NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CLANDESTINE COMMUNICATIONS FOR THE 21ST-CENTURY INSURGENT

by

Mitchell J. Gunter

June 2023

Thesis Advisor: Raymond R. Buettner Jr.
Co-Advisor: Gordon H. McCormick

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
CLANDESTINE COMMUNICATIONS FOR THE 21ST CENTURY INSURGENT

5. FUNDING NUMBERS

6. AUTHOR(S) Mitchell J. Gunter

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 resurgence of Great Power Competition and the approaching era of conventional military parity in the Pacific emphasizes the need for force multiplicative strategies inclusive of irregular warfare activities. Irregular forces may soon become a primary method of power projection and competition within regions contested by Great Power Competitors. One critical aspect of enabling and employing irregular forces is the provision of concealed or protected communications resources. The purpose of this thesis is to model the predicted impact of clandestine communications support to irregular forces, identify emergent commercial technologies that may be repurposed into clandestine mediums, and highlight the role of irregular forces and requisite clandestine communications within NATO's Comprehensive Defense Strategy and the U.S. Marine Corps Expeditionary Advanced Base Operations.

This thesis finds that aid to clandestine communications may drastically improve the operational capacity of proxy forces. Further, this thesis finds that clandestine communications may be securely transmitted via steganographic embedding in virtual environments and pLEO satellite downlinks. However, current naval and amphibious operations lack training, education, and modern employment mechanisms for irregular warfare activities. This thesis recommends that the U.S. Navy and Marine Corps immediately adopt and employ irregular warfare activities within their power projection and deterrence strategies.

14. SUBJECT TERMS clandestine communications, virtual environments, proliferated low earth orbit, pLEO, insurgent, insurgency, emergent technologies, communications, satellites, security, clandestine, covert, unconventional, steganography, Expeditionary Advanced Base Operations, EABO, Comprehensive Defense, NATO, NATO Special Forces Headquarters	**15. NUMBER OF PAGES** 147
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CLANDESTINE COMMUNICATIONS FOR THE 21ST CENTURY INSURGENT

Mitchell J. Gunter
Captain, United States Marine Corps
BS, United States Naval Academy, 2017

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

and

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

NAVAL POSTGRADUATE SCHOOL
June 2023

Approved by: Raymond R. Buettner Jr.
Advisor

Gordon H. McCormick
Co-Advisor

Alex Bordetsky
Chair, Department of Information Sciences

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The resurgence of Great Power Competition and the approaching era of conventional military parity in the Pacific emphasizes the need for force multiplicative strategies inclusive of irregular warfare activities. Irregular forces may soon become a primary method of power projection and competition within regions contested by Great Power Competitors. One critical aspect of enabling and employing irregular forces is the provision of concealed or protected communications resources. The purpose of this thesis is to model the predicted impact of clandestine communications support to irregular forces, identify emergent commercial technologies that may be repurposed into clandestine mediums, and highlight the role of irregular forces and requisite clandestine communications within NATO's Comprehensive Defense Strategy and the U.S. Marine Corps Expeditionary Advanced Base Operations.

This thesis finds that aid to clandestine communications may drastically improve the operational capacity of proxy forces. Further, this thesis finds that clandestine communications may be securely transmitted via steganographic embedding in virtual environments and pLEO satellite downlinks. However, current naval and amphibious operations lack training, education, and modern employment mechanisms for irregular warfare activities. This thesis recommends that the U.S. Navy and Marine Corps immediately adopt and employ irregular warfare activities within their power projection and deterrence strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADC	Asymmetric Defense Component
ADT	Acoustic Data Transmission
AIB	Allied Intelligence Bureau
EABO	Expeditionary Advanced Base Operations
EP	Electronic Protection
ESRB	Entertainment Software Rating Board
EW	Electronic Warfare
GEO	Geosynchronous Orbit
GHQ	General Headquarters
GWOT	Global War on Terror
IFFT	Inverse Fast Fourier Transform
IW	Irregular Warfare
JGSDF	Japan Ground Self Defense Force
JOC	Joint Operating Concept
LEO	Low Earth Orbit
MBPS	Megabits Per Second
MCC-IS	Mobile Communication Company of Iran
MMORPG	Massively Multiplayer Online Role Player Game
NASA	National Aeronautics Space Administration
NATO	North Atlantic Treaty Organization
NSHQ	NATO Special Operations Headquarters
OFDM	Orthogonal Frequency Division Multiplexing
OSS	Office of Strategic Services
PIPL	Personal Information Protection Law
PLAN	People's Liberation Army-Navy (China)
pLEO	Proliferated Low Earth Orbit
QR	Quick Response Code

TM-EABO	Tentative Manual for Expeditionary Advanced Base Operations
USAID	United States Agency for International Development
USFIP	United States Forces in the Philippines
USMC	United States Marine Corps
USSOCOM	United States Special Operations Command
VE	Virtual Environment
VSAT	Very Small Aperture Terminal
WEZ	Weapons Engagement Zone
Wi-Fi	Wireless Fidelity

EXECUTIVE SUMMARY

A. INTRODUCTION

The approaching era of conventional military parity in the Pacific between the United States and China has fostered a resurgence in the strategic importance of irregular warfare techniques and methodologies. Specifically, the cultivation and employment of proxy organizations and guerrilla forces may once again become primary methods of power projection and competition within contested regions located on the geographic periphery of Great Power Competitors. As proxy forces may serve as critical force multipliers or supporting elements within larger conventional military campaigns, it is absolutely paramount that the U.S. and its allies prepare to cultivate, activate, and employ these forces globally.

One critical aspect of enabling and employing irregular forces, especially in contested or denied regions, is the provision of concealed or protected communications resources. The purpose of this thesis is to model the predicted impact of clandestine communications support to insurgent organizations, identify emergent commercial technologies that may be repurposed into clandestine communications mediums, and to highlight the role and importance of insurgent organizations and requisite clandestine communication technologies within emergent military doctrine.

If the United States seeks to maintain its power projection capabilities in the Pacific and beyond, it must innovate and employ irregular warfare techniques to supplant its growingly contested conventional military capacity.

B. MODELING INSURGENT CAPACITY

To quantify the operational capacity provided by an insurgent organization or cell, this thesis uses the models of insurgent operational capacity provided by McCormick and Owen's "Security and Coordination in a Clandestine Organization."[1] According to

[1] Gordon H. McCormick and G. Owen. "Security and Coordination in a Clandestine Organization." *Mathematical and Computer Modelling* 31, no. 6–7 (May 2000): 175–192. https://doi.org/10.1016/s0895-7177(00)00050-9.

McCormick and Owen, insurgent cells experience operational capacity growth in tandem with increases in organizational membership subject to diminishing marginal returns and efficiency related limitations.[2] This thesis proposes that, in addition to the framework provided by McCormick and Owen, the impact of emergent technologies – specifically those that conceal or protect data transmissions—may be modeled as an additional scaling variable that demonstrates the net positive impact imparted by technology on an insurgency's operational capacity.

This thesis proposes that an additional Technology Scaling Variable (C_j) be included to capture the positive scaling effects of access to protected internet resources and clandestine mediums. Based on the hypothesis that emergent communications technologies provide insurgent organizations with more effective internal communication as well as greater reach in external, recruitment-oriented communications, the Technology Scaling Variable may be defined as:

$$Technology\ Scaling\ Variable, \qquad C_j = \frac{(1 + Q_j)}{(1 - P_j)}$$

Within this proposed equation, variable Q_j represents the percentage of a population with access to concealed communications mediums, and variable P_j represents the percentage of a population with access to protected communications mediums. When calculating an insurgent cell's operational capacity, the inclusion of this Technology Scaling Variable allows military planners to visualize operational impacts and allocate resources in such a manner that maximizes the utility of resource investments and the efficacy of the supported insurgent organization.

C. EMERGENT TECHNOLOGIES AND CLANDESTINE COMMUNICATIONS

In order to identify and evaluate emergent technologies as potential channels for clandestine communications, this thesis proposes that in order for a technology to serve as

[2] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 175–178.

a viable medium for the transmission of insurgent communications it must meet four general requirements:

1. The technology must be commercially available.
2. The technology must have minimal complexity or training requirements.
3. The technology must be concealing or protective of data transmissions.
4. The technology must be capable of transmitting insurgent messages both internally within the organization and externally to the public in a timely manner.

In applying these criteria to emergent technological trends, this thesis identifies virtual environments and proliferated low-earth orbit-based (pLEO) satellite communications as potential channels for clandestine communication. By pairing virtual environments with historical methods of clandestine tradecraft, this thesis proposes that "virtual clandestine tradecraft," the use of virtual environments—specifically those provided by commercially available videogames—may be utilized as steganographic mediums and distribution networks for insurgent communications. Similarly, proliferated low-earth orbit satellite communications also satisfy the evaluation criteria and may be employed as protected mediums for insurgent data transmission. This thesis uses case studies containing videogame-generated graphics and modeled evaluations of real-world insurgent activity to highlight the use and applicability of these technologies as mediums for modern clandestine communications.

D. INSURGENCY AND EMERGENT MILITARY DOCTRINE

The employment of proxy organizations and irregular warfare techniques will undoubtedly be a critical aspect of future competition and conflict. Just as the Allied Intelligence Bureau (AIB) employed Filipino guerrillas to counter the conventionally superior Imperial Japanese military, the U.S. and its allies may similarly rely on insurgent espionage and sabotage networks to counteract the growing influence of strategic competitors in the Pacific and Eastern Europe.

Emergent military doctrines like the United States Marine Corps Tentative Manual for EABO (TM-EABO) and NATO Special Operations Headquarters' Comprehensive Defense Manual are prime examples of the pivot towards irregular warfare as both a deterrent force and an element of power projection. However, while this emergent doctrine recognizes the importance of irregular warfare techniques and activities, this thesis finds the U.S. Marine Corps' adoption of these strategies to be solely an administrative one. Currently, the U.S. Marine Corps training and international cooperation efforts are almost exclusively centered on conventional military cooperation or naval integration efforts and are fundamentally lacking in the application of irregular warfare methodologies.

E. CONCLUSION

This thesis finds that improvements in clandestine communications channels may impart significant increases in the operational capacity of irregular or proxy forces. By providing irregular forces with increased communications security and data transmission capacity, an external enabler may drastically increase the tactical and operational capacity borne of an allied non-state actor. Further, this thesis identifies virtual environments and proliferated low earth orbit satellite constellations as viable mediums for the transmission of clandestine communications. Both virtual environments and pLEO satellite communications are commercially available, operationally simplistic, concealing or protective of data transmission, and viable mediums for clandestine communications as exhibited in the virtual demonstrations and historical case studies contained within this thesis.

