in space also pays dividends for users on the ground. Thanks to the expansive networks in LEO, operators on the ground are able to have almost guaranteed clear transmit and receive capabilities to hundreds if not thousands of satellites. This makes operation on the ground very simple. Operators are merely required to have small, highly mobile antennas that provide connection to overhead satellites. As the satellites move through their orbits, connection is passed from one to another, providing seamless service throughout a session.

2. Technical Benefits of pLEO

As space domain technology continues to grow, it is important to understand the technical justifications for employing pLEO satellites rather than traditional GEO or HEO

²³ “FAQ – Space Development Agency.” Space Development Agency. Accessed May 1, 2023. <https://www.sda.mil/home/about-us/faq/>.

spacecraft. The Space Development Agency (SDA) summarizes some of the technical benefits in the following justification for the expanded use of Low Earth Orbit satellites:

Low Earth orbit offers a number of benefits when compared to orbits of higher altitude, including less expensive orbit insertion, better viewing geometries for space-based earth observation, and lower latencies and power requirements for communications transmissions to terrestrial systems. For these reasons, there has also been an emergence of technology providers in the commercial sector seeking to deliver communications capabilities through satellite constellations in LEO. These are some of the reasons why SDA will initially proliferate capabilities in LEO.²⁴

Communication effectiveness is dictated by many factors of the physical world. Satellite communication requires an understanding of factors that limit the effectiveness of transmitting and receiving, especially over the large distances required to reach systems in space. The link budget is the equation and analysis conducted to explain the ability of a satellite to carry out its role as a communications link.²⁵ Understanding the factors that make up the link budget ensure that we are able to achieve a signal to noise ratio (SNR), the ratio between the signal transmitted to the noise interference, that is satisfactory for our communications system. pLEO satellites offer advantages in this realm that traditional GEO or HEO satellites do not. Specifically, from a military perspective, the ability to utilize lower power requirements and achieving lower latencies are characteristics that can provide significant advantages on the battlefield. The following sections will provide technical verification of these assertions.

a. Radar Range Equation

In order to understand the benefits of pLEO SATCOM on a battlefield, it is important first to understand the equations that go into the technical characteristics of communications. A simplified version of the radar range equation is given as follows:

²⁴ Space Development Agency, “FAQ – Space Development Agency.”

²⁵ Gordon, *Principles of Communications Satellites*, 56.

$$P_r = \frac{P_t G_t G_r \sigma \lambda^2}{(4\pi)^3 R^4}$$

This formula describes the factors that go into the power received by an antenna, P_r . In the case of this thesis, that antenna serves as either a pLEO satellite or subsequent ground station. Furthermore, because there are a variety of SATCOM options available this section will focus not on the engineering aspects of the devices, but rather the ways in which a LEO orbit cause increases in the power received and the tactical benefits that come of that. The focus will be on how the decrease in altitude of the pLEO satellites results in a lower R value, where R is the range between transmitter and receiver.

In comparison to GEO or HEO satellite constellations, LEO satellites have significantly lower altitudes. According to the textbook *Principles of Communications Satellites* LEO constellations operate at an altitude between 500 to 2000 kilometers.²⁶ In comparison, GEO satellites operate at an altitude of 35,786 kilometers while HEO satellites are beyond even that.²⁷ Understanding the ways in which the decrease in range affects this equation are instrumental in the argument for the benefits of pLEO SATCOM.

b. Decreased Satellite Link Delays

Perhaps the simplest benefit of the difference in altitude between orbits is the change in the link delays between receiver and transmitter. As mentioned in the previous Space Development Agency quote, a decreased delay results in the lower latency that pLEO benefits from. A signal between a transmitter and receiver, moving at the speed of light, still takes time to travel the physical distance between the two. In the following equation that describes this delay:

²⁶ Gordon, *Principles of Communications Satellites*, 56.

²⁷ Gordon, *Principles of Communications Satellites*, 56–57.

$$t = \frac{S}{c} \quad (\text{seconds})$$

t is equal to time in seconds while S and c are the distance between transmitter and receiver and the speed of light, respectively.²⁸

While still small, the difference in milliseconds between LEO or GEO satellites could result in grave consequences on the battlefield. The modern battlefield continues to demonstrate the necessity for attaining speed in relation to the enemy in order to coordinate, strike, and displace before their electronic warfare or other sensors are able to target friendly positions. By minimizing the time required to actively transmit and receive, pLEO SATCOM increases the survivability of operators even in an environment with a currently more and more compromised electromagnetic spectrum.

c. Smaller Transmit Power Requirements

Another facet of the decreased range between ground station and satellite is the relationship between power transmitted, P_t , and power received, P_r in the radar range equation. By decreasing R , we are able to decrease P_t in the equation while not sacrificing the power received from the transmitter in our system. It is readily apparent that Power received by a transmitter is directly proportional to the distance that a signal is required to cover. At the same time, if a threshold P_r is set by an operator, given a fixed altitude of a satellite, there is an allowable range in transmit power that can achieve the necessary effects.

In a military application, the ability to reach a satisfactory received power level while operating at lower transmit power levels is often a valued tactic for operating in emission-controlled environments. The Marine Corps EMCON standard operating procedure specifically recommends operating all radios and transmitting devices at the lowest power levels allowable for mission success in order to hide electronic signatures from enemy forces.²⁹ By referencing the radar range equation, we can understand that pLEO SATCOM, due to its closer proximity to ground terminals, offers an opportunity to

²⁸ Gordon, *Principles of Communications Satellites*, 56–57.

²⁹ U.S. Marine Corps, *EP EMCON SOP: A Guide to Reduce Technical Signature* (Virginia Beach, VA: Marine Corps Intelligence Schools, 2020), 2–20.

exploit the relationship between range and lower transmit power while ultimately still achieving the effects needed by friendly forces.

Furthermore, by decreasing power requirements for transmitting to and from satellites, this opens up more avenues for the operator on the ground. Because the end user can operate at lower power levels, pLEO SATCOM terminals are able to be operated from a variety of power sources. In Ukraine specifically, vehicles, generators, and normal civilian power grids have been utilized to power Starlink terminals.

d. Flexibility Against Jamming

A function of the Power Received by a transmitter is the signal to noise ratio (SNR). The SNR describes the signal that arrives at a receiver in comparison to the noise, or interference, that the transmission experiences due to natural and man-made causes. Noise acts as a destructive agent, impairing the receipt of a transmission. While communication systems are designed to ensure that the power received is greater than the loss due to noise, the phenomenon can be weaponized as a form of electronic warfare. Jamming, or the introduction of artificial noise into a communication system, is a more and more commonplace electronic warfare measure seen on the modern battlefield.

Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations*, defines electromagnetic jamming as the “deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing [one’s] effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing [one’s] combat capability.”³⁰ With this in mind, a simplified mathematical explanation of jamming equates to an additional artificial noise factor, caused by a deliberate influx of electromagnetic energy, added to the noise captured in the SNR.³¹ This effectively inhibits the signal a receiver captures and degrades communication efficiency.

³⁰ Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations*, JP 3-85 (Washington, DC: Joint Chiefs of Staff, 2020), I-7. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

³¹ Poisel, Richard A. *Information Warfare and Electronic Warfare Systems*. Artech House Electronic Warfare Library. (Norwood: Artech House, 2013), 332.

Figure 1 depicts the injection of a noise signal into a communications link. The depiction demonstrates the jamming process. For the case of pLEO SATCOM, the transmitter is potentially one of hundreds or thousands that can transmit to multiple receivers on the ground. To be effective, jamming efforts would require precise targeting or large amounts of power.

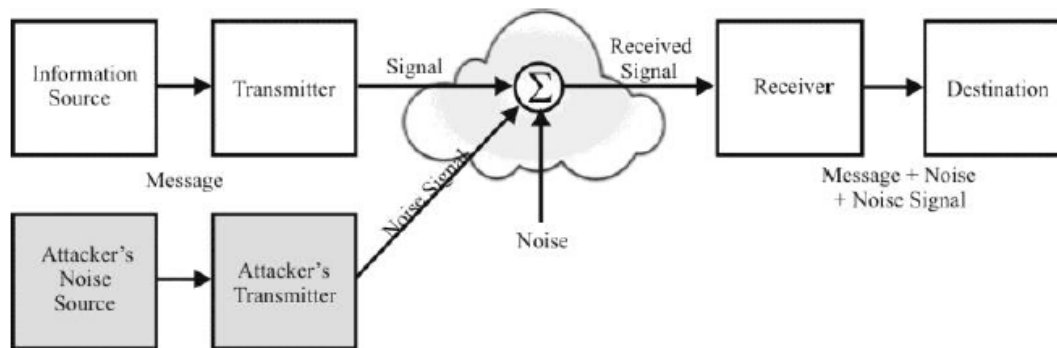


Figure 1. Depiction of Jamming Concepts³²

Information Warfare and Electronic Warfare Systems by Richard A. Poisel dives deep into the considerations that must be undertaken when employing jamming. Two of these considerations are directionality and power. He explains that jammers are only as effective as their ability to direct electromagnetic energy on a specific target.³³ Following the same principles expressed earlier in the radar range equation, it is clear that in order to jam a target, large amounts of power are required to be focused on a specific target or range needs to be decreased. This is where a communication system like pLEO SATCOM greatly benefits the operator. With thousands of emitters in the atmosphere and potentially hundreds of terminals on the ground, the enemy is forced to focus its jamming efforts on a specific target. In the case of these pLEO constellations, they are already designed to quickly hand-off transmission responsibilities due to the nature of their orbital mechanics. In a jamming situation, this simply means that an alternate spacecraft takes the place of the

³² Poisel, *Information Warfare and Electronic Warfare Systems*, 274.

³³ Poisel, *Information Warfare and Electronic Warfare Systems*, 273–274.

jammed system. Furthermore, if the enemy elects to jam the ground stations rather than the spacecraft, the power requirements and proximity required to achieve effects require a potentially deadly decision. To achieve the desired effects, the enemy must get close enough to the front lines to be identified and targeted, while drawing large amounts of power, factors that open the door for friendly force targeting. This is the crux of an effort the Commandant of the Marine Corps refers to as the Reconnaissance and Counter-Reconnaissance Fight which will be discussed later in this thesis.