Despite the United States' waning conventional supremacy in the Pacific and beyond, the codified employment and force multiplicative effects of allied irregular forces are currently confined to emergent military doctrine. This thesis recommends that conventional naval and amphibious operations adapt to include and employ the operational capacity borne of non-state irregular forces. Current international training exercises and operations observably lack the inclusion and employment of irregular forces. This thesis recommends that indigenous proxy forces be included as operational elements within all future joint and international training exercises in the Pacific.

Proxy organizations and irregular warfare techniques may potentially serve as critical operational stopgaps for the United States' contested military capacity in localized regions on the periphery of Great Power Competitors. By modeling insurgent capacity, military planners may maximize the operational output of an allied proxy force. And further, by identifying and facilitating emergent technologies as channels for clandestine communications, military planners may cultivate and employ proxy organizations as force multipliers for conventional military operations or as deterrent organizations against the aggressive expansion of strategic competitors like China or Russia. Only by integrating irregular warfare as a supplement to conventional strategy and fostering alliances with global insurgent populations will the United States successfully defend its interests abroad in the coming competition and potential future conflict.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is dedicated to Chief Warrant Officer Joshua Levine, USMC.

Josh, thank you for inadvertently setting me on this path and for being a steadfast exemplar of leadership, ethics, innovation, and common sense. The Corps is a better place for having you all these years.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE ROLE OF INSURGENCY IN MODERN CONFLICT

The United States and its allies are entering into an era of global strategic competition wherein their previous military advantages are no longer decisive indicators of success in armed conflict. As global competitors like the Russian Federation and the Chinese Communist Party expand their military capacity, political predominance, social influence, and economic leverage over their geographic peripheries, it is paramount that the U.S. and its allies incorporate irregular warfare activities (insurgencies) as both instruments of international statecraft and supplements to conventional military operations.

The Chinese Communist Party, in particular, is a pacing threat to the U.S. While the United States maintains primacy as the world's predominant superpower, this advantage exists primarily as a numerical comparison and is agnostic of localized military capacity. For example, if the Chinese escalate a conflict with Taiwan, it is possible that the United States will not be able to provide the decisive military intervention required to defend the Taiwanese landmass. The precision strike, air, surface, and undersea capacity of the People's Liberation Army-Navy (PLAN) in the northwestern Pacific is—locally—asymmetrically advantaged over any forward-deployed adversary.[1]

To meet the global requirements expected of a preeminent superpower, the United States must thus seek to employ additional supplementary activities to bolster the defenses of its geographically disparate allies. To adequately deter its adversaries and defend the sovereignty of its allies, the U.S. must reestablish its primacy within the now-contested military domain. Within this effort, insurgent movements, guerrilla networks, and clandestine activities must be employed to supplement conventional military capacity. On battlefields and in campaigns wherein all parties are equally advantaged in conventional

[1] Eric Edelman et al., *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: National Defense Strategy Commission, 2018), https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

military capacity, irregular operations may yet serve as the deciding factor in the success or failure of a military operation and perhaps the overall conflict itself.

B. INSURGENT COMMUNICATIONS

Communicative capacity is critical to an insurgent organization's recruitment, education, employment, and security. For countries seeking to create, leverage, or empower civilian insurgent movements in support of conventional military operations, the provision of protected, clandestine communication technologies and methodologies is a critical enabling factor. This thesis addresses the role of communications within an insurgent movement, the importance of technology to communicative capacity, and the growing responsibility of U.S. and allied forces to establish clandestine and covert networks of insurgent movements in support of their overall defensive and deterrent postures.

The role of communications technologies and techniques will be evaluated using various frameworks in order to analyze and depict the potential gains and losses they impart on an insurgent organization's operational capacity. Using mathematical models provided by Professors McCormick and Owen in "Security and Coordination in a Clandestine Organization," as a foundation for further analysis, this thesis will propose updated modeling considerations to include the role of emergent technology and their ability to provide protection and concealment against adversarial targeting efforts.[2]

C. EMERGENT COMMUNICATIONS TECHNOLOGIES

Using the analytical framework provided in "Security and Coordination in a Clandestine Organization" by Professors McCormick and Owen, this thesis will identify the potential gains in communicative capacity created by emergent technologies such as Proliferated Low Earth Orbit (pLEO) satellite technology and Virtual Environment (VE) based communication mediums.[3] This thesis will address case studies and potential

[2] Gordon H. McCormick and G. Owen. "Security and Coordination in a Clandestine Organization," *Mathematical and Computer Modelling* 31, no. 6–7 (May 2000): 175–192. https://doi.org/10.1016/s0895-7177(00)00050-9.

[3] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 175–192.

employment methods for both of the technologies listed above. Additionally, one to two potential clandestine or covert communications methods will be evaluated for each category with regard to their security, availability, usability, and survivability in physically and electromagnetically contested terrain.

D. ENABLING INSURGENCY

The last section of this thesis will identify the growing responsibility of military organizations like the United States Marine Corps (USMC), United States Special Operations Command (USSOCOM), and NATO Special Operations Headquarters (NSHQ) to both enable and integrate with insurgent organizations against Great Power Competitors. Decades of counter-terrorism operations by U.S. and allied forces have eroded our competitive and technological military advantage over our adversaries.[4] This strategic atrophy of our overall warfighting capacity has also seen a decline in our military's use and support for large-scale insurgent operations and proxy forces. To compete with adversaries of technological and conventional military parity, the U.S. must reestablish its ability to leverage large-scale, supplementary irregular warfare activities.

Specifically, it is paramount that the United States Marine Corps, U.S. Special Forces Command, and NATO Special Forces adopt the use and employment of insurgent organizations as dictated within the Tentative Manual for Expeditionary Advanced Base Operations (TM-EABO) and Comprehensive Defense Manuals, respectively.

[4] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: 2018). https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. BACKGROUND

1. Insurgent Competition

While much of the past two decades of U.S. military operations has been dedicated to counter-insurgency efforts in support of the Global War on Terror (GWOT), the study and application of pro-insurgency tradecraft may still be found in academia and operational publications made by elements of the U.S. Special Operations Command. As the United States pivots towards a return to the operational employment of insurgent organizations, these publications and analytical models become increasingly important for military leaders' understanding of clandestine insurgent movements. In order to optimize the support and efficacy of supplementary insurgent operations, leaders must first understand the nature of insurgent movements and leverage their strengths to maximize operational capacity and minimize vulnerability.

For this thesis' evaluation of modern insurgent operations, the life cycle, activities, and survivability of an insurgent organization will be modeled using the S-shaped operational capacity curve provided by McCormick and Owen's "Security and Organization in a Clandestine Organization," McCormick's "Diamond" Counterinsurgency Model, and the analytical framework provided in McCormick and Giordano's "Things Come Together: Symbolic Violence and Guerrilla Mobilization."[5] The viewpoints provided in these articles are critical to understanding insurgent movements and the role of communications in a clandestine organization. Ultimately, insurgent movements experience phased periods of growth, activity, and decline defined by the characteristics of the local population, the success of the insurgency's recruitment

[5] Gordon H. McCormick and Frank Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," *Third World Quarterly* 28, no. 2 (2007): 295–320. https://doi.org/10.1080/01436590601153705; Michael Freeman, Hy S. Rothstein, and Greg Wilson. "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," Essay. In *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, 15–20. Monterey, CA: Naval Postgraduate School, Department of Defense Analysis, 2011; McCormick and Owen, "Security and Coordination in a Clandestine Organization," 175–192.

efforts, and attrition at the hands of the state or conventional military opposition.[6] Thus, the existence and activities of an insurgent organization may be viewed through the analytical lens of a competition wherein an insurgent organization is competing against a conventional adversary like a standing government or encroaching military force for the support of a civilian population and control of a contested region.[7] This insurgent competition is further enabled by communicative technologies, clandestine human networks, and international intervention—culminating in a militarized effort against an established and conventional adversary.[8]

This competitive relationship between insurgent movements and their governmental opponents is best demonstrated in McCormick's Diamond Counterinsurgency Model (Figure 1), wherein each player—the insurgency and the conventional force—interacts with both the civilian population of a contested region and a compilation of international actors in order to garner public support and establish legitimacy.[9]

[6] McCormick and Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," 301.

[7] Freeman, Rothstein, and Wilson, "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," 15–16.

[8] McCormick and Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," 301.

[9] Freeman, Rothstein, and Wilson, "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," 15–16.

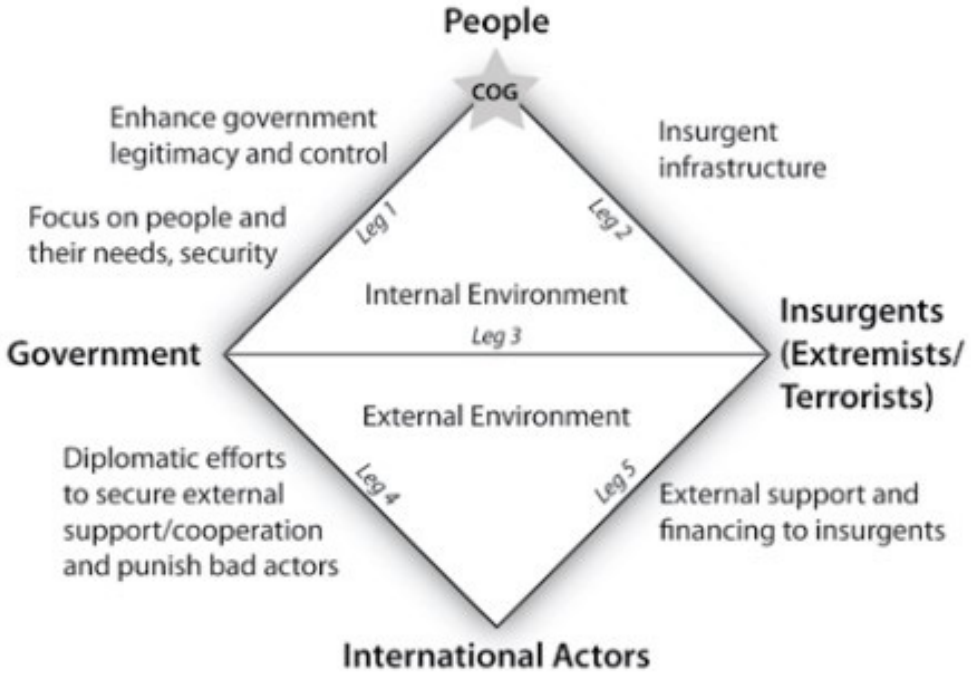

Figure 1. Gordon McCormick's Diamond Counterinsurgency Model.[10]

Furthermore, using the framework provided in "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," the population of a contested region may be divided into three categories—supporters of the insurgency, supporters of the state, or individuals who support neither side.[11] Within this framework, an insurgency must recruit individuals from the latter two categories while preventing the adversarial group from recruiting or eliminating their current membership.[12] Critical to these efforts is the insurgent movement's ability to recruit and operationalize members of the civilian public without attracting unwanted attention or incurring the targeting efforts of their of the conventional opponent within the contested region. This thesis will not focus on the social, political,

[10] Source: Greg Wilson and Hy Rothstein, "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," Essay. In *Gangs and Guerrillas – Ideas from Counterinsurgency and Counterterrorism*, edited by Michael Freeman, 15–21. Monterey, CA: Naval Postgraduate School, 20111.