3. Operational Benefits of pLEO

pLEO satellites provide globally accessible, space-based internet services. While the previous section discussed the technical benefits of these internet providing systems, this section delves into the operational benefits. In its current capacities, a physical connection is required to an internet service provider in order to access the internet. This can be achieved through cable or fiber optic connections and sometimes large antenna relays for access in remote environments. As is easy to imagine, this equates to relatively stationary and localized access. Even cellularly provided internet services require accessibility to large cellphone towers to function properly.³⁴ Subsequently, internet access, while readily available in areas with well built-up infrastructures, is still a rare commodity in remote regions of the world. This, however, is rapidly changing with the introduction of pLEO internet service providers.

As has been discussed previously, the concept of satellite provided communications are not new or revolutionary. Previously, though, because constellations were so finite and latency was poor, these providers were expensive and inconsistent in the services provided.³⁵ While frustrating, this helped manage the large numbers of people who would hope to use SATCOM for their daily lives. pLEO SATCOM brings a fresh new take to this field. As was discussed in the previous section, by understanding simple latency

³⁴ Rose Qingyang Hu and Yi Qian. *Heterogeneous Cellular Networks* (Hoboken, NJ: John Wiley and Sons Ltd, 2013) Chap. 1, 1–25. <https://doi.org/10.1002/9781118555262.ch1>.

³⁵ Richard VanderMeulen, and Bruce Cathell. “High Capacity Satellite Communications- Cost Effective Bandwidth Technology.” (Presentation, 31st Space Symposium, Colorado Springs, CO, April 2015).

calculations, it is apparent that pLEO internet services are faster and due to the larger number of spacecrafts, more readily available. Impressively, this new approach has already quickly made SATCOM provided internet more readily accessible in all corners of the globe. Places that previously struggled to maintain connections to internet infrastructures now do not face the same struggles that they did previously. The introduction of one terminal into a region immediately generates enough bandwidth for up to 128 people to access high speed internet. Users can connect cell phones, laptops, and any other internet protocol devices quickly to the worldwide web.

With this understanding, it is important to focus on the fact that remote areas, those that often find themselves at the forefront of military action, will soon have access to internet capabilities at a level not previously seen. For example, in nations like Palau, where many tiny islands make an archipelago of a nation, high speed internet will soon be available throughout the country without a reliance on complex infrastructure that each individual island would need to support in order to provide internet access. Another example would be in remote areas of underdeveloped nations like Afghanistan. The cost per terminal is far lower than the investment required to build and maintain normal internet-providing infrastructure. The growth of pLEO satellites and the services they provide will result in drastic changes towards internet access across the world. The United States and the military will need to be ready to meet this changing environment head on.

B. CHAPTER SUMMARY

The growth of commercial pLEO satellite systems offer a multitude of advantages that enhance military capabilities. In short, pLEO constellations significantly decrease latency rates between transmitters and receivers while also providing flexibility in the event of adversary interference. Ultimately, this provides operators with an ability to limit power requirements while simultaneously circumventing enemy EW actions yet still maintaining high power requirements. Additionally, the growth of this technology will afford connectivity in traditionally remote regions, enabling a truly worldwide communication architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE UKRAINIAN CASE STUDY

In recent years, the United States began a much-awaited shift in focus towards emerging threats in the form of near-peer and peer adversaries. With only assumptions to operate off, the United States' military began its planning for future conflicts with the information that it had readily available. Services, like the Marine Corps, identified that the structure and missions of the institution needed dramatic changes in order to compete in the contemporary operating environment. With little concrete evidence available, the service quickly adapted itself as it saw fit for its next mission. In the opinions of many former officers, the Marine Corps could not properly explain its decisions to drastically cut traditional battlefield combat power in the form of tanks and cannon artillery. It is my belief that the ongoing war in Ukraine justifies these decisions, as seen by the undersized Ukrainian Army's ability to overwhelm the traditionally perceived Russian juggernaut via a complex formula of network creativity, advanced weaponry, and the will to fight. At the root of this success was the Ukrainian ability to organize and maintain communication during the churning Russian advances of February 2022. This was in part thanks to the readily available communications networks established by civilian providers.

A. UKRAINE CONFLICT PRE-FEBRUARY 2022

Prior to the outright invasion in 2022, Ukraine and Russia had been fighting a prolonged conflict in the Eastern portion of Ukraine known as the Donbass. Evaluation of this protracted, relatively static conflict ultimately resulted in many of the assumptions made with regards to cell phone usage on the battlefield. Given the relatively confined battlespace and minimal commitment of Russian ground forces, the Russian military was able to operate its vaunted electronic warfare assets with impunity.³⁶ As such, given a Ukrainian lack of secure radios and static lines of combat, the Ukrainians found themselves

³⁶ Duncan McCrory. "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States." *The RUSI Journal* 165, no. 7 (November 9, 2020): 34–44. <https://doi.org/10.1080/03071847.2021.1888654>.

subject to intense Russian electronic warfare and information operations.³⁷ From geolocations, interception, and deception campaigns, the Russians leveraged multiple avenues of electronic warfare against their Ukrainian foes.

It is necessary to evaluate enemy tactics, techniques, and procedures based on their employment within a specific operating environment. Of note, the battle lines from 2014 to 2022 were, for the most part, stagnant. This allowed for a robust complex system of electronic warfare and signals intelligence systems to establish and collect on Ukrainian forces.³⁸ Like in any collections effort, periods of little to no change, allow for the establishment of a baseline understanding of the battlefield's electronic environment. The static nature of the conflict aided Russian collections of commercial cellular signals due to the fact that the same operators, operating the same devices, in the same area for extended periods of time relied solely on cellular data for communication between positions as well as back home to their families.³⁹ Because of the well-developed collections efforts and established baseline, Russians were able to isolate individual key leaders as well as intercept communications and geolocate positions. The Ukrainian forces, in turn, used similar tactics against the Russians themselves. In fact, Russian cellphone data was used to corroborate the presence of Russian soldiers on the front line, as opposed to the “little green men” as claimed by the Kremlin.⁴⁰

Without surprise, many observers around the world drew lessons from soldiers' testimonials and observation of the type of combat conducted in the region. The United States Marine Corps' Signature Management Handbook, specifically cites instances of Russian electronic warfare in Ukraine as reasons to limit personal electronic devices in

³⁷ Roman Horbyk. “The War Phone’: Mobile Communication on the Frontline in Eastern Ukraine.” *Digital War* 3, no. 1 (December 1, 2022): 9–24. <https://doi.org/10.1057/s42984-022-00049-2>.

³⁸ McCrory, “Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States,” 36.

³⁹ Horbyk, “The War Phone’: Mobile Communication on the Frontline in Eastern Ukraine,” 13.

⁴⁰ Bellingcat Investigation Team. “How EchoSec Found Evidence of a Russian Fighting in Ukraine.” Bellingcat, February 19, 2015. <https://www.bellingcat.com/news/uk-and-europe/2015/02/19/how-echosec-found-evidence-of-a-russian-fighting-in-ukraine/>

combat entirely.⁴¹ However, unlike the Ukrainian army during this period, the Marine Corps does not subscribe its troops to attrition style, static warfare. Marine Corps doctrine encourages rapid, maneuver centric combat, utilizing speed and efficiency to keep the enemy from operating how it desires. It cannot be stressed enough that the dangers in the reliance on commercial communication assets stem from static fighting and the reliance on traditional, fixed cellular network architectures. In the next sections, the case will be made that the introduction of highly mobile and adaptable internet services provided by commercial SATCOM has become a game changer for the Ukrainian Army. As will become apparent in the next section, an evaluation of the Ukrainian Army's response to the overt Russian invasion of their territory in February 2022 shows that the pairing of civilian communication architectures and the integration of creative, distributed operations resulted in novel successes that thwarted Russian advances. The Marine Corps should learn from these actions, particularly because the operational method employed by Ukrainian forces is similar to that espoused in *Force Design 2030*.

B. UKRAINE CONFLICT POST FEBRUARY 2022

On February 24, 2022, the Russian Army invaded the sovereign nation of Ukraine from multiple directions and engaging on multiple fronts. Based on their observations of the Russian force build up and intelligence updates from allied countries, the Ukrainians immediately began to execute a well-planned and coordinated defense of their country. As the Russians came hurtling out of Belarus towards Kyiv, Ukrainian military units, hand in hand with local territorial defense forces, wreaked havoc on the large, immobile convoys and armored formations that made up the power of the Russian invasion force.⁴² The same actions were being taken across the country, specifically in the vicinity of the cities Sumy and Kharkiv to the East.⁴³ Interestingly, despite the predictions of many Western pundits, Ukraine did not fall within the three days that many expected, but rather executed a staunch defense that continues to this day. As many may remember, in the immediate aftermath of

⁴¹ U.S. Marine Corps, *EP EMCON SOP: A Guide to Reduce Technical Signature*, 2–16.

⁴² Anderson, "How Ukraine's Roving Teams of Light Infantry Helped Win the Battle of Sumy."

⁴³ Anderson, "How Ukraine's Roving Teams of Light Infantry Helped Win the Battle of Sumy."

the invasion, news cycles and social media became inundated with images from the frontlines. Given the scale of the conflict, unseen in Europe for over 75 years, and the interconnectedness of the continent, public support immediately began to mobilize in favor of the Ukraine. While global leaders watched with interested speculation, it quickly became apparent that the Ukrainian people themselves had mobilized as the government executed a masterful information operation campaign, inspiring their citizens and the world that Ukraine would not roll over to Russian aggression.

C. ENTER STARLINK

With the Ukrainians fighting tooth and nail to protect their capital in places like Hostomel airport and Irpin, Ukrainian politicians and influential figures began soliciting global aid. On February 26, 2022, a Ukrainian politician named Mykhailo Fedorov tweeted, appealing to the billionaire tech mogul Elon Musk for access to SpaceX's commercial satellite internet service in the form of Starlink.⁴⁴ That same day, Musk responded that Ukraine would have access to Starlink and his firm would be sending thousands of terminals to the country. In the span of two tweets, Ukraine, its population, and most importantly, its military became connected to a global architecture of low earth orbit (LEO) satellites that were utilized in conjunction with creative tactics and fierce determination to further stymie Russian advances. As the invasion has played out, the ability to keep Ukraine connected to the world via satellite internet has proven to be a major benefit and remains a priority for the country. Even as the Russians targeted power grids and critical infrastructure, Starlink terminals allowed Ukrainian President Volodymyr Zelenskyy and people across Ukraine to address the global population and ensuring that the world was directly aware of what the Russian aggression looked like firsthand. This maintained connectivity has proven to be a boon for controlling the information space, as Ukraine has continually circumvented Russian attempts at disinformation and controlling the narrative. Finally, Ukraine's frontline troops have not only been able to maintain

⁴⁴ Mykhailo Fedorov [@FedorovMykhailo]. “@elonmusk, While You Try to Colonize Mars — Russia Try to Occupy Ukraine! While Your Rockets Successfully Land from Space — Russian Rockets Attack Ukrainian Civil People! We Ask You to Provide Ukraine with Starlink Stations and to Address Sane Russians to Stand.” Tweet. *Twitter*, February 26, 2022. <https://twitter.com/FedorovMykhailo/status/1497543633293266944>.

connections with their families back home, they have also successfully integrated many of their operations, including targeting via drones, through Starlink.⁴⁵ In one extraordinary example, the troops inside the besieged Azovstal steel plant in Mariupol were able to maintain communications with their government and the world, coordinating resupplies and support, despite being completely surrounded by the Russian invasion force.⁴⁶

With the war dragging on, what initially appeared to be a knee jerk reaction to Russian aggression has caused new concerns to rise with the commercial company so intimately involved in an ongoing conflict. As its use has grown and entered different facets of the conflict, questions have been raised as to the legalities of using civilian systems for military purposes, drawing condemnation from Musk and threats from the Russian government.⁴⁷ Additionally, in late 2022, as quickly as Starlink appeared in Ukraine, signs began to show that economic principles had caught up to the philanthropic donation of hundreds of terminals and service providers. In an exchange on Twitter, Elon Musk explained that it was not fiscally reasonable for his company to fund the Ukrainian use of Starlink indefinitely.⁴⁸ Within a few days, after apparent negotiations with the U.S. government, and protests from Ukrainian supporters, Musk reaffirmed the commitment to providing satellite communications for the Ukrainian people.⁴⁹

While the loss of capability was negligible, what this episode did show, however, is the dangers of closely tying military and government capabilities to commercial companies that require profits and assured funding in order to function. The most current issue threatening the synergistic relationship between commercial and military assets

⁴⁵ “UkraineX: How Elon Musk’s Space Satellites Changed the War on the Ground,” Politico, June 8, 2022. <https://www.politico.eu/article/elon-musk-ukraine-starlink/>.

⁴⁶ Politico, “UkraineX: How Elon Musk’s Space Satellites Changed the War on the Ground.”

⁴⁷ Christian Davenport. “Russia Threatens Commercial Satellites That Pentagon Sees as Its Future.” *Washington Post*, October 29, 2022. <https://www.washingtonpost.com/technology/2022/10/28/space-war-ukraine-pentagon-russia/>

⁴⁸ Elon Musk. [@elonmusk] “@SawyerMerritt @rfdctr SpaceX Is Not Asking to Recoup Past Expenses, but Also Cannot Fund the Existing System Indefinitely *and* Send Several Thousand More Terminals That Have Data Usage up to 100X Greater than Typical Households. This Is Unreasonable.” Tweet. *Twitter*, October 14, 2022. <https://twitter.com/elonmusk/status/1580802376973230080>.

⁴⁹ Elon Musk, “SpaceX Is Not Asking to Recoup Past Expenses.”

occurred in February of 2023. In reaction to the tactic of using Starlink provided internet to control armed drones on the front lines, SpaceX announced that it would be restricting the Ukrainian military's ability to leverage Starlink in an offensive capacity.⁵⁰ In a public statement, the president of SpaceX, Gwynne Shotwell, stated that the Starlink systems were "never meant to be weaponized...[the] Ukrainians have leveraged it in ways that were unintentional and not part of any agreement."⁵¹ Once again, as lines blurred between civil and military applications, SpaceX found itself in murky waters regarding how the internet service it provided quickly filled more roles than they expected. As capacities provided by commercial companies match or surpass those of the military, unforeseen threats and situations will continue to emerge, much like we have seen in Ukraine. It will take foresight and creative thinking to ensure a smooth integration between military and commercial.

From a military perspective, there is much to take away from the fierce resistance put up by the Ukrainian people throughout many facets of their society. However, for this paper, it is most important to draw comparisons between the nimble yet powerful units that harassed the Russian military throughout the countryside, punching way above their weight through speed, creativity, and coordination that brought devastating effects upon their enemies. It does not take much imagination to quickly draw comparisons between the Ukrainian forces that fought the Russians to a standstill, and the currently evolving concepts for the Marine Corps' own stand in forces.⁵² Speaking strictly at a small unit level, the Ukrainian Army's use of light infantry, distributed throughout the area of operations, supported by combined arms, and massing to bring fires to bear on enemy formations is a glimpse into the evolving doctrine of Marine Corps infantry.

⁵⁰ "Elon Musk's SpaceX Restricts Ukraine's Use of Its Satellite Internet for Drones," Politico, February 9, 2023. <https://www.politico.eu/article/elon-musk-spacex-restricts-ukraine-use-of-its-satellite-internet-for-drone-control/>.

⁵¹ Joey Roulette. "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones -Company President." *Reuters*, February 2023. <https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/>.

⁵² Berger, David H. "A Concept for Stand-In Forces." *Proceedings* 147, no. 11 (November 2021). <https://www.usni.org/magazines/proceedings/2021/november/concept-stand-forces>

D. THE UKRAINIAN CONFLICT TO THE PRESENT DAY

At the time of this writing, the Ukrainian Armed Forces continue to face hordes of Russian invaders daily. The distributed, rapid defensive operations conducted in the early days of the conflict have molded into traditional land-based warfare, characterized by clearly defined frontlines, infantrymen, and a plethora of artillery. Multiple counteroffensives have been conducted by the Ukrainian Armed Forces with resounding success. While the conflict no longer looks the way it did during the frantic Russian invasion, Starlink continues to be at the forefront of Ukrainian command and control. In an article published in October 2022 by the Ukrainian military, a Polish volunteer serving as a gunner with a Ukrainian artillery unit explains how his D-20 howitzer unit was comprised of not only the artillery piece, but also a supporting compliment of drones and its own Starlink terminal.⁵³ He explains that,

thanks to the communication through the Starlink terminals, it was enough just to shoot regularly and adjust the fire. The voice communication was 24/7, so we regularly received corrections or, for example, information that the ammunition did not explode and other detonators need to be screwed in.⁵⁴

The article goes on to describe how this particular artillery unit has integrated the capabilities provided by Starlink into their battle drills and tactics, using the mobility and assured communications provided by the terminal to quickly receive firing data, shoot, and displace.⁵⁵ Tactics like these, a hallmark of a disciplined, cohesive unit, are magnified by modern equipment that enhances lethality through speed and communication. At the same time, the speed and assurance provided by modern communication technology increases survivability and resiliency for the unit.

The proliferation of Starlink terminals throughout Ukraine provided the Ukrainian military the ability to integrate Western combat systems into their operations while also demonstrating battlefield ingenuity in finding effective solutions for their type of fighting.

⁵³ “Starlink Has Become Indispensable for Ukrainian Gunners.” Militaryni. 22 October, 2022. <https://mil.in.ua/en/news/starlink-has-become-indispensable-for-ukrainian-gunners/>.

⁵⁴ Militaryni, “Starlink Has Become Indispensable for Ukrainian Gunners.”

⁵⁵ Militaryni, “Starlink Has Become Indispensable for Ukrainian Gunners.”

For example, in a recent *New York Times* piece, Thomas Gibbons-Neff details how in the battered city of Bakhmut, a team of observers snuck to a vantage point in the city to identify enemy positions. Using a Starlink terminal at their position to establish communications with higher headquarters, the soldiers were fed real time battlefield updates while under the enemy's nose.⁵⁶ By securing the communications link with higher headquarters, the soldiers were able to create a targeting network reminiscent of Western doctrine. In the same channel that they were fed updates about enemy drones and movements, the observers coordinated an artillery strike on a Russian position; achieving effects from a firing unit well beyond the range of line-of-sight communications.⁵⁷

While the previous example focused on targeting in the near battle area, the Ukrainian military has also demonstrated the ability to leverage Starlink in order to conduct deep strike operations within Russian occupied territories. While the success of the U.S. provided artillery combined with pLEO SATCOM has proven effective, it is important to note how the technology has also allowed the Ukrainians to use innovation to circumvent staunch Russian EW defenses. As the battlelines have stagnated, the conflict has seen a major growth in commercial unmanned aerial systems (UAS) for both reconnaissance and crude targeting.⁵⁸ While the Ukrainian Army has remained relatively tight-lipped about how this process works, images of a captured Ukrainian drone, shared on social media by Russian troops may help answer the question. Shared by Rob Lee, a senior fellow at the Foreign Policy Research Institute, the image, one of many, appears to be a drone with a Starlink Maritime terminal affixed to the top of it.⁵⁹

⁵⁶ Thomas Gibbons-Neff, "The Infrared Hunt for Russian Troops in the Battle for Bakhmut," *New York Times*, December 15, 2022. <https://www.nytimes.com/2022/12/15/world/europe/bakhmut-ukraine-russia-war.html>.

⁵⁷ Gibbons-Neff, "The Infrared Hunt for Russian Troops in the Battle for Bakhmut."

⁵⁸ "Soldiers in Ukraine Say Some Drones Affected After SpaceX Limits Starlink," *Wall Street Journal*, February 10, 2023. <https://www.wsj.com/articles/soldiers-in-ukraine-say-some-drones-affected-after-spacex-limits-starlink-321a9dd7>.

⁵⁹ Rob Lee [@RALee85], "Photos of a Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces. https://vk.com/Milinfoive?W=wall-123538639_3532115 <https://t.co/QfvYHFhRPa>," Tweet, *Twitter*, March 25, 2023. <https://twitter.com/RALee85/status/1639749679079383042>



Figure 2. Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces.⁶⁰

While the authenticity of this image cannot be corroborated, it still suggests the astounding creativity in which the Ukrainian military utilized the capabilities of Starlink to circumvent Russian localized EW attempts. Based on the capabilities of front line jamming equipment, the Russian Army was most likely conducting localized jamming, targeting the drone ground control stations and drones itself, within a relatively small radius.⁶¹ Simple but effective, this likely frustrated the Ukrainians to the point that they fixed the Starlink terminal to the top of the drone, ultimately allowing a Starlink satellite to serve as a relay station between the ground controller and the drone, sidestepping Russian jamming attempts.

⁶⁰ Rob Lee, "Photos of Ukrainian UAV."

⁶¹ Dominika Kunertova. "The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game." *Bulletin of the Atomic Scientists* 79, no. 2 (March 4, 2023): 95–102. <https://doi.org/10.1080/00963402.2023.2178180>.