[11] McCormick and Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," 301.

[12] McCormick and Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," 313.

economic, or other motivating factors that are responsible for converting civilian populations into militant insurgencies; rather it will focus on key enabling factors like communicative capacity and operational security that allow an insurgency to recruit members and increase its operational capacity. The following sections of this literature review will address the key relationships between security, coordination, technology, and external support that are critical enabling factors for the operations and survivability of an insurgent organization.

B. SECURITY AND COORDINATION: AN ANALYTICAL FRAMEWORK

1. Operational Trade-Offs in Insurgent Communication

The foundational relationship between an insurgency and its communicative capacity is best demonstrated in "Security and Coordination in a Clandestine Organization" by Professors McCormick and Owen of the Naval Postgraduate School.[13] Within this framework, an insurgent organization trades operational security for operational capacity via the activation and use of clandestine communication networks.[14] This model asserts that insurgent communications are subject to targeting efforts by the adversary's intelligence apparatus and are inherently risky for the insurgency. Furthermore, insurgent organizations benefit from clandestine communication networks with lower probabilities of detection and are able to communicate and operate more effectively with less risk.

2. Modeling Operational Capacity

In order for an insurgent organization to successfully compete against a conventionally advantaged opponent, it must maximize its operational capacity while minimizing its exposure to the intelligence, surveillance, and targeting efforts of the adversary. McCormick and Owen hypothesize that the operational capacity of an insurgent organization may be modeled as an S-shaped curve ultimately defined by the number of members within the organization and the governing assumption that there will be diminishing marginal returns to additional members associated with difficulties in

[13] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 175.

[14] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 175.

supervision, control, and management of a larger insurgent population.[15] Viewing the positive correlational relationship between operational capacity and cell membership (Figure 2), it is clear that in order for an insurgent movement to succeed, it must actively increase its membership in order to maximize its operational capacity. McCormick and Owen stipulate that operational capacity is also subject to scaling associated with effective coordination and successful communication transmission.[16] Because the existence and activities of an insurgency are conducted in contested physical, digital, and electromagnetic terrain, it is possible—and likely—that the communications channels employed by the insurgency will be subject to degradation and surveillance by the adversary.

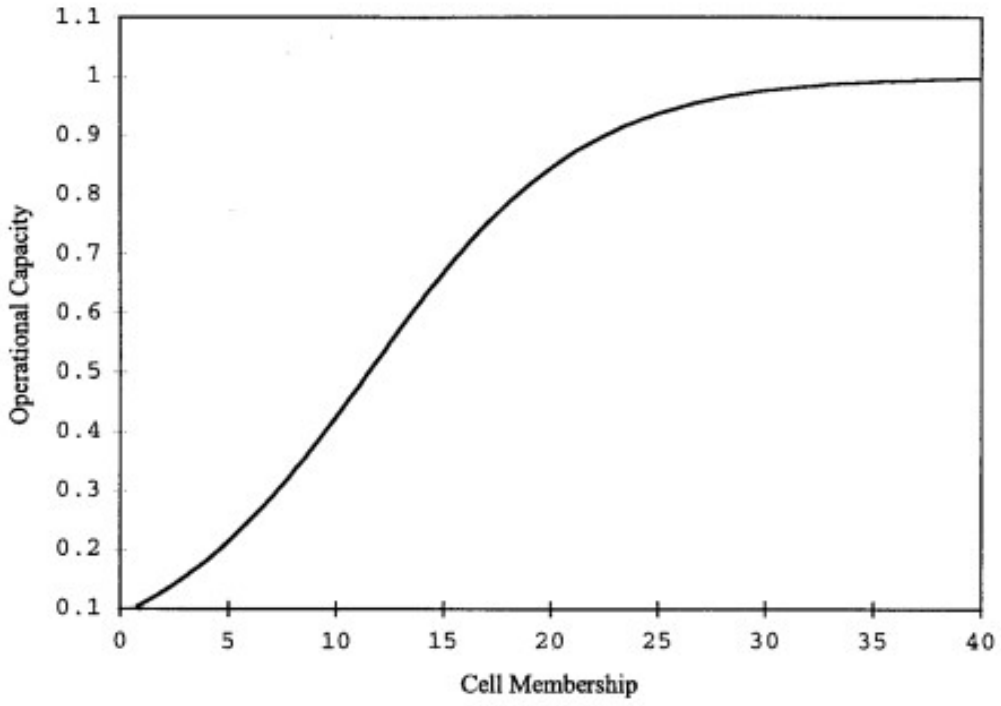

Figure 2. Insurgent Operational Capacity versus Cell Membership.[17]

[15] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177–178.

[16] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177–178.

[17] Source: McCormick and Owen, "Security and Coordination in a Clandestine Organization," 178.

3. Modeling Organizational Risk

As an insurgent organization competes for the support of the local populace, it must successfully publicize its cause, recruit members, coordinate internally, and conduct rudimentary guerrilla warfare education amidst its ranks.[18] These core tasks are foundational activities in the insurgent organization's ability to develop its operational capacity. Furthermore, underlying each of these activities, insurgent communications are the enabling and limiting determinants of success. Within the insurgent competition framework, communications are key enablers and vulnerabilities for the insurgency. From the perspective of the insurgency, communication and operational capacity are positively correlated. However, in a contradictory manner, communications and the likelihood of detection and destruction are also positively related. For the conventional adversary to target and attrite elements of the insurgency, they must detect insurgent communications and execute a kill chain or web against nodes within the insurgent network. Thus, the operational security of an insurgent organization is dependent on the security of the communications and the interconnectivity of the insurgent cells within the overarching network.

As demonstrated in Figures 3 and 4, two hypothetical insurgent organizations with the same number of cells (nodes 1–8) and located in the same notional geographic regions (rings 1–3) may have different communications architectures and levels of interconnectivity. For the purposes of this analytical evaluation, the solid lines between numbered insurgent cells represent an unprotected form of communication. Thus, as the cell depicted in Figure 4 exhibits a higher level of unprotected connectivity than the cell in Figure 3, it is inherently more vulnerable to the targeting and attrition of an adversary's intelligence operations.

[18] Gordon H. McCormick, "The Shining Path and Peruvian Terrorism," *Journal of Strategic Studies* 10, no. 4 (1987): 114. https://doi.org/10.1080/01402398708437317.

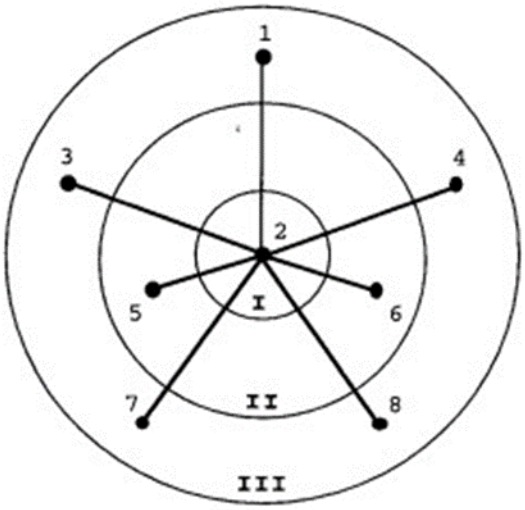

Figure 3. Network Diagram: Insurgency with Low Interconnectivity.[19]

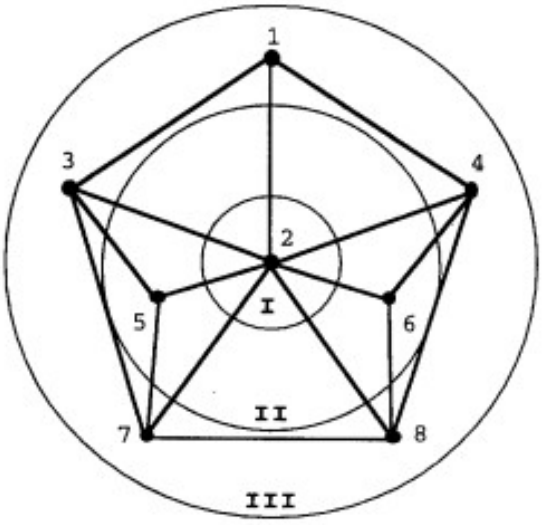

Figure 4. Network Diagram: Insurgency with High Interconnectivity.[20]

Within the insurgent competition, detection may result in the targeting and destruction of elements of the insurgency. Conversely, for a conventional military

[19] Source: McCormick and Owen, "Security and Coordination in a Clandestine Organization," 182.

[20] Source: McCormick and Owen, "Security and Coordination in a Clandestine Organization," 182.

intelligence apparatus seeking to attrite an insurgent competitor, the unprotected communication connections between insurgent cells serve as target indicators that may establish the threat validity, target identification, target location, optimal weaponeering solutions, and expected effects that are required for the completion of a pre-strike, target detection and development operation.[21] This phenomenon is confirmed in the comparative analysis made by McCormick and Owen's "Security and Coordination in a Clandestine Organization." Using a hypothetical set of probabilities aligned to insurgent risk, detection, and operational capacity, McCormick and Owen demonstrate that within the S-Shaped operational capacity curve, highly interconnected insurgent organizations (with higher numbers of intercell links) have greater expected operational capacities and likewise greater vulnerability to targeting whereas less interconnected organizations (with lower numbers of intercell links) have lower expected operational capacities but maintain lower vulnerabilities to targeting and destruction.[22] Additionally, McCormick and Owen demonstrate the value of protected lines of communication over unprotected lines by comparing estimated organizational vulnerability and predicted attrition (via adversary targeting). In the comparative analysis between insurgent organizations using secure versus nonsecure communications channels, the net expected capacity of insurgencies using secure communications is higher, and intuitively the risk borne of these protected communications is less imposing on the organization, resulting in less targeting and destruction of elements of the insurgency.[23]

The foundational relationship between the organization, communications, and insurgent security has persisted across centuries of conflict and eras of technology. Mao Tse-tung's Yu Chi Chan (Guerrilla Warfare)—guerrilla warfare doctrine borne of the 1937

[21] David H. Petraeus, James F. Amos, and John A. Nagl. "Targeting," Essay. In The U.S. Army/ Marine Corps Counterinsurgency Field Manual U.S. Army Field Manual No. 3–24: Marine Corps Warfighting Publication No. 3–33.5, 191–96. Chicago, IL: University of Chicago Press, 2007.