E. RUSSIAN STRUGGLES WITH ELECTRONIC WARFARE

It is true that commercial SATCOM does not immediately offer the same robust data protection against electronic warfare that we expect military hardware to provide. The fear of jamming or interception remains persistent threats for the U.S. military in future conflicts among more and more technically savvy rivals. However, Russia has consistently been seen as one of the preeminent nations in electronic warfare, yet they have had little definitive success since their invasion of Ukraine in 2022.

Perhaps one of the most condemning pieces of evidence towards the struggles of Russian Electronic Warfare (EW) abilities in the conflict is the fact that the Ukrainian military has not requested large SATCOM capabilities from its allied partners. In comparison to the thousands of Starlink terminals that flooded the country in the immediate aftermath of the Russian invasion, by analyzing the Presidential Drawdown Security Assistance provided to Ukraine, one can see that tactical secure communications were not provided until August of 2022.⁶² The reports did not specify what kind of communications systems these were, however it can be assumed that until this point in the conflict, Ukraine had been able to subsist on their organic communications and the capabilities provided by Starlink. Furthermore, on October 28, 2022, the United States announced its first explicit donation of equipment necessary for military grade SATCOM: four SATCOM antennas.⁶³

As stated previously, due to the ongoing nature of this conflict, concrete evidence of the reasoning for the methodology behind the transactions has not been announced to date. However, one can make sound assumptions by correlating the Security Assistance Packages with the corresponding battlefield events. First and foremost, in the early stages of the conflict, without criticizing Russian capabilities, it appears that Ukrainian military operated with relative impunity using its Starlink systems for battlefield communication. Dave Tremper, the director of electronic warfare for the Office of the Secretary of Defense, noted how in the early stages of the conflict, as Russia attempted to rapidly seize urban

⁶² U.S. Department of State, *U.S. Security Cooperation with Ukraine* (Washington, DC: Department of State, May 2023), <https://www.state.gov/u-s-security-cooperation-with-ukraine/>.

⁶³ U.S. Department of State, *U.S. Security Cooperation with Ukraine*.

centers, the complexity of synchronizing and coordinating EW efforts led to poor implementation as opposed to the robust EW efforts seen in the more static fighting on the border of Ukraine from 2014–2022.⁶⁴ As seen in Figures 3 and 4, with the announcements of the security assistance packages, a correlation between shifting forms of warfare, from an elastic defense into a more traditional stronghold defense, and the need for more military-grade communications equipment is made apparent. Figure 3 shows the extent of Russian advances in 2022, at this point, with the Ukrainian Army conducting mobile, distributed operations the United States had yet to provide military grade communication equipment. This provides evidence that the use of available Starlink systems was sufficient for the warfare being conducted. Figure 4 depicts the battlelines as they were in September 2022 after Ukrainian counterattacks in Kharkiv. The battlefield became more clearly delineated and for the first time, the United States provided military grade SATCOM in an assistance package. As lines became stagnant, it is likely that Russia was able to bring more of its traditional EW assets to bear in support of front-line units. The shift to attrition style warfare may have been the point in which Ukrainian forces first met limitations with the effectiveness of their commercial SATCOM, necessitating a request for more robust and secure systems.

⁶⁴ Valerie Insinna. “SpaceX Beating Russian Jamming Attack Was ‘Eyewatering’: DOD Official.” *Breaking Defense*, April 20, 2022. <https://breakingdefense.sites.breakingmedia.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/>.



Figure 3. Russian Advances in March 2022⁶⁵

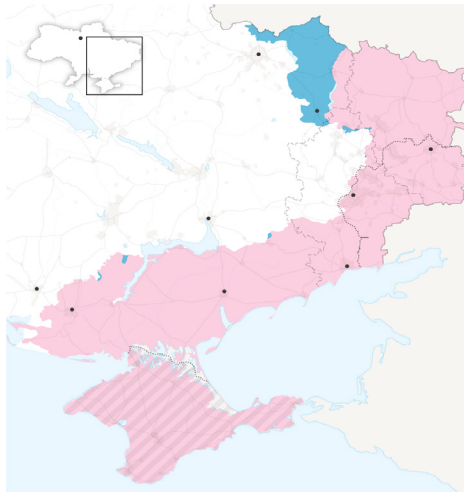


Figure 4. Battlelines September 2022⁶⁶

Despite this, the Security Assistance Packages still do not reflect an apparent urgent need for military grade SATCOM, with only a limited number being sent to Ukraine.⁶⁷ The most urgent Ukrainian requests for assistance with regards to SATCOM continues to be when Elon Musk announced that SpaceX could not continue to fund usage alone.

⁶⁵ “Maps: Tracking the Russian Invasion of Ukraine.” *New York Times*, February 14, 2022. <https://www.nytimes.com/interactive/2022/world/europe/ukraine-maps.html>

⁶⁶ “Maps: Tracking the Russian Invasion of Ukraine.”

⁶⁷ U.S. Department of State, *U.S. Security Cooperation with Ukraine*.

Another facet of the Starlink and Ukraine integration is the quick reaction and flexibility to counter jamming attempts and cyber-attacks when the Russians have been able to conduct a coordinated electronic warfare plan. In another situation well documented via Tweet, on March 25, 2022 Elon Musk tweeted that, “Starlink had resisted all hacking and jamming attempts [to that point].”⁶⁸ Additionally, Dave Tremper, noted how during a subsequent EW attack targeting Starlink, the company was able to update software among its systems within a matter of hours, rendering the exploit useless.⁶⁹ He subsequently addressed the company’s adaptability in creating a solution without drastically losing the ability to function.⁷⁰ This adaptability can also be seen not only as a byproduct of software, but also a benefit of the mutually supportive network of pLEO satellites. Understanding that Russian EW tactics and systems were developed to target the traditional communication and networking capabilities of NATO and Western armies, it becomes readily apparent that the influx of thousands of transmitters and receivers onto the battlespace has stymied legacy Russian EW doctrine.

F. CHAPTER SUMMARY

Prior to the full-scale invasion in February 2022, the Ukrainian military relied on a mix of military and commercial equipment that rendered them vulnerable to Russian electronic warfare. After the invasion, third party support in the form of Elon Musk and Starlink injected a capability into Ukraine that had not been anticipated. Through creative integration, the Ukrainian people were able to quickly leverage the capabilities of pLEO SATCOM to execute complex defenses and targeting. At the same time, global connectivity helped Ukrainians maintain a lifeline to the world, while simultaneously SpaceX helped circumvent Russian attempts at network interference. With the progression of the war, there has been a continued effort to integrate the tools provided by Starlink in order to better command, communicate and target.

⁶⁸ Elon Musk [@elonmusk]. “@slashdot Starlink, at Least so Far, Has Resisted All Hacking & Jamming Attempts.” Tweet. *Twitter*, March 25, 2022. <https://twitter.com/elonmusk/status/1507505633259630599>.

⁶⁹ Insinna. “SpaceX Beating Russian Jamming Attack Was ‘Eyewatering’: DOD Official.”

⁷⁰ Insinna. “SpaceX Beating Russian Jamming Attack Was ‘Eyewatering’: DOD Official.”

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A MARINE CORPS FOR EMERGING CHALLENGES

Upon taking over the Marine Corps, the Commandant, General David Berger, instilled rapid, institutional change upon the force. Quickly divesting elements that were seen as too bulky and dated, overnight the Marine Corps found itself learning to fight in the modern age of peer competition, no longer burdened by fighting irregular forces in the deserts of Iraq and Afghanistan. With a rising power in China threatening the status quo in the Western Pacific, the focus shifted to the Pacific and with that, a return to naval expeditionary operations.

Roughly 100 years ago, Lieutenant Colonel Earl “Pete” Ellis on assignment to study and gain intelligence on the emerging Japanese threat in the Pacific, foresaw the need for an expeditionary Marine Corps, amphibious in nature, and capable of seizing and holding naval bases.⁷¹ In his assessment, *Advanced Base Operations in Micronesia*, Ellis makes clear that decisive action in the Pacific will be decided by ten factors. A timeless document, his factors are true to this day, the most applicable to present day warfare being:

1. A main fleet action will decide the war in the Pacific.
2. Operations preliminary to a fleet action must be carried out by (as far as possible) the minimum naval forces and those of least fleet value in fleet action.
3. Marine forces of reduction, occupation and defense must be of such strength and composition (so far as maybe compatible with the conditions under which they must operate) as to require the least possible naval support.
4. An offensive projection into the enemy’s strategic front must be made in a series of well-defined and rapid moves (sea objectives) in order to afford the battle fleet the greatest protection for the greatest portion of the time.

⁷¹Earl H. Ellis, *Advanced Base Operations in Micronesia*, 712H Operational Plan (Quantico, VA: U.S. Marine Corps, 1921), https://www.google.com/books/edition/Advanced_Base_Operations_in_Micronesia/MRpL_niBlcYC?hl=en&gbpv=1&printsec=frontcover.

(Long-drawn-out operations, with the fleet and its base subject to close attack by the enemy light forces, are to be avoided).

5. A sea objective must be more or less isolated and include an area that can be reduced practically simultaneously.⁷²

At the time, these concepts were revolutionary and required dramatic changes to the traditional training and mission of the Marine Corps. Despite complaints, Ellis's predictions proved to be quite accurate. One hundred years later, one could argue that his predictions remain relevant.

In his planning guidance released in 2019, General Berger addresses the rising issues in the Pacific with the same foresight and introspection as Ellis did in the interim period between great conflicts. Like Ellis, he believes that Marine ground forces will be called on once again in support of naval formations, establishing advanced bases, and conducting distributed operations.⁷³ While his guidance goes on to explain how the Marine Corps will change its structure to meet emerging threats conducting Expeditionary Advanced Base Operations and Distributed Operations, for the purpose of this thesis, the focus will be on his warfighting concept of Stand-in Forces.⁷⁴

A. STAND-IN FORCES

As part of the Commandant's Planning Guidance released in 2019, the Marine Corps introduced the concept of Stand-In Forces (SIF) as a key component of future Marine Corps operations, specifically in the Pacific, in defense of key maritime terrain and allies in the region. Specifically designed to complement the Navy's Distributed Maritime Operations Concept, *A Concept for Stand-In Forces* defines stand-in forces as "small but lethal, low signature, mobile, relatively simple to maintain and sustain forces designed to operate across the continuum within a contested area as the leading edge of a maritime

⁷²Earl H. Ellis, *Advanced Base Operations in Micronesia*.

⁷³U.S. Marine Corps, *Commandant's Planning Guidance*.

⁷⁴U.S. Marine Corps, *Commandant's Planning Guidance*.

defense-in-depth in order to intentionally disrupt the plans of a potential or actual adversary.”⁷⁵

Stand-in Forces are envisioned at the “forward edge of a partnered maritime defense-in-depth that denies the adversary freedom of action.”⁷⁶ As such, they operate within proximity of potential adversaries, inhibiting their plans and operations within a maritime environment. SIF will require the use of an array of skillsets and technology to leverage effects on adversary forces while operating within the effective ranges of enemy weapon systems, as seen in Figure 5. Furthermore, SIF operations will require robust interoperability with host nations and host nation forces to sustain and operate while minimizing their logistical and communications footprint.⁷⁷

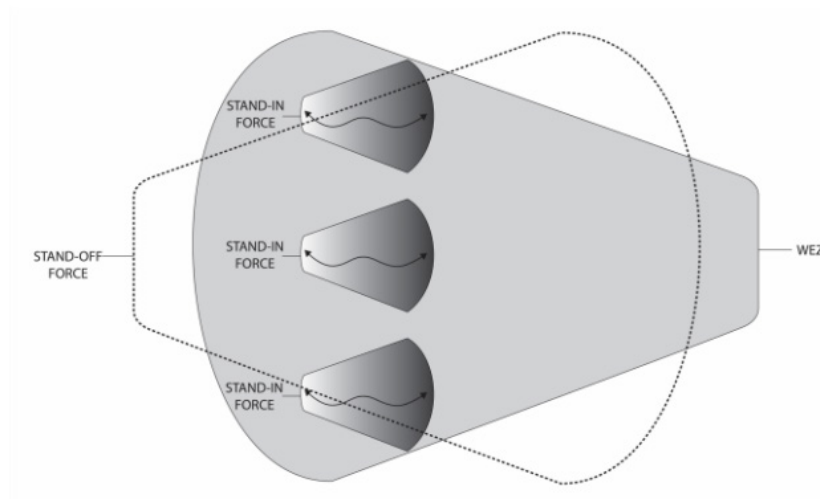


Figure 5. Idealized Conceptual Depiction of Stand-Off and Stand-In Engagement.⁷⁸

⁷⁵ U.S. Marine Corps, *A Concept for Stand-In Forces*, 4.

⁷⁶ U.S. Marine Corps, *A Concept for Stand-In Forces*, 4.

⁷⁷ U.S. Marine Corps, *A Concept for Stand-In Forces*, 17.

⁷⁸ U.S. Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations*, 1st Ed. (Washington, DC: U.S. Marine Corps, 2021).

Within the constructs of Force Design 2030, the SIF responsibility will fall on the same units that have borne the brunt of Marine Corps operations since its inception, the Ground Combat Element (GCE). The GCE, made up of infantry, artillery, reconnaissance, logistics, and aided by special operations will train to meet the complex requirements of SIF throughout the coming years. The concepts demonstrated in *A Concept for Stand-In Forces* are yet to be tested, however, to strengthen the approach, the Marine Corps needs to adopt emerging technologies in order to solidify its positions as a forward operating force ready to counter adversary actions in contested maritime environments.

B. USMC GCE NEED FOR ASSURED COMMUNICATIONS IN A CONTESTED ENVIRONMENT

The United States has long held a monopoly on operations within the space domain. Throughout the wars in Iraq and Afghanistan, the United States was able to make use of SATCOM without having to worry about the potential for adversarial interference. As the adversarial interactions shift to peer competition, it has become apparent that this monopoly may be put into jeopardy. Both China⁷⁹ and Russia⁸⁰ have demonstrated the ability to conduct anti-satellite (ASAT) targeting in clearly directed statements towards the United States. By threatening the domain in which the United States has grown accustomed to operating within, adversaries have forced the United States military to identify solutions for this newly contested environment.

In addition to the physical threat, GCE forces will face increased potential for non-kinetic EW based attacks on their networks and communication equipment much like those seen in the ongoing Russo-Ukrainian War. As such, the GCE has a need to identify alternatives for ground force communications if it hopes to bring to bear the capabilities promised in *Force Design 2030* and *A Concept for Stand-In Forces*. These reasons demonstrate a need to take lessons learned from the Ukrainian integration of commercial

⁷⁹ Gene V. Milowicki and Joan Johnson-Freese, "Strategic Choices: Examining the United States Military Response to the Chinese Anti-Satellite Test," *Astropolitics* 6, no. 1 (March 10, 2008): 1–21, <https://doi.org/10.1080/14777620801907913>.

⁸⁰ Courtney Albon. "Spacecom Confirms Russian ASAT Test, Creating Debris Field." *Inside the Pentagon* 37, no. 46 (Nov 18, 2021). ProQuest.

communication systems into their tactics and procedures and apply them to Marine Corps operations.

C. UKRAINE IN RELATION TO USMC STAND-IN FORCES

Removing the maritime component, it is easy to make a comparison between the USMC Stand-In Forces concept and the Ukrainian Army's demonstrated capabilities in the defense of their country in the early stages of their conflict. For all intents and purposes, the Russian military should have been able to steamroll the Ukrainian military as many predicted. Instead, as already acknowledged, the Ukrainian Army, through competence and creativity, fought the Russians to a standstill which allowed Western aid and popular mobilization to generate the forces and equipment needed to conduct traditional counteroffensives and defensive operations. Like the USMC concept for SIFs, Ukrainian Army troops operated in small, highly agile and lethal units, who conducted complex ambushes and raid type operations against the traditionally lumbering and heavily armored Russian forces.⁸¹ Their agility and lethality helped level the playing field despite being outnumbered and outgunned by the Russian Army. Furthermore, much of Ukraine falls well within the range of Russian long-range missiles and rockets. The aspect of contesting by missile coverage is nearly identical to the environment in which the Marine Corps foresees itself operating. The most applicable lesson that the Marine Corps can learn from the Ukrainian Army is their ability to rapidly integrate commercial satellite technology into their military operations while still operating under constant harassment and contention from the Russian military.

The integration of pLEO SATCOM has permeated down to tactical level units, influencing tactics, techniques, and procedures (TTPs). Because of the ongoing nature of the conflict, it is impossible to truly analyze how Ukraine has implemented their Starlink accessibility into current TTPs, however, reporting and assessments from the frontlines offers glimpses into the everyday fighting that allow for conclusions to be drawn on their implementation. In its current stages, the Marine Corps already has an exorbitant amount

⁸¹ Anderson, "How Ukraine's Roving Teams of Light Infantry Helped Win the Battle of Sumy"

of information to garner from the conflict for its ground combat forces. The Marine Corps GCE, understanding its role as stand in forces for a potential conflict with China, needs to take away key lessons learned about the Ukrainian ability to integrate pLEO command and control into their battle rhythm while retaining combat effectiveness within the WEZ of the Russian military.

D. CHAPTER SUMMARY

The United States Marine Corps understands the necessity for change in order to meet rising threats within the Pacific theatre. Using lessons from the past, the Commandant of the Marine Corps has restructured the Marine Corps to meet these threats. The Stand-In Force concept has been designed to operate within the WEZs of enemy forces as a means to defend, sense, and provide targeting solutions for the United States. Without a model to follow, it is important to look around the globe for case studies to learn from. The Ukrainian Army currently operates in the exact same manner. The lynchpin of Ukrainian success against the Russian invasion has been their ability to rapidly mass fires on enemy positions and formations while remaining nimble enough to evade punishing, retaliating blows. At the root of this ability is their expansive communication network powered by the integration of commercial pLEO communication capabilities. This is a lesson that the Marine Corps needs to learn from if it hopes to achieve the same measures of success in future conflict.

V. APPLICATIONS OF COMMERCIAL SATCOM FROM THE UKRAINIAN CONFLICT FOR THE U.S. MARINE CORPS

In the previous chapter, comparisons are drawn between the Marine Corps SIF concept and the Ukrainian military in the early stages of the Russian invasion. Characterized by nimble infantry capable of bringing devastating effects to bear on enemy units, there are striking similarities in the two forces. At the crux of both forces is the need for persistent communications operated within close proximity to the enemy. Without a military satellite pLEO satellite constellation in orbit, it is imperative for the Marine Corps to understand the distinct benefits afforded by leveraging commercial technology. In this section, the benefits of commercial pLEO SATCOM from the Ukrainian perspective will be applied to Marine operating concepts.

A. PLEO ARCHITECTURE FLEXIBILITY

As mentioned in the section on the benefits of pLEO communications, current commercial architectures are made up of thousands of small satellites purpose built to provide internet services to terminals on the ground. Given the orbital mechanics of LEO satellites, in order to maintain constant communications, satellites require seamless transitions or “hand offs” between the spacecraft that make up the network to maintain viable connection to the ground terminal. As these networks become more robust and complete, more and more commercial satellites will cover the sky, creating an effective net that covers the globe.

One of the most persistent EW threats faced by United States forces is the threat of jamming. Mentioned previously in this thesis, jamming involves flooding a receiver with so much noise, it is unable to process the signals on the frequency that it is receiving.⁸² In a combat scenario, the enemy conducting traditional satellite jamming must decide which receiver to jam, either the ground station or the satellite. Satellite architectures currently rely on robust anti-jam capabilities because the targets are few and identifiable by enemy

⁸² Poisel, *Information Warfare and Electronic Warfare Systems*, 112–113.

forces. With the integration of commercial pLEO satellites, jamming becomes immediately more difficult. As technology increases, it is likely that commercial satellite companies will be able to use primary and alternative routing options in order to circumvent either naturally decaying spacecraft, damaged spacecraft, or spacecraft compromised by outside actors.

1. Placing the Enemy in an EW Dilemma

While it is true that during the fighting in Ukraine the Russian Army has effectively jammed Ukrainian communications from commercially provided platforms like Starlink, most of this jamming has been localized to the frontlines, targeting Starlink receivers and individuals using cell phones for communication.⁸³ For a country like Ukraine, with a necessity to safeguard some of its EW assets, this can provide challenges in command, control, and operations. However, for a nation like the United States that can leverage a vast number of weapon systems in its arsenal, a situation where the enemy cannot truly operate how they want to, is ideal. In the jamming commercial SATCOM scenario, the choice must be made how to allocate finite EW resources; either attempting to jam hundreds if not thousands of rapidly changing satellites or attempting to jam the units on the ground receiving signals, placing valuable assets much closer to harm's way.