[22] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 184.

[23] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 184.

Japanese Imperial Army's invasion of China—remarks that "unorganized guerrilla warfare cannot contribute to victory."[24]

C. CLANDESTINE COMMUNICATIONS

Above all, secrecy is a keystone within an insurgent organization's ability to defend itself against the detection and targeting efforts of its opponent within the insurgent competition. For an insurgent organization to be effective, it must be able to disseminate information, communicate leadership decisions, and coordinate activities without being detected or surveilled by the intelligence monitoring of the state or encroaching conventional adversary.[25] The capability to conduct secure, secret, and timely communications is not a trivial one, however, and the costs of acquiring protected communications channels may force an insurgency to adopt less secure communications mediums in order to maintain operational continuity.[26] Clandestine communications channels—therefore—are the ideal medium for an insurgent organization seeking to maximize its stealth capacity while conducting operations.

Joint Publication 1-02—the Department of Defense Dictionary of Military and Associated Terms—defines "clandestine" as "any activity or operation sponsored or conducted by governmental agencies with the intent to assure secrecy and concealment."[27] A clandestine operation must conceal its very existence, as the mere detection of its presence betrays its subversive intent.[28] These definitions, when applied to the context of insurgent communications, highlight the operational need for secret communications networks that are both unknown to the adversary and protected against said adversary's

---

[24] Mao Tse-Tung, "What Is Guerrilla Warfare?" Essay. In On Guerrilla Warfare – Translated and with an Introduction by Brigadier General Samuel B. Smith USMC (Ret.), 43–51. New York, NY: Praeger, 1961.

[25] J. Bowyer Bell, "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence* 3, no. 1 (1989): 15–43. https://doi.org/10.1080/08850608908435089.

[26] Bell, "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem," 41.

[27] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington, DC: Joint Chiefs of Staff, 2010), https://dcsg9.army.mil/assets/docs/dod-terms.pdf.

[28] Andrew R. Molnar, "Definitions of Clandestine and Covert Behavior," Essay. In *Human Factors Considerations of Undergrounds in Insurgencies.* 101–2. Washington, DC: U.S. Army Headquarters, 1966.

efforts to detect, identify, or surveil message traffic. Unlike underground movements and insurgencies of decades past, modern insurgent movements must contend with intelligence and surveillance threats of a modernized digital information environment. The evolution of insurgent statecraft must advance in order to counter the surveillant capacity of nation-states' control over digital infrastructure and telecommunications providers. For example, Article 71 of the Russian Constitution and Government Decree 2385, issued in December 2020, stipulate that digital telecommunications data on Russian users and/or transmitted through Russian telecommunications providers is subject to the regulation, examination, and protection of the Russian government and its associated intelligence agencies.[29] Similarly, the "National Intelligence Law (2017)" enacted by the People's Republic of China officially sanctions a deliberate integration of private industry and state-level intelligence collection activities.[30] Under Article 7 of this national legislation, all Chinese organizations, companies, and individuals are compelled to cooperate with state intelligence. Furthermore, under Article 11, this coerced cooperation is extended to overseas entities and individuals, ensuring that the Chinese state intelligence is able to leverage private companies abroad to achieve their intelligence collection and surveillance goals.[31]

In order for an insurgency to achieve clandestine communications in the digital environment of the 2020s and onward, it must either circumvent potentially compromised digital infrastructures or conceal itself within normal civilian data flows. Using new technologies, old technologies in innovative ways, or by embedding clandestine communications within the almost incomprehensible volume of daily digital transmissions,

[29] Walter Sapranov, "Telecoms, Media, and Internet Report: Russia," ICLG.com. International Comparative Legal Guides, accessed May 1, 2023, https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/Russia.

[30] Canadian Security Intelligence Service, "China's Intelligence Law and the Country's Future Intelligence Competitions," Government of Canada, May 17, 2018. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html.

[31] 12th Chinese National People's Congress, National Intelligence Law of the People's Republic (2017). https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

an insurgency may achieve the secrecy it needs to communicate effectively without being detected and destroyed by its competitor within the insurgent competition.

D. EMERGENT TECHNOLOGIES

If communications are the keystone in an insurgency's bid for success, the technology it uses is the mortar holding its operations together. To successfully recruit members, coordinate activities, and leverage leadership decisions, an insurgency must outmaneuver the spying eyes of its adversaries. It is expected that the insurgency will be asymmetrically disadvantaged in terms of technological capacity and infrastructure. Thus, a modern insurgency's success depends on its ability to innovate clandestine communication channels from commercially available technologies or by repurposing existing forms of communication into clandestine mediums. This thesis will focus on two emergent technologies—virtual environments and proliferated low-earth orbit satellite technologies.

1. Virtual Environments

For this thesis' analysis of insurgent communications, virtual environments will be defined as computer-generated displays that allow users to experience and interact with each other and/or elements of simulated multidimensional environments. Critical to this definition is the multi-user or collaborative nature of a shared simulated environment; in order for a virtual environment to bear communicative capacity, it must enable interaction (data transmission between users).[32] This thesis will continue the work started by Ryan Rippeon's "Clandestine Message Passing in Virtual Environments" to include considerations of virtual environment technologies and trends that have emerged in the intervening 14 years as well as a shift in operational focus to enabling insurgencies vice combatting them.[33]

[32] Ralph Schroeder, "Defining Virtual Worlds and Virtual Environments," *Journal For Virtual Worlds Research* 1, no. 1 (July 2008). https://doi.org/10.4101/jvwr.v1i1.294.

[33] Ryan Rippeon, "Clandestine Message Passing in Virtual Environments" (master's thesis, Naval Postgraduate School, 2009), https://calhoun.nps.edu/handle/10945/3967.

Moore's Law, a techno-economic model of digital computing capacity, states that the functionality and performance of digital electronics will double every two years within the parameters of fixed cost, power, and size.[34] In the past decade alone, Moore's law stipulates that the functional capacity of our digital devices has increased thirty-fold. This increase in computing capacity, when paired with the global proliferation of internet connectivity, has made access to virtual environments both commercially available and financially affordable for much of the global population. However, while there are a range of available virtual environment options, for a shared virtual environment to serve as an effective and clandestine medium for insurgent communications, it must satisfy multiple suitability criteria in order to serve as an effective communications channel for an insurgent user.

Online virtual environments have been growing in popularity in the form of internet-enabled video games. In the five years since 2017, global online video game membership has increased from approximately 650 million users to over 1 billion users by the end of 2022.[35] Similarly, forecasting models of online video game use predict a continuation of this growth with the addition of another 200 million users in the coming five years.[36] Driving this steady growth in online gaming is the penetration of mobile phone technology and mobile gaming to an ever-expanding portion of the global population. As mobile phone and cellular technology continues to proliferate, so too will access to online gaming platforms and participation in collaborative virtual environments. The application digital devices as mediums for clandestine communication is limited only by the creativity of the insurgent organization, the availability of internet-based data, and access to commercial devices to act as conduits for information. As insurgent organizations seek to establish clandestine communications networks, the employment of data

[34] John Shalf "The Future of Computing Beyond Moore's Law," *The Royal Society Publishing – Mathematical, Physical and Engineering Sciences* 378, no. 2166 (January 2020). http://doi.org/10.1098/rsta.2019.0061.

[35] Statista, "Number of Smartphone Subscriptions Worldwide from 2016 to 2021," 2022. https://www.statista.com/outlook/dmo/digital-media/video-games/online-games/worldwide#analyst-opinion.

[36] Statista, "Number of Smartphone Subscriptions Worldwide from 2016 to 2021."

dissemination through commercially available applications and devices may serve as a useful tool in their host of available communications options. Later portions of this thesis will address the predicted positive impact on communicative gain created by access to virtual environments and case studies outlining methodologies that may be employed to use virtual environments as mediums for clandestine communications.

2. Proliferated Low Earth Orbit Satellite Technology

The National Aeronautics and Space Administration (NASA) defines Low-Earth orbits (LEOs) as Earth-centered orbits with altitudes of less than 2,000 kilometers. Low-Earth orbit satellite constellations are considered near enough to Earth for convenient transport, communication, and observation and are a rapidly emerging sector for satellite-based communications technologies.[37] Recent advances in commercial re-usable orbital delivery vehicles have driven significant declines in the cost of space launches. While previous NASA-sponsored launches cost upwards of $1.5 billion, commercial solutions like SpaceX's Falcon 9 provide similar—if not superior—orbital delivery services for a fraction of the cost at an estimated 62 million dollars.[38] This substantial decrease in the cost per weight of orbital delivery has enabled the emergence of radical new space architecture. No longer constrained by prohibitive costs of delivery, satellite-based communication companies like SpaceX, OneWeb, Boeing, and Kuiper (Amazon) are able to construct vast constellations of thousands of satellites in Low-Earth orbit with the desired goal of providing higher fidelity communications, imagery, and tracking services to their customers.[39]

Unlike previous, expensive, and military-exclusive forms of satellite communications, communications provided by the emerging mega-constellations of

[37] Darcy Elburn, "Low Earth Orbit (LEO) Economy," NASA. February 2022. https://www.nasa.gov/leo-economy/faqs.

[38] Harry W. Jones, "The Recent Large Reduction in Space Launch Cost," in *28th International Conference on Environmental Systems,* (Albuquerque: ICES, 2018), 1–10, https://ttu-ir.tdl.org/bitstream/handle/2346/74082/ICES_2018_81.pdf.

[39] Matthew Hallex and Travis Cottom, "Proliferated Commercial Satellite Constellations – Implications for National Security," *Joint Forces Quarterly*, (April 2020): 20–30. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_20-29_Hallex-Cottom.pdf?ver=2020-03-31-130614-940.

proliferated low earth orbit satellites are commercially available and affordable to normal communications consumers. Very Small Aperture Terminal-based (VSAT) satellite communications systems like the Starlink Wi-Fi Router provide high-speed and encrypted communications globally for under one thousand dollars at start-up and under 120 dollars monthly.[40] Furthermore, as many of the mega-constellations are still under construction, it is expected that the cost and availability of satellite communications solutions will decrease and increase, respectively, in the coming years as more and more of the constellations come online.

In addition to traditional terminal-based low-earth orbit satellite communications, telecommunications consumers will also increasingly be able to connect their mobile devices directly to satellite-delivered data streams. Emergent "cell-tower-in-space" connectivity like that provided by Lynk Global Incorporated allows mobile cellular users to connect their cellphones directly to Lynk Global Shannon satellites operating in 500km altitude low-earth orbits.[41] Enabled by advances in mobile computing capacity and advantages in signal transmission from lower orbits, technologies like Lynk Global's satellite-to-mobile-phone communication networks will allow telecommunications users of the future to bypass terrestrial-based communications infrastructure and directly access satellite data provisions without additional hardware.[42]

The advent of proliferated low-earth orbit satellite constellations is indisputably a revolution in communications technologies. In the decade between 2011 and 2021, the number of active satellites in orbit has increased fourfold from 1,033 to 4,877.[43] Furthermore, the rapid changes to satellite technologies are continuing at an accelerating

---

[40] Starlink, "Starlink WiFi Router Specifications," SpaceX. Accessed January 8, 2023. https://www.starlink.com/specifications.

[41] Lynk Global Incorporated, "Lynk Shannon Satellite Narrative Statement," Federal Communications Commission. 2020. https://apps.fcc.gov/els/GetAtt.html?id=266627&x=.

[42] Lynk Global Incorporated, "Lynk Proves Direct Two-Way Satellite-to-Mobile-Phone Connectivity," September 29, 2021. https://lynk.world/lynk-proves-direct-two-way-satellite-to-mobile-phone-connectivity.

[43] Statista, "Number of Active Satellites from 1957 to 2021," 2022. https://www.statista.com/statistics/897719/number-of-active-satellites-by-year/#:~:text=This%20statistic%20illustrates%20the%20number,3%2C291%20active%20satellites%20in%202020.

pace. The current Starlink-SpaceX mega-constellation alone is planned to include 12,000 satellites—upwards of five times more active satellites than were in orbit at the time of the first Starlink launch in 2019.[44] These increases in space launch capacity and commercial satellite technologies have already revolutionized the availability of global broadband communications and, specifically, satellite-based data transmission capacity, data transfer speed, and overall accessibility.[45]

It is expected that continuing advances in space launch capacity and growth in the commercial satellite communications industry will contribute to an ever-increasing availability of satellite-based digital communications and a decreasing reliance on the previous terrestrial-based telecommunications infrastructures of the preceding century. With every space launch and delivery of communications satellites into orbit, the options for communications and the availability of data transmission increase. These increases in data availability and options will play critical roles in the development of clandestine communications channels in the coming decades as insurgent movements will no longer be tethered to the vulnerable ground-based telecommunications infrastructures servicing their areas of activity.

The application of satellite-connected devices as mediums for clandestine communication is limited only by the creativity of the insurgent organization, the availability of internet-based data, and access to commercial devices to act as conduits for information. As insurgent organizations seek to establish clandestine communications networks, the employment of data dissemination through commercially available appliances and devices may serve as a useful tool in their host of available communications options.

---

[44] National Aeronautics and Space Administration (NASA), "NASA Space Science Data Coordinated Archive – Starlink 1010," 2022. https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2019-074D

[45] Emmi Yonekura et al., *Commercial Space Capabilities and Market Overview: The Relationship Between Commercial Space Developments and the U.S. Department of Defense*. R 578–2 (Santa Monica, CA: RAND, 2022). https://www.rand.org/pubs/research_reports/RRA578-2.html.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COORDINATION AND ORGANIZATION IN MODERN INSURGENCY

A. THE IMPACT OF EMERGENT TECHNOLOGY ON MODELS OF INSURGENT CAPACITY

1. Introduction: The Impact of Emergent Technology

As previewed in the literature review of this thesis, the continual modernization of communications technology creates significant potential for insurgent organizations to organize, operate, and communicate through protected internet resources and across concealed mediums or disguised environments. This increase in the availability of protected communications options will increase the operational capacity and survivability of insurgent organizations in future conflicts. In order to demonstrate the positive impact of emergent communications technologies on both internal coordination and external recruiting, this thesis will propose updates to previous models of insurgent organizations and operations. Specifically, this thesis will address McCormick and Owen's models of insurgent operational capacity through the lens of an external player within the insurgent competition that is seeking to enable an insurgency through the provision of communications resources and technologies.

2. Updated Modeling: Insurgent Operational Capacity

For the purpose of evaluating the expected impact of new or emergent communications technologies on an insurgency's operational capacity, this thesis will use the mathematical models provided in McCormick and Owen's "Security and Coordination in a Clandestine Organization" (listed below).[46] Specifically, these models will cover the operational capacity of a single insurgent cell within an overall movement, subject to organizational limits and geographically defined parameters.

$$Operational\ Capacity\ of\ an\ Insurgent\ Cell: \quad h_j(m_j) = \frac{k(e^{am}-1)}{ke^{am}+1} t_j$$

[46] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177.

Within this equation, the m input variable represents the total membership of the insurgent cell, and the variables k and a represent operational parameters that define the S-shaped nature of the insurgent cell's operational capacity curve. Lastly, variable t_j represents a scaling variable that is tied to the strategic importance of the area of operations of the insurgent cell.[47] For this equation and all following equations, the subscript j will be used to denote the specific insurgent cell within an overall insurgent organization. Using the conditions provided in McCormick and Owen's original calculations, the following parameters will be used for the entirety of this thesis' modeling of insurgent organizations: $k = 0.1$ and $a = 0.2$.[48] Additionally, the t_j variable will be set to 1 to demonstrate the nature of the relationship between cell membership and operational capacity—without addressing specific strategic implications or geographic considerations.[49] As depicted previously in Figure 2 and recreated in Figure 5, this model of operational capacity represents an S-shaped curve when applied to a Y-axis of operational capacity and an X-axis of insurgent cell membership.

[47] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177.

[48] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177.

[49] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177.

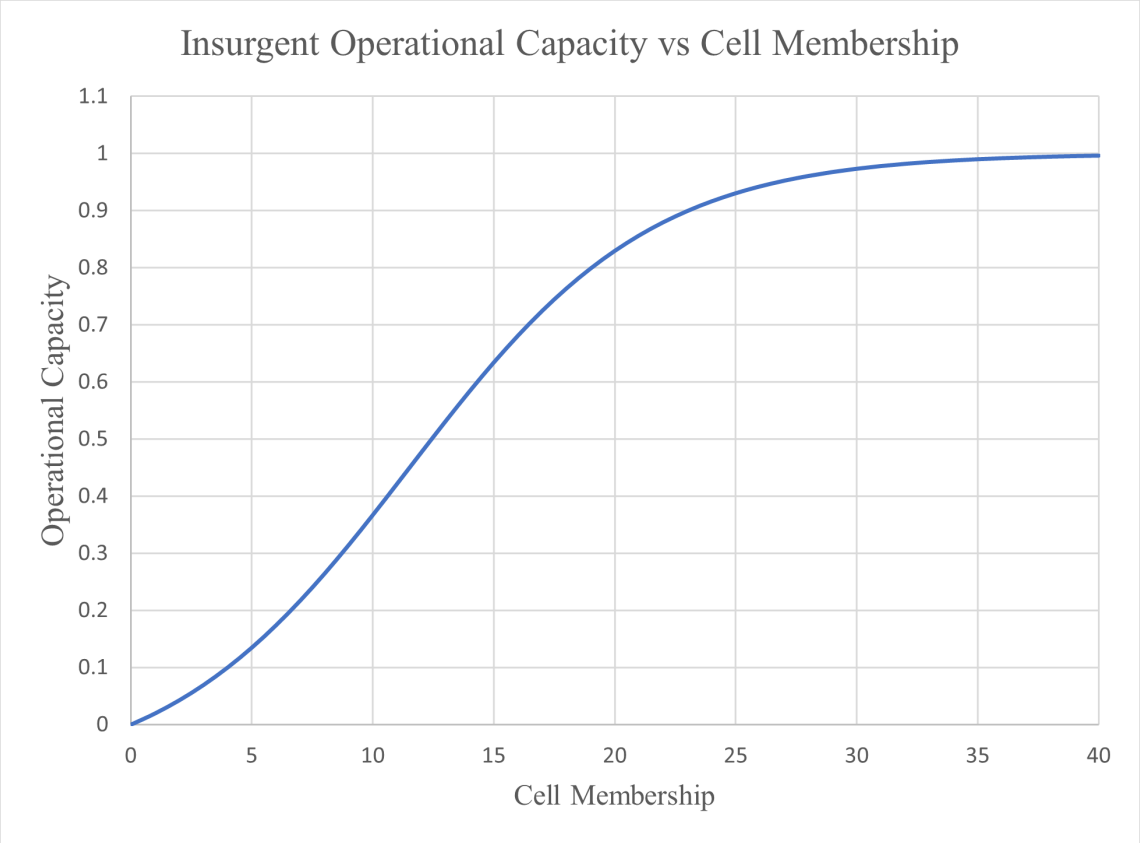

Figure 5. Insurgent Operational Capacity versus Cell Membership.[50]

As expected, the operational capacity of the baseline insurgent cell is exhibited as an S-shape curve subject to diminishing marginal returns to additional members and an asymptotic operational capacity ceiling equivalent to 1 (or t_j). McCormick and Owen's advanced models further account for additional operational considerations by introducing probabilities of detection and scaling effects on the t_j variable as well as summative equations that account for multiple insurgent cells that comprise an overall insurgent movement.[51] This model in particular may be used to demonstrate the logical phenomenon of higher security protocols producing higher levels of operational capacity and lower levels of security producing higher probabilities of detection and resultingly lower operational capacity. While McCormick and Owen introduce additional variables and

[50] Adapted from McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177.

[51] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 181.

scaling effects within the original model to account for communications, security, and capacity, the model may yet be improved by the introduction of a quantitative scaling variable that captures the availability of protected internet-enabled communications and commercially accessible clandestine communication mediums.