Marine SIF can leverage the concept of pLEO flexibility in the ways mentioned above. Implementation of commercial pLEO communications would provide Marine forces at the forward edge the ability to utilize data-based communication that was flexible enough to provide robust solutions in the case of jamming. At the same time, if the enemy were to attempt to jam terminals at the ground level, these actions afford Marine SIF the opportunity to integrate the capabilities provided by the Marine Air Ground Task Force to sense and target valuable enemy assets. This concept is explicitly described in the section of *A Concept for Stand-In Forces* section “Win the Maritime Reconnaissance and Counter-Reconnaissance Battle.”⁸⁴ In describing actions taken by SIF to fight for information, the

⁸³ Sam Skove, “Using Starlink Paints a Target on Ukrainian Troops,” Defense One, March 23, 2023, <https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/>.

⁸⁴ U.S. Marine Corps, *A Concept for Stand-In Forces*, 10.

document explains that, “[fighting for information] includes fighting with the intent to cause an enemy reaction that can be observed by SIF or another sensor,” ultimately building a more complete concept of the operating environment and giving commanders the ability to better target the enemy system.⁸⁵

The flexibility provided by commercial pLEO SATCOM is readily apparent for SIF in a maritime environment. By complicating an adversary’s ability to conduct jamming, the pLEO satellite architecture places the actor in a dilemma. This predicament plays directly into the SIF concept. Either the enemy struggles using traditional methods to jam thousands of transmitting satellites or, the enemy, making the decision to jam local receivers, is forced to move valuable assets closer to the front lines where they can be sensed and targeted by SIF forces.

B. MOBILITY

The concept for SIF forces explicitly states a need for survivability while operating within contested areas. Facets of survivability involve lightening the Marines’ footprint both physically and logistically.⁸⁶ Speaking from experience, one of the largest limiting factors for extended operations are the batteries needed to operate the communications required to command and control even a small unit. One 2590 battery alone, required to operate a 7.1-pound radio, weighs 3.1 pounds, resulting in weight being spread across units and increasing the individual load of each Marine. At the same time, communications can become logistically heavy as well, especially in comparing the assets required to provide services comparable to commercially available SATCOM.⁸⁷ The integration of commercially available communication solution helps alleviate both of these scenarios.

Current commercial SATCOM terminals continue to be developed and continue to decrease in size with each release. In addition, because the systems are designed to be sold

⁸⁵ U.S. Marine Corps, *A Concept for Stand-In Forces*, 12.

⁸⁶ U.S. Marine Corps, *A Concept for Stand-In Forces*, 18.

⁸⁷ “Mobile Satellite System Reduces Communication Gaps, Increases Naval Interoperability,” Marine Corps Systems Command, <https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/2872370/mobile-satellite-system-reduces-communication-gaps-increases-naval-interoperabi/>.

to a public audience, the systems are meant to be powered by traditional means, power grids, generators, and vehicles to name some of the potential power sources. This requirement ensures that the hardware required to operate the equipment is adaptable to any area of the world. As seen in Ukraine, the lightweight mobility afforded using Starlink terminals has been a gamechanger on the battlefield. The previously mentioned summary of the Ukrainian howitzer team's battle drill explained how the unit's ability to emplace, fire, and displace was a direct result of the maneuverability and reliability of the Starlink terminals.⁸⁸ Marine SIF will "prioritize gaining contact with the potential adversary but balance it against survivability and the need to keep the sustainment burden inside the contested area as light as possible."⁸⁹ These types of rapid engagements and withdrawals are real world examples of the tactics envisioned within *A Concept for Stand-In Forces*. Leveraging the commercially available tools helps aid the future development of these concepts while real world scenarios from Ukraine offer insight into the development of best practices.

1. Speed versus Security

Some will argue that the electronic signature emitted by commercial SATCOM terminals can be a dangerous byproduct of its use. There is no question that this is a danger faced by operators in Ukraine.⁹⁰ However, on the modern battlefield it is almost impossible to operate without emitting a signal on the electromagnetic spectrum. Success comes from limiting traffic to only necessary communications and then terminating all transmissions. Due to the persistent overhead nature of pLEO satellite constellations and the continued growth of the constellations, the ability to connect, transmit, and terminate a connection will only get faster. At the same time, the high latency of the systems ensures that transmissions will be brief and succinct. This affords operators the opportunity to send a message and quickly displace before enemy direction-finding equipment can home in on a suspected location. In the case of SIFs this means emanating a signal long enough to

⁸⁸ Militaryni, "Starlink Has Become Indispensable for Ukrainian Gunners."

⁸⁹ U.S. Marine Corps, *A Concept for Stand-In Forces*, 6.

⁹⁰ Skove, "Using Starlink Paints a Target on Ukrainian Troops."

coordinate follow on actions, like high precision strikes on enemy targets. At the same time, as mentioned in *A Concept for Stand-In Forces*, a byproduct of leveraging the full strength of the U.S. joint force is the ability to bring to bear the full depth of the military's sensing and targeting capabilities.⁹¹ In this sense, SIFs using commercial SATCOM could bait the enemy into exposing their vital warfighting assets to higher level sensors and shooters.

C. LEVERAGING INDUSTRY RESPONSE TO ATTACKS

One of the most striking examples of the benefit of commercial SATCOM in the Ukrainian conflict has been the agile response of SpaceX to attempts by the Russians to degrade and diminish its effectiveness on the battlefield. As mentioned in previous sections, the personnel working for the company have displayed the ability to alleviate Russian hacking and jamming attempts within hours. While one instance early in the conflict made the most news, Elon Musk has mentioned that these fixes are regular occurrences for the company.⁹²

During complex military operations, it is readily apparent that cyberwarfare will be treated as a form of fires, with both sides attempting to cripple one another through offensive cyber operations. Currently, with Department of Defense systems, the onus is on government personnel to diagnose and rectify adversary attempts at cyber disruption. While effective, this process has been self-described as slow and reactive.⁹³ By allowing industry to find and manage their own solutions to interference with their products, the Department of Defense would be able to allocate manpower and resources to other cyber related matters while still ensuring connectivity for the warfighter at the ground level.

⁹¹ U.S. Marine Corps, *A Concept for Stand-In Forces*, 5.

⁹² Elon Musk [@elonmusk], "Starlink Has Resisted Russian Cyberwar Jamming & Hacking Attempts so Far, but They're Ramping up Their Efforts <https://t.co/W62yCsDA5w>," Tweet, *Twitter*, May 11, 2022, <https://twitter.com/elonmusk/status/1524191785760788480>.

⁹³ Stephen Losey, "SpaceX Shut down a Russian Electromagnetic Warfare Attack in Ukraine Last Month — and the Pentagon Is Taking Notes," C4ISRNet, April 22, 2022, <https://www.c4isrnet.com/air/2022/04/20/spacex-shut-down-a-russian-electromagnetic-warfare-attack-in-ukraine-last-month-and-the-pentagon-is-taking-notes/>.

D. MAINTAINING INFLUENCE

In the early stages of the February invasion, Russia attempted to isolate Ukraine from the world by targeting existing cyber infrastructure within the country.⁹⁴ The near immediate introduction of Starlink into the battlespace effectively rendered this tactic useless. The Ukrainian government and military's continuing success in countering Russian information warfare demonstrates a retained capability to operate in the information sphere by maintaining access to the internet. Meanwhile, Starlink self-reported data, seen in Figure 6, shows internet access by SATCOM has exponentially increased since the beginning of the war.⁹⁵ As a byproduct of the increased connectivity, Ukrainians were able to quickly share images and perspectives from the frontlines, winning over public support from around the world. The Ukrainian president and other members of the government were able to send appeals to the world while reassuring citizens that they would stand with their countrymen in the fight against Russian aggression. After the disheveled Afghan government retreat from Kabul in 2021, the world was inspired by the stoic response from the Ukrainian government and rallied behind the cause. To date, countless amounts of weaponry, supplies, and money have flooded into the country as a response to the global backing of the nation. Additionally, the availability of internet connection has proved to continue to be a boon for Ukrainian servicemen and women as they are able to communicate with family and share experiences from the frontlines. Social media continues to be filled with morale inspiring pictures and videos that appeal to the human condition found in warfare.

⁹⁴ Patrick Howell O'Neill, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion," MIT Technology Review, May 10, 2022, <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.

⁹⁵ Elon Musk [@elonmusk], "@FedorovMykhailo Starlink Data Usage Growth in Ukraine Https://T.Co/C4IWNwKwLR," Tweet, *Twitter*, October 13, 2022, <https://twitter.com/elonmusk/status/1580572380535001088>.

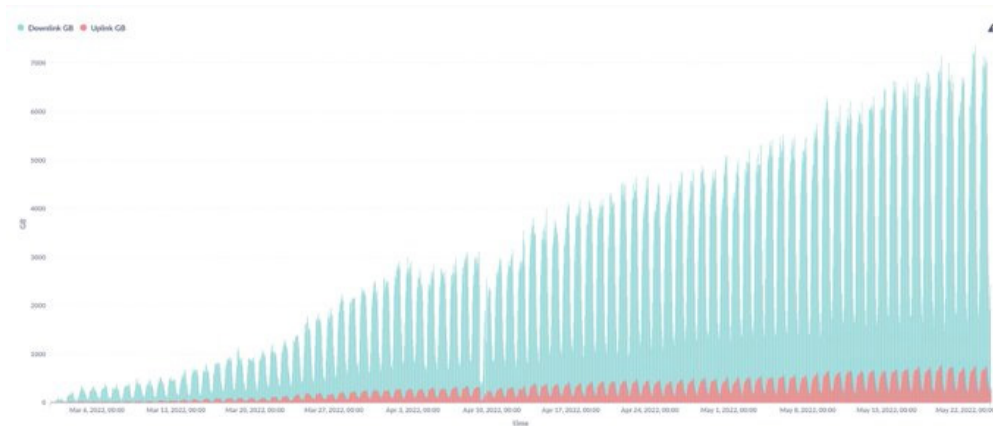


Figure 6. Starlink Data Usage in Ukraine March to May 2022⁹⁶

It has long been dictated that the information space is one of the most important domains of modern conflict. The Ukrainian ability to influence the global population while maintaining operational security has been a masterclass on dominance of the information domain. If the Marine Corps wants to succeed in the future, it must take these lessons and implement them into its TTPs. Frontline messaging can be a double-edged sword, but the Ukrainian military has for the most part displayed an uncanny ability to engage with worldwide audiences while preventing adverse effects on its troops. The Russian ability to control the narrative of the conflict has proven ineffective to the point that many of its information campaigns are laughable to the world. Commercial SATCOM is not a requirement for this kind of information campaign however, Ukraine has proven time and time again that it is an effective force multiplier in this realm.