This thesis proposes that an additional scaling variable C_j be included to capture the positive scaling effects resulting from access to protected internet resources and clandestine mediums. Based on the hypothesis that emergent communications technologies provide insurgent organizations with more effective internal communication as well as greater reach in external, recruitment-oriented communications, this thesis will propose specific updates to the models provided in McCormick and Owen's "Security and Coordination in a Clandestine Organization." First, the updated operational capacity equation for an individual insurgent cell would be as follows:

$$Updated\ Operational\ Capacity\ of\ an\ Insurgent\ Cell: \quad h_j(m_j) = \frac{k(e^{am}-1)}{ke^{am}+1} t_j C_j$$

In order to quantify the positive relationship between the availability of clandestine communication mediums, protected internet connectivity, and operational capacity, we may further define C_j as:

$$Technology\ Scaling\ Variable, \quad C_j = \frac{(1+\ Q_j)}{(1-\ P_j)}$$

Within this construct, variable Q_j represents the percentage of a population in a contested region *j* with operational knowledge of clandestine communication mediums such as virtual environment-based communications or other comparable forms of concealed data distribution. Variable P_j represents the percentage of a population in a contested region *j* with access to protected internet resources such as commercial satellite communications technologies, satellite-to-cellphone services, or any other form of protected internet access that mitigates the vulnerabilities associated with vulnerable or exploited terrestrial telecommunications infrastructure. Thus, based on the nature of the proposed technology scaling variable, it may be inferred that both the knowledge of clandestine mediums and access to protected internet resources may serve as critical

enablers for the positive scaling of an insurgent cell's operational capacity. If either the concealed communications variable (Q_j) or the protected internet access variable (P_j) is non-zero in the updated model, an insurgent cell evaluated using McCormick and Owen's operational capacity equation will be observed to experience an increase in its operational capacity over the previous baseline—the scenario in which the Technology Scaling Variable (C_j) is not applied to the model.

The use of the Technology Scaling Variable (C_j) within McCormick and Owen's models of insurgent capacity is predicated on the concept of external support to an insurgent organization. Within the context of the Great Power Competition, it is highly likely that the U.S. and its allies will leverage insurgent organizations as instruments of international influence. As an external enabler within this updated model, the U.S. or its allies may choose to allocate resources to support the introduction and employment of concealed mediums or protected internet technologies. This model will further postulate that given a limited amount of resources, an external enabler may dedicate resources to the development of concealed mediums, protected internet connectivity, or some combination of both. The following modeled scenarios will all operate under the following assumptions:

1. Positive impacts of clandestine communications technologies may be modeled by the proposed Technology Scaling Variable.
2. An external actor may expend resources (R) to increase a population's access to clandestine mediums (Q_j) or access to protected internet (P_j).
3. The goal of the external actor is to maximize the insurgent cell's operational capacity via provision of resources.
4. The external actor possesses only a limited number of resources (R).
5. Each unit of resource (R) expended will yield a 0.01 (1%) increase in either Q_j or P_j.
6. The external enabler can only allot resources (R) in increments of 25. (For demonstrative purposes and categorical comparisons.)

7. The external enabler must use all resources available within the scenario allotment. There is no operational incentive to save or withhold resources.

8. Lower Bound: Both Q_j and P_j must be greater than or equal to 0.00.

9. Upper Bound: Both Q_j and P_j must be less than or equal to 0.75.

10. The external enabling actor may not lower either Q_j or P_j.

Table 1 demonstrates the different Technology Scaling Variables (C_j) options achievable by an external enabler given different sets of available resources (R). Row 1 in white demonstrates the baseline for operational capacity scaling that will be used as a comparison throughout the following models. The Low Resource Scenario represented by rows 2 and 3 in light green demonstrates the achievable Technology Scaling Variable options given a resource limitation of R=25. The Medium-Low Resource Scenario represented by rows 4–6 in yellow demonstrates the achievable Technology Scaling Variable options given a resource limitation of R=50. The Medium Resource Scenario represented by rows 7–10 in light orange demonstrates the Technology Scaling Variable options given a resource limitation of R=75. The Medium-High Resource Scenario represented by Rows 11–13 demonstrates the Technology Scaling Variable options given a resource limitation of R=100. The High Resource Scenario represented by Rows 15 and 15 demonstrates the Technology Scaling Variable options given by a resource limitation of R=125. And, lastly, the Maximum Resource Scenario represented by Row 16 in purple demonstrates the Technology Scaling Variable option available to an external enabler willing to expend a maximum amount of financial and technological resources on a contested region and insurgent population. Additionally, the rightmost column of Table 1 denotes whether or not a resource expenditure combination is optimal or not when compared to other Technology Scaling Variables within the same spending category.

Table 1. Computation of Technology Scaling Variable Values (Cj) Given Sub-Variable Inputs (Q_j and P_j).

Row	Resource Category	Clandestine Medium Availability (Q_j)	Protected Internet Availability (P_j)	Technology Scaling Variable (C_j)	Optimal Resource Allocation? Y/N
1	Minimum	Null (0.00)	Null (0.00)	**1.00**	**Y**
2	Low	Null (0.00)	Low (0.25)	**1.33**	**Y**
3		Low (0.25)	Null (0.00)	**1.25**	**N**
4	Medium Low	Null (0.00)	Medium (0.50)	**2.00**	**Y**
5		Low (0.25)	Low (0.25)	**1.667**	**N**
6		Medium (0.50)	Null (0.00)	**1.50**	**N**
7	Medium	Null (0.00)	High (0.75)	**4.00**	**Y**
8		Low (0.25)	Medium (0.50)	**2.50**	**N**
9		Medium (0.50)	Low (0.25)	**2.00**	**N**
10		High (0.75)	Null (0.00)	**1.75**	**N**
11	Medium High	Low (0.25)	High (0.75)	**5.00**	**Y**
12		Medium (0.50)	Medium (0.50)	**3.00**	**N**
13		High (0.75)	Low (0.25)	**2.33**	**N**
14	High	Medium (0.50)	High (0.75)	**6.00**	**Y**
15		High (0.75)	Medium (0.50)	**3.50**	**N**
16	Maximum	High (0.75)	High (0.75)	**7.0**	**Y**

The following hypothetical scenarios will address each resource allocation category and highlight the lessons learned from the application of the proposed Technology Scaling Variable to McCormick and Owen's models of insurgent operational capacity. Referencing the provided list of assumptions, the following scenarios will limit the hypothetical adoption rates of concealed mediums and protected internet technologies to 75% of the notional population in an attempt to properly model the infeasible nature of achieving a population that is universally educated on clandestine tradecraft or in possession of emergent communications technologies like satellite-connected devices.

a. Scenario 1: Minimal Resource Scenario, R=0 (Baseline)

The U.S. (external enabler) has identified an insurgent cell on the strategic periphery of a Great Power Competitor's domain. This insurgent cell maintains low operational priority and has not been allocated any units of the resource. Given a lack of

resources, the U.S. is unable to cultivate or develop any additional forms of clandestine communications in support of the insurgency, and the insurgency is forced to accept its original operational capacity. Figure 6 demonstrates the mathematical result that both Q_j and P_j equaling zero creates a Technology Scaling Variable value of 1.00, which, when applied to the model of insurgent operational capacity, yields no change to the insurgent cell's capacity.

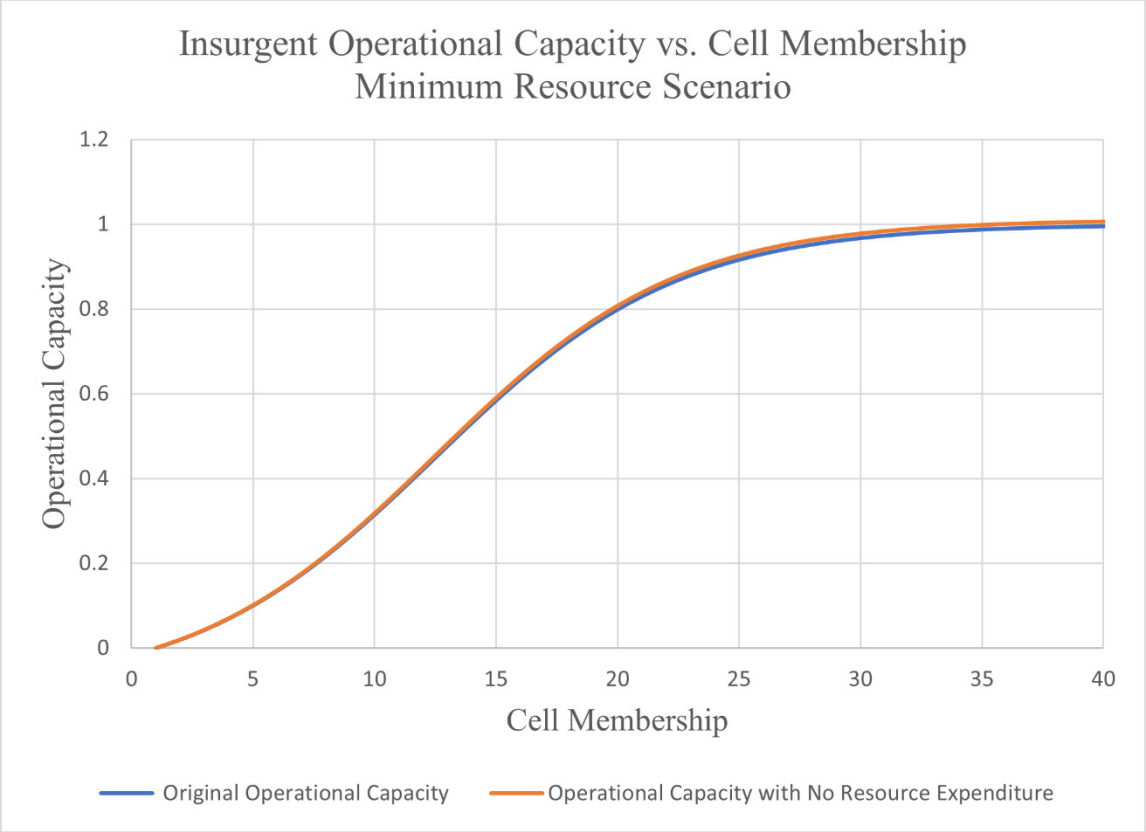

Figure 6. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in Minimum Resource Scenario, R=0.

b. Scenario 2: Low Resource Scenario, R=25

The U.S. (external enabler) has identified an insurgent cell on the strategic periphery of a Great Power Competitor's domain. This insurgent cell maintains a low operational priority but has been allocated 25 units of resource (R)—enough to collectively increase the values of the insurgent cell's Q_j or P_j variables by 0.25. Using the minimum

spending increment of R=25, the U.S. must choose to allocate all of the available resources to either the development of clandestine mediums (Q_j) or protected internet resources (P_j). As demonstrated in the comparison between rows 2 and 3 of Table 1, the U.S. will achieve the highest Technology Scaling Variable value of 1.33 by allocating all available resources to the development of protected internet resources (P_j). Figure 7 demonstrates the positive impact that even a small amount of resources may yield when invested into an insurgent organization's ability to communicate securely.

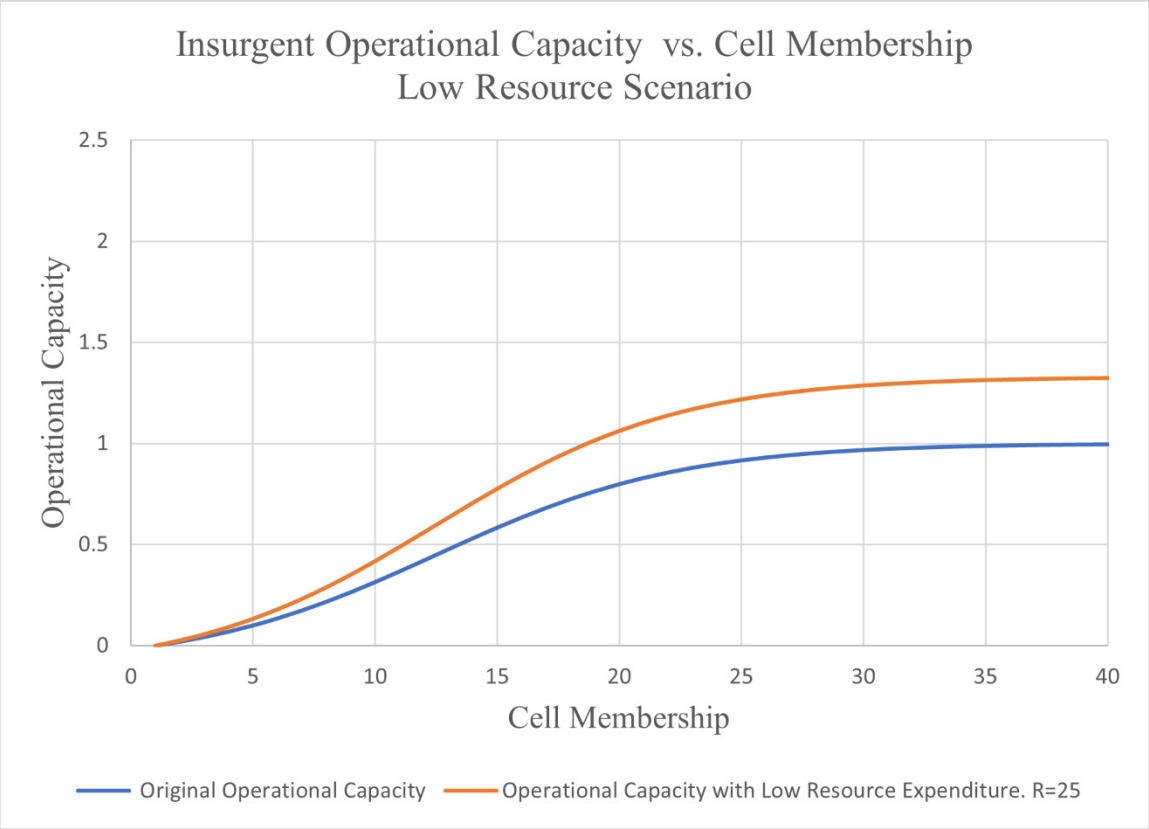

Figure 7. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in Low Resource Scenario, R=25.

Similar to the original model, this updated model maintains the S-shaped nature of the insurgent cell's operational capacity curve; however, the impact of the Technology Scaling Variable is demonstrated in the increase in the operational capacity limit (higher asymptotic capacity ceiling), as well as an increase in operational capacity production per

member (steeper capacity curve with higher values when compared to similar values on the original curve). These differences demonstrate the hypothesized increases in internal communications efficiencies and external recruitment efforts that may be generated through the employment of protected internet resources.

For this scenario, the real-world course of action that corresponds to the maximization of the C_j variable would be a devotion of the operation's limited resources to the procurement, distribution, and funding of satellite communications hardware and subscription services to a small portion of the population. In a low resource scenario these protected communications resources would likely be reserved for key players within the insurgent organization or for the creation of a sparse but distributed communications network in the region supporting the insurgent cell or organization.

c. Scenario 3: Medium-Low Resource Scenario, R=50

The U.S. (external enabler) has identified an insurgent cell operating in indirect competition with the military apparatus of a Great Power Competitor. The insurgent cell has demonstrated limited operational significance and viability as an influence medium through a sporadic series of engagements with the adversary's conventional military forces. The U.S. has allocated a total of 50 units of resource (R) to the insurgency—enough to collectively increase the combined values of Q_j and P_j by a total of 0.50. Using the minimum spending increment of R=25, the U.S. must choose to between allocating all of the resources to the development of clandestine mediums (Q_j), allocating all of the resources to protected internet resources (P_j), or splitting the resources equally between the two communication subsets. As demonstrated in the comparison between rows 4, 5, and 6 of Table 1, the U.S. will achieve the highest Technology Scaling Variable value of 2.00 by allocating all of the available resources to the development of protected internet resources (P_j). Figure 8 again demonstrates the positive impact that the allocation of resources yields when invested in an insurgent organization's ability to communicate securely. Additionally, when compared to Figure 7, Figure 8 demonstrates the positive relationship between resource expenditure and net gain in operational capacity experienced by an insurgent cell. In the Low Resource Scenario, the maximum notional level of operational

capacity achievable by the insurgent cell was approximately 1.4. However, with the increased resource expenditure of the Medium-Low Scenario, the same cell's maximum notional operational capacity is increased to approximately 2.0.

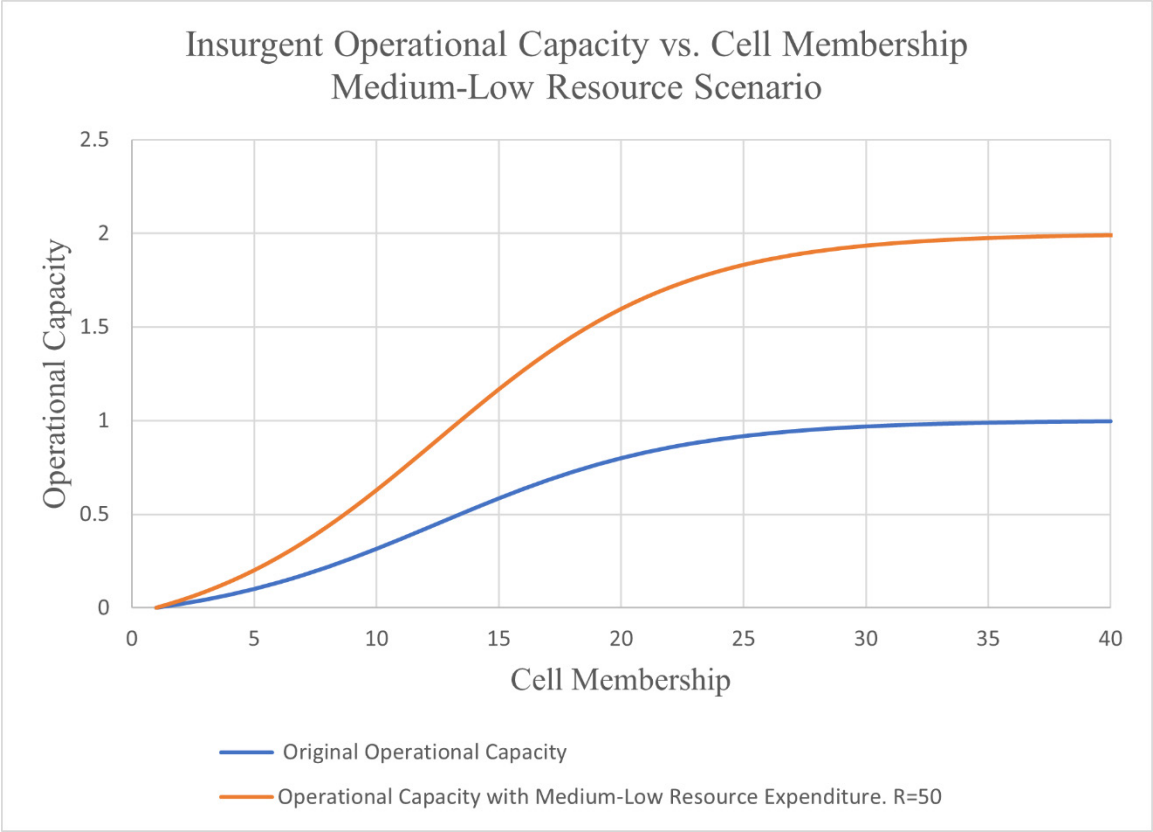

Figure 8. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in Medium-Low Resource Scenario, R=50.

For this scenario, like the previous Low Resource Scenario, the real-world course of action that would correspond to this maximization of the Technology Scaling Variable (C_j) would be a devotion of all of the operation's resources to the procurement, distribution, and funding of satellite communications hardware and subscription services for the population of the modeled region. However, in comparison to the sparse network created by the previous scenario's lower resource allocation, the network of protected internet resources created in this scenario would be marginally more robust, potentially providing for a denser connectivity network with additional nodes distributed amidst the population

and the insurgency within the region to enhance the cooperative relationship between the two.

d. Scenario 4: Medium Resource Scenario, R=75

The U.S. (external enabler) has identified an insurgent cell operating in direct competition with the military apparatus of a Great Power Competitor. The insurgent cell has demonstrated operational significance through a continuing series of engagements with the adversary's conventional military forces. The U.S. has allocated a total of 75 units of resource (R) to develop the insurgency's operational capacity. The allocated resources may collectively increase the combined values of Q_j and P_j by a total of 0.75. Using the minimum spending increment of R=25, the U.S. must choose between maximizing the region's access to clandestine mediums (Q_j), maximizing the region's access to protected internet resources (P_j), or distributing the resources unequally between the two communications options. As demonstrated in the comparison between rows 7, 8, 9, and 10 of Table 1, the U.S. will achieve the highest Technology Scaling Variable value of 4.00 by using the allotted resources to maximize the region's access to protected internet resources (P_j). Figure 9 demonstrates the large positive impact that this additional access to protected internet resources yields.

Additionally, Figure 9 also demonstrates the continuing positive relationship between resource expenditure and the overall increase in the operational capacity of the recipient insurgent organization. Compared to the maximum achievable operational capacity of the Low Resource Scenario (1.4) and the maximum achievable operational capacity of the Medium-Low Resource Scenario (2.0), the maximum operational capacity of the Medium Resource Scenario has increased nonlinearly to a value of 4.0. This phenomenon is explained mathematically in the composition of the Technology Scaling Variable with the placement of P_j in the denominator of the equation but is also valid in terms of real-world military application. As more resources are invested in protected satellite communications, the number of satellite-connected devices and users within a region will likewise increase. As the number of users and devices increases in a region, adversarial intelligence and targeting efforts will incur proportional increases in the volume

of screening and targeting activities they must conduct to identify and attrite members of the insurgency.

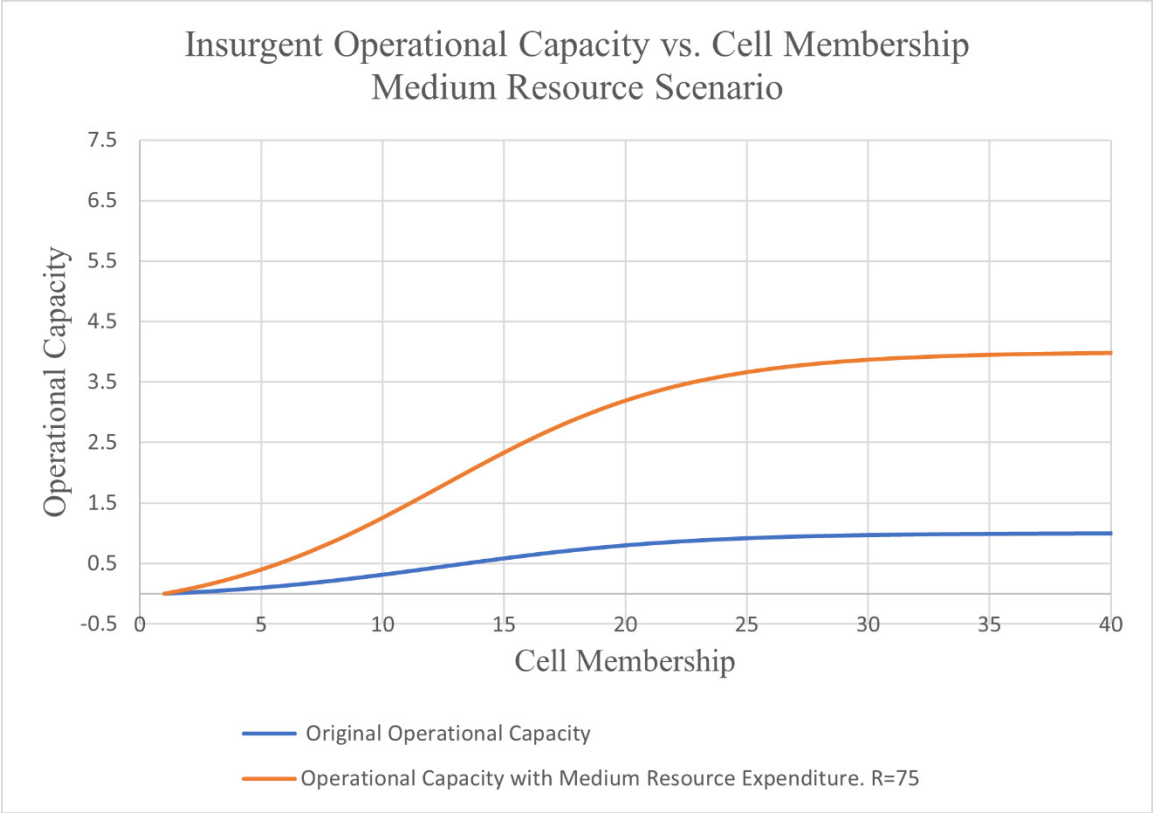

Figure 9. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in Medium Resource Scenario, R=75.

e. Scenario 5: Medium-High Resource Scenario, R=100

The U.S. (external enabler) has identified an insurgent cell operating in a region directly bordering a Great Power Competitor. This insurgency is in constant and direct competition with the military apparatus of its Great Power Competitor neighbor. The insurgent cell has demonstrated operational significance through a continuing series of engagements with the adversary's conventional military forces. The U.S. has allocated a total of 100 units of resource (R) to develop the insurgency's operational capacity. The allocated resources may collectively increase the combined values of Q_j and P_j by a total of 1.00. Using the minimum spending increment of R=25, the U.S. must choose between

maximizing the region's access to clandestine mediums (Q_j) and providing the remaining 25 units of resource to the region's protected internet resources (P_j), maximizing the region's access to protected internet resources (P_j) and providing the remaining 25 units of resource to the regions clandestine mediums (Q_j), or distributing the resources equally between the two communications options. As demonstrated in the comparison between rows 11, 12, and 13 of Table 1, the U.S. will achieve the highest Technology Scaling Variable value of 5.00 by using the allotted resources to maximize the region's access to protected internet resources (P_j) and spending the remaining 25 resources on the clandestine mediums access (Q_j).

In addition to continuing to demonstrate the positive relationship between resource allocation and operational capacity, Figure 10 demonstrates the synergistic nature of both sub-variables P_j and Q_j within the Technology Scaling Variable equation. While—given the notional parameters established for these scenarios—P_j yields a higher operational capacity return to investment, there are logical limits on the ability of an external enabler to distribute an emergent technology to the population of a contested region. Figure 10, when compared to Figure 9, demonstrates the opportunity for additional technological support when one technology or medium is saturated or potentially unavailable. Compared to the maximum operational capacity of 4.0 in Figure 9, the maximum operational capacity of 5.0 in Figure 10 illustrates the added benefit that diversifying an insurgent communications portfolio may yield.

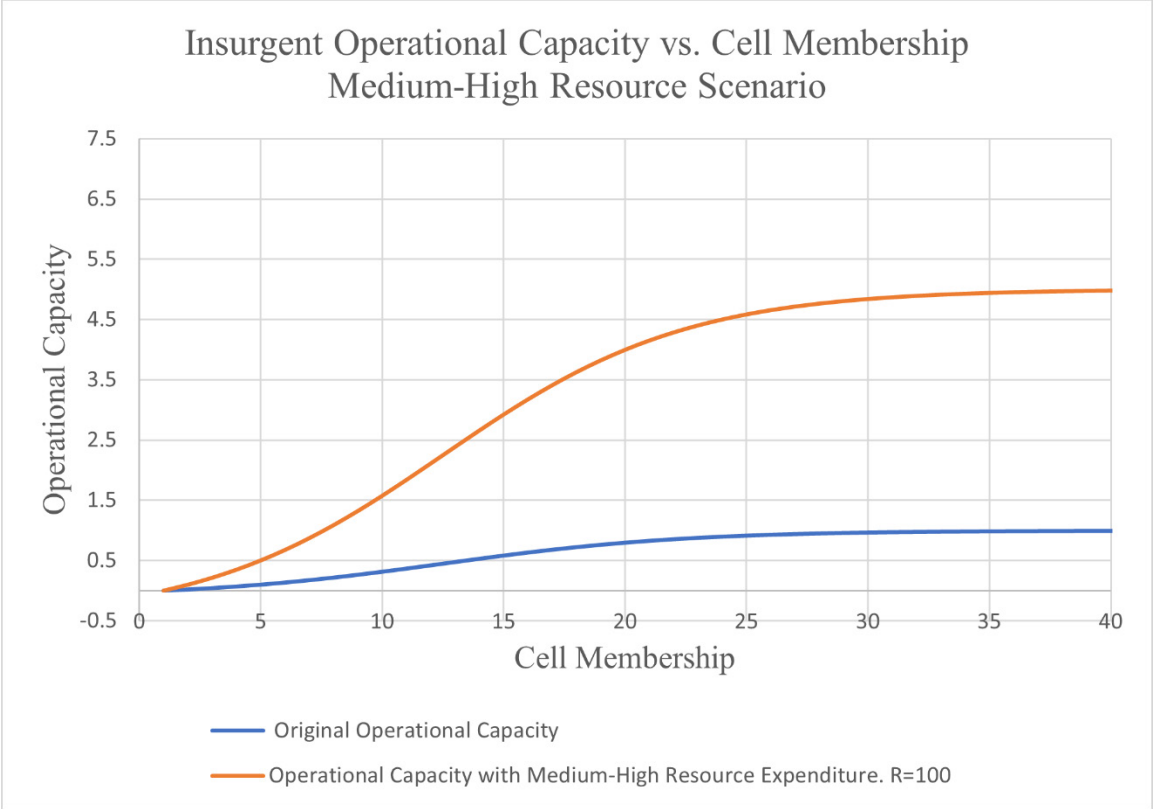

Figure 10. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in Medium-High Resource Scenario, R=100.

Another critical output of the Technology Scaling Variable is visible in the comparison between the Medium Resource Scenario and the Medium-High Resource Scenario. If an external enabler allocates resources suboptimally in support of an insurgent organization, it may facilitate increases in operational capacity that may have been achieved at lower levels of resource investment. For example, if an external enabler employs the suboptimal resource allocation from row 12 in Table 1, a "Medium High" resource category option, and split the 100 units of resource (R) evenly between P_j and Q_j, they would incur a Technology Scaling Variable of 3.00. However, as demonstrated in the Medium Resource Scenario, optimal employment of 75 units of resource (R) will yield a higher Technology Scaling Variable value of 4.00. Thus, despite its notional origins, the Technology Scaling Variable demonstrates the importance of allocating resources into optimal portfolios that will result in the maximization of a supported organization's operational capacity.

f. Scenario 6: High Resource Scenario, R=125

The U.S. (external enabler) has identified an insurgent cell operating on key contested terrain within geographic regions denied to friendly forces by a Great Power Competitor. This insurgent cell has been identified as a critical element in the strategic contest for control of the region. The U.S. has allocated a total of 125 units of resource (R) to support the cell—enough to collectively increase the combined values of Q_j and P_j by 1.25. Using the minimum spending increment of R=25, the U.S. must choose between maximizing the region's access to clandestine mediums (Q_j) and providing the remaining 50 units of resource to the region's protected internet resources (P_j) or maximizing the region's access to protected internet resources (P_j) and providing the remaining 50 units of resource to the regions clandestine mediums (Q_j). As demonstrated in the comparison between rows 14 and 15 of Table 1, the U.S. will achieve the highest Technology Scaling Variable value of 6.0 by prioritizing resource allocations to protected internet resources (P_j). Figure 11 demonstrates the added benefit that the additional resources available to clandestine medium resources (C_j) impart on the cell's operational capacity ceiling—an increase from 5.0 to 6.0 between the Medium High Resource Scenario and the High Resource Scenario.

Figure 11 affirms the concept that despite the maximized use of one communications technology, the addition of another may continue to add operational capacity gains for an insurgency. Later sections of this thesis will address employment recommendations for insurgent communications portfolios, and key among these guidelines is the recommendation for a diversified communications plan. By having multilayered communications plans, insurgent organizations may increase their resilience to enemy counter-communications activities such as jamming, spoofing, and surveillance.