E. ADDITIONAL CONSIDERATIONS

In conducting research for this thesis, two interesting potential military applications of commercial SATCOM made themselves apparent. *A Concept for Stand-In Forces* stresses the need for signature management and an increased use of tactical deception.⁹⁷ Both of these topics leave much to the creativity of the individuals conducting combat operations. For Marine ground combat units, integrating commercial SATCOM into

⁹⁶ Elon Musk “@FedorovMykhailo Starlink Data Usage Growth in Ukraine.”

⁹⁷ U.S. Marine Corps, *A Concept for Stand-In Forces*, 20–21.

operations offers possibilities for refining new TTPs for both signature management and deception.

1. Hiding in the Noise

There are predictions that future conflicts will rely on artificial intelligence and machine learning to manage the large amounts of data collected by networks of sensors.⁹⁸ This emerging warfare concept requires creative solutions to defeat and deceive the capabilities that artificial intelligence brings to the table. Integration of commercial SATCOM into the communication architecture of SIFs offers a potential solution to this new threat that would provide an overall increase in force protection and operational security.

As witnessed in Ukraine, the future battlefield will be littered with the terminals needed to successfully utilize pLEO SATCOM. One can imagine the large amount of data emanating from these terminals, readily available for collection and exploitation by enemy forces. At the same time, the large number of terminals offers an opportunity to confuse enemy sensors. It is expected that pLEO SATCOM usage will continue to expand across the globe. In the Pacific, where the Marine Corps is preparing to operate SIFs, countries are continuing to adopt the technology.⁹⁹ This increases the opportunity for Marine Corps units to maneuver within the growing electromagnetic space in this region. By using the same frequencies as local emitters, Marine Corps forces can blend within the ambient electromagnetic spectrum in the operating environment. This allows the units to mask their signals in the noise generated by local users, again, increasing the SIFs ability to confuse enemy sensors.

An article recently published by the Modern Warfare Institute, titled “Hiding In The Noise: Preparing The Irregular Warfare Community For The Age Of AI,” explains how the inclusion of artificial intelligence (AI) on the battlefield will require a change in

⁹⁸ U.S. Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations*, 2nd Ed. (Washington, DC: U.S. Marine Corps, 2023), 3–9.

⁹⁹ Veronica John, “SpaceX Starlink Satellites to Operate in the Pacific,” Vanuatu Daily Post, April 16, 2021, https://www.dailypost.vu/news/spacex-starlink-satellites-to-operate-in-the-pacific/article_71ed8298-9e40-11eb-bcd4-0b022f5709ea.html.

how military operations are conducted. In order to combat the emerging threat of AI and machine learning, the author proposes a concept called data poisoning. Data poisoning works by corrupting an artificial intelligence algorithm through manipulation of the data input into the system. In this manner, the machine processes the incorrect information, resulting in less accurate outputs.¹⁰⁰ With an ever-increasing number of terminals in the operating environment, Marine units have the potential to purposely control the outputs from their terminals, essentially providing the poisoned data fed to enemy sensor systems. Additionally, the enemy collections efforts will already be strained to identify Marine units among the noise generated by military, host-nation, and civilian transmissions, while simultaneously being fed manipulated data targeting machine learning processors.

2. Deception

The Marine Corps GCE is woefully behind in its implementation of electronic warfare. The concept and techniques are misunderstood and often an afterthought. To achieve success in a future conflict, this needs to change. Marine officers have previously expressed a need and desire for the ability to protect their units by utilizing electromagnetic decoys.¹⁰¹ Tactically placed, these decoys would mimic friendly positions and generate signatures that disguised capabilities. Despite these frustrations, a viable solution has yet to be proposed.

Commercial pLEO SATCOM provides a viable answer. Cheap and effective, a COTS pLEO terminal can be used almost immediately as a hasty decoy. As more units learn from the lessons in Ukraine and adopt commercial SATCOM the electronic signature from one terminal will become synonymous with a tactical formation. As such, well placed terminals, programmed to operate on their own, will effectively appear as units to enemy EW teams. This application provides an immediate solution, increasing force protection and offering commanders the ability to tactically employ electromagnetic deception.

¹⁰⁰ Matthew Moellering. "Hiding in the Noise: Preparing the Irregular Warfare Community for the Age of AI." Modern War Institute, September 26, 2022. <https://mwi.usma.edu/hiding-in-the-noise-preparing-the-irregular-warfare-community-for-the-age-of-ai/>.

¹⁰¹ Walker Mills. "A Tool For Deception: The Urgent Need For EM Decoys." *War Room – U.S. Army War College*, February 27, 2020. <https://warroom.armywarcollege.edu/articles/tactical-decoys/>.

3. Policy Support

Due to the nature of the platforms necessary for operating commercial SATCOM, there needs to be clarification of the responsibilities between civil and military applications for commercial SATCOM, especially during times of war. The Civil Reserve Air Fleet (CRAF) is an effective model for the use of pLEO satellite constellations by the military during extremis situations. The CRAF is a selection of commercial aircraft that can be committed to Department of Defense use in extreme situations.¹⁰² Like the CRAF, satellites within commercial constellations should be designated for military use if required. With this in mind, the military would have a dedicated network of satellites that would be able to ensure a full spectrum of capabilities in extremis situations.

F. CHAPTER SUMMARY

This chapter explored the ways in which the Invasion of Ukraine has demonstrated a viable implementation of commercial SATCOM for Marine Corps Stand-In Forces. Because of its unique capabilities utilizing pLEO constellations, commercial SATCOM has many benefits for integration with Marine Corps doctrine and operations. While many of these benefits have already been demonstrated by the ongoing conflict in Ukraine, there are still unexplored advantages to leverage if the Department of Defense were to adopt the complete implementation of commercial SATCOM.

¹⁰² Government Accountability Office, *The Civil Reserve Air Fleet – An Effective Program to Meet Defense Emergency Airlift Requirements*, GAO LCD-78-239 (Washington, DC: Government Accountability Office, 1978), 1–6.

VI. RECOMMENDATIONS AND CONCLUSION

It is apparent that the Ukrainian use of pLEO SATCOM validates the potential for similar operation by Marine Corps SIFs in line with *Force Design 2030*. The conflict has demonstrated that creative implementation of commercial space technology can be effective on a modern battlefield. Integrating the Ukrainian employment concepts in the following recommendations and future research suggestions will only enhance the Marine Corps ability to achieve similar successes.

A. RECOMMENDATIONS

1. Table of Equipment Recommendation

Evidence from frontline troops in Ukraine demonstrates the effectiveness of a Starlink terminal within individual units, especially fire support agencies. The Marine Corps should evaluate its capabilities and look to provide a SATCOM solution that mimics the Ukraine use. For example, in a rifle company, two ground terminals could be provided as a means to facilitate communication between the company headquarters element and the weapons platoon. This would allow for more decentralized operations with a commensurate increase in capability and range. Much like the Ukrainian artillery unit mentioned in Chapter III, the Marine Corps should also experiment with providing commercial SATCOM to its individual fire support units, augmenting traditional communications with pLEO SATCOM to increase speed and flexibility.

2. Training and Education

Training and education for ground combat officers focuses specifically on traditional radio communications. There is little focus on the importance of data and its subsequent benefits in the future battlefield. At the same time, little focus is made to fully train officers on the importance of operations within the electromagnetic spectrum. Training needs to be improved to allow Marine officers the confidence and competence to plan operations within the electromagnetic spectrum. In turn, this would ensure that officers are able to employ systems, like commercial SATCOM, in the right time and place

to maximize its effects while maintaining the force protection of their units. Commercial SATCOM has the ability to revolutionize combat operations, as long as officers are able to effectively employ its full range of capabilities.

3. Integration at Large Scale Exercises

The Marine Corps conducts multiple iterations of its Marine Air-Ground Task Force Warfighting Exercise (MWX) each year. On top of MWX, dozens of other training exercises are conducted across the Marine Corps each year. To provide a realistic training environment, it is imperative that these exercises are designed with conditions that mimic future operating environments. With this in mind, exercise controllers need to look to integrate pLEO SATCOM into the training scenarios. Whether it includes use by Marine forces or simulated civilian use, there is no denying that commercially provided SATCOM will be increasingly apparent on the battlefield. Marines need to learn to operate in an increasingly more electronically complex environment both offensively and defensively.

B. FUTURE RESEARCH

1. Spectrum Evaluations

The Marine Corps should encourage the evaluation of pLEO SATCOM within the electromagnetic spectrum compared to legacy communications systems. A more robust understanding of the signatures that appear with the use of pLEO SATCOM will better shape the proper employment techniques. Also, a comparison should also be conducted analyzing data flow between commercial SATCOM and traditional communication platforms with the focus being on the differences in speed afforded by each system.

2. Unit Evaluations

A study should be conducted that evaluates the effectiveness of units operating with pLEO SATCOM in comparison to traditional communication equipment. Metrics could include an evaluation of operational range and time to receive data and then take action on that data. Furthermore, an evaluation of the correct number of systems needed to maximize a unit's potential should also be conducted.

C. CONCLUSION

The invasion of Ukraine has made it abundantly clear that commercial SATCOM is a feasible option for tactical units, especially Marine Corps Stand-In Forces. Stand-In Forces will be called upon to operate within close proximity of the enemy, participating in highly distributed operations requiring the ability to rapidly integrate sensor and shooter information to serve as the lynch pin for targeting networks. As seen in Ukraine, commercial SATCOM provides a robust and flexible infrastructure that ensures persistent communications while simultaneously hindering enemy ability to conduct uncontested EW operations. The mobility provided by the lightweight systems has been a distinct advantage for Ukrainian elements structured in a manner similar to Marine SIF units. At the same time, due to the commercial nature of the system, the Ukrainian military has benefited significantly from the luxury of industry support to maintain the functionality of the system. Furthermore, the implementation of pLEO SATCOM has ensured that Ukraine was able to counter the Russian information campaign by providing a robust link to the outside world. Both are lessons that the United States Marine Corps should look to replicate as it seeks similar successes on future battlefields.

The Ukrainian implementation of Starlink has demonstrated that properly employed commercial pLEO SATCOM is a valuable asset on the modern battlefield. For Marine units to be successful in future combat operations, the Corps needs to learn from the Ukrainian examples and experiment with the use of this continually growing technology. Given my findings, I believe that the Marine Corps should look to integrate commercial SATCOM with its tactical units as a means to succeed in more diverse, electromagnetic spectrum heavy future battlefields.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Albon, Courtney. "Spacecom Confirms Russian ASAT Test, Creating Debris Field." *Inside the Pentagon* 37, no. 46 Nov 18, 2021. ProQuest.
- Anderson, Michael G. "How Ukraine's Roving Teams of Light Infantry Helped Win the Battle of Sumy: Lessons for the U.S. Army." Modern War Institute, August 17, 2022. <https://mwi.usma.edu/how-ukraines-roving-teams-of-light-infantry-helped-win-the-battle-of-sumy-lessons-for-the-us-army/>.
- Bellingcat, "How EchoSec Found Evidence of a Russian Fighting in Ukraine." February 19, 2015. <https://www.bellingcat.com/news/uk-and-europe/2015/02/19/how-echosec-found-evidence-of-a-russian-fighting-in-ukraine/>.
- Berger, David H. "A Concept for Stand-In Forces." *Proceedings* 147, no. 11 November 2021. <https://www.usni.org/magazines/proceedings/2021/november/concept-stand-forces>
- Bonds, Timothy M., John E. Peters, Endy Y. Min, Lionel A. Galway, Jordan R. Fischbach, Eric S. Gons, Garrett D. Heath, and Jean M. Jones. *Army Network Enabled Operations*. Santa Monica, CA: RAND Corporation, 2012.
- Davenport, Christian. "Russia Threatens Commercial Satellites That Pentagon Sees as Its Future." *Washington Post*, October 29, 2022. <https://www.washingtonpost.com/technology/2022/10/28/space-war-ukraine-pentagon-russia/>.
- Dodge, Jonathan S., and James G. Carlton. "Using Commercial 5G And LEO Technologies To Enhance Navy-Army Sensor-To-Shooter Networks." Master's Thesis, Naval Postgraduate School, December 2022, <https://hdl.handle.net/10945/71449>.
- Ellis, Earl H., *Advanced Base Operations in Micronesia*, 712H Operational Plan, Quantico, VA: U.S. Marine Corps, 1921, https://www.google.com/books/edition/Advanced_Base_Operations_in_Micronesia/MRpL_niBIcYC?hl=en&gbpv=1&printsec=frontcover
- Elmasry, George F. Elmasry. *Tactical Wireless Communications and Networks*. Hoboken, NJ: John Wiley and Sons, Ltd., 2012, 261–274.
- Fidler, Stephen, and Thomas Grove. "Smartphones Are Changing the War in Ukraine." *Wall Street Journal*, February 16, 2023. <https://www.wsj.com/articles/smartphones-are-changing-the-war-in-ukraine-adb37ba1>.

- Gibbons-Neff, Thomas. "The Infrared Hunt for Russian Troops in the Battle for Bakhmut." *New York Times*. December 15, 2022. <https://www.nytimes.com/2022/12/15/world/europe/bakhmut-ukraine-russia-war.html>.
- Government Accountability Office. *The Civil Reserve Air Fleet – An Effective Program to Meet Defense Emergency Airlift Requirements*, GAO LCD-78-239 (Washington, DC: Government Accountability Office, 1978), 1–6.
- Gordon, Gary D. *Principles of Communications Satellites*. New York, NY: John Wiley and Sons, Inc., 1993.
- Horbyk, Roman. "'The War Phone': Mobile Communication on the Frontline in Eastern Ukraine." *Digital War* 3, no. 1 December 1, 2022: 9–24. <https://doi.org/10.1057/s42984-022-00049-2>.
- Hu, Rose Qingyang, and Yi Qian. *Heterogeneous Cellular Networks*, Hoboken, NJ: John Wiley and Sons Ltd, 2013, Chap. 1, 1–25, 2013. <https://doi.org/10.1002/9781118555262.ch1>.
- Insinna, Valerie. "SpaceX Beating Russian Jamming Attack Was 'Eyewatering': DOD Official." *Breaking Defense*, April 20, 2022. <https://breakingdefense.sites.brekingmedia.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/>.
- Jbeilly, Mark K. "Satellites in the Crosshairs," *Proceedings* 147, no. 6 (June 2021). <https://www.usni.org/magazines/proceedings/2021/june/satellites-crosshairs>.
- John, Veronica, "SpaceX Starlink Satellites to Operate in the Pacific," *Vanuatu Daily Post*, April 16, 2021, https://www.dailypost.vu/news/spacex-starlink-satellites-to-operate-in-the-pacific/article_71ed8298-9e40-11eb-bcd4-0b022f5709ea.html.
- Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations*, JP 3-85 Washington, DC: Joint Chiefs of Staff, 2020 I-7. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf
- Jones, Seth G., Riley McCabe, and Alexander Palmer. "Ukrainian Innovation in a War of Attrition," Center for Strategic and International Studies, February 27, 2023. <https://www.csis.org/analysis/ukrainian-innovation-war-attrition>.
- Kunertova, Dominika. "The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game." *Bulletin of the Atomic Scientists* 79, no. 2 March 4, 2023: 95–102. <https://doi.org/10.1080/00963402.2023.2178180>.
- Losey, Stephen. "Military Must Train to Fight When Communications Break Down: Experts" *Defense News*, April 24, 2023. <https://www.defensenews.com/battlefield-tech/2023/04/26/experts-military-must-train-to-fight-through-communications-breakdown/>.

- Losey, Stephen. "SpaceX Shut down a Russian Electromagnetic Warfare Attack in Ukraine Last Month — and the Pentagon Is Taking Notes." C4ISRNet, April 22, 2022. <https://www.c4isrnet.com/air/2022/04/20/spacex-shut-down-a-russian-electromagnetic-warfare-attack-in-ukraine-last-month-and-the-pentagon-is-taking-notes/>.
- Marine Corps Systems Command, "Mobile Satellite System Reduces Communication Gaps, Increases Naval Interoperability," <https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/2872370/mobile-satellite-system-reduces-communication-gaps-increases-naval-interoperabi/>.
- Marine Corps Systems Command. "Mobile Satellite System Reduces Communication Gaps, Increases Naval Interoperability." Accessed May 2, 2023. <https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/2872370/mobile-satellite-system-reduces-communication-gaps-increases-naval-interoperabi/https%3A%2F%2Fwww.marcorsyscom.marines.mil%2FNews%2FNews-Article-Display%2FArticle%2F2872370%2Fmobile-satellite-system-reduces-communication-gaps-increases-naval-interoperabi%2F>.
- McCrory, Duncan. "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States." *The RUSI Journal* 165, no. 7 November 9, 2020: 34–44. <https://doi.org/10.1080/03071847.2021.1888654>.
- Militaryni. "Starlink Has Become Indispensable for Ukrainian Gunners." 22 October, 2022. <https://mil.in.ua/en/news/starlink-has-become-indispensable-for-ukrainian-gunners/>.
- Mills, Walker. "A Tool For Deception: The Urgent Need For EM Decoys." *War Room – U.S. Army War College*, February 27, 2020. <https://warroom.armywarcollege.edu/articles/tactical-decoys/>.
- Milowicki, Gene V., and Joan Johnson-Freese. "Strategic Choices: Examining the United States Military Response to the Chinese Anti-Satellite Test." *Astropolitics* 6, no. 1 March 10, 2008: 1–21. <https://doi.org/10.1080/14777620801907913>.
- Moellering, Matthew. "Hiding in the Noise: Preparing the Irregular Warfare Community for the Age of AI." Modern War Institute, September 26, 2022. <https://mwi.usma.edu/hiding-in-the-noise-preparing-the-irregular-warfare-community-for-the-age-of-ai/>.
- New York Times*, "Maps: Tracking the Russian Invasion of Ukraine." February 14, 2022. <https://www.nytimes.com/interactive/2022/world/europe/ukraine-maps.html>.

- O'Neill, Patrick Howell. "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion." MIT Technology Review, May 10, 2022. <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.
- Poisel, Richard A. *Information Warfare and Electronic Warfare Systems*. Artech House Electronic Warfare Library. Norwood: Artech House, 2013, 332.
- Politico, "Elon Musk's SpaceX Restricts Ukraine's Use of Its Satellite Internet for Drones," February 9, 2023. <https://www.politico.eu/article/elon-musk-spacex-restricts-ukraine-use-of-its-satellite-internet-for-drone-control/>.
- Roulette, Joey. "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones -Company President." *Reuters*, February 2023. <https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/>.
- Ryan, Michael J., and Michael R. Frater. *Tactical Communications for the Digitized Battlefield*. Boston, MA: Artech House, 2002, 79.
- Satellite Today*, "US Military Places a Bet on LEO." June 3, 2021. ProQuest.
- Seck, Hope Hodge. "Ukraine Lessons Take Center Stage in Marines' New Information Warfare Plan." *Marine Corps Times*, June 29, 2022. <https://www.marinecorpstimes.com/news/your-marine-corps/2022/06/29/ukraine-lessons-take-center-stage-in-marines-corps-new-information-warfare-plan/>.
- Skove, Sam. "Using Starlink Paints a Target on Ukrainian Troops." *Defense One*, March 23, 2023. <https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/>.
- Space Development Agency. "FAQ – Space Development Agency." Accessed May 1, 2023. <https://www.sda.mil/home/about-us/faq/>.
- U.S. Department of State. "U.S. Security Cooperation with Ukraine." Washington, DC: Department of State May 2023. <https://www.state.gov/u-s-security-cooperation-with-ukraine/>.
- U.S. Marine Corps, *A Concept for Stand-In Forces*, Arlington, VA: U.S. Marine Corps, December 2021.
- U.S. Marine Corps, *Commandant's Planning Guidance*, Arlington, VA: U.S. Marine Corps, 2019.
- U.S. Marine Corps, *EP EMCON SOP: A Guide to Reduce Technical Signature*, Virginia Beach, VA: Marine Corps Intelligence Schools, 2020.

U.S. Marine Corps, *Force Design 2030*, Arlington, VA: U.S. Marine Corps, March 2020.

U.S. Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations*, 1st Ed. Washington, DC: U.S. Marine Corps, 2021.

U.S. Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations*, 2nd Ed. Washington, DC: U.S. Marine Corps, 2023.

VanderMeulen, Richard, and Bruce Cathell. “High Capacity Satellite Communications-Cost Effective Bandwidth Technology.” Presentation, 31st Space Symposium, Colorado Springs, CO, April 2015.

Wall Street Journal. “Soldiers in Ukraine Say Some Drones Affected After SpaceX Limits Starlink.” February 10, 2023. <https://www.wsj.com/articles/soldiers-in-ukraine-say-some-drones-affected-after-spacex-limits-starlink-321a9dd7>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

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



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE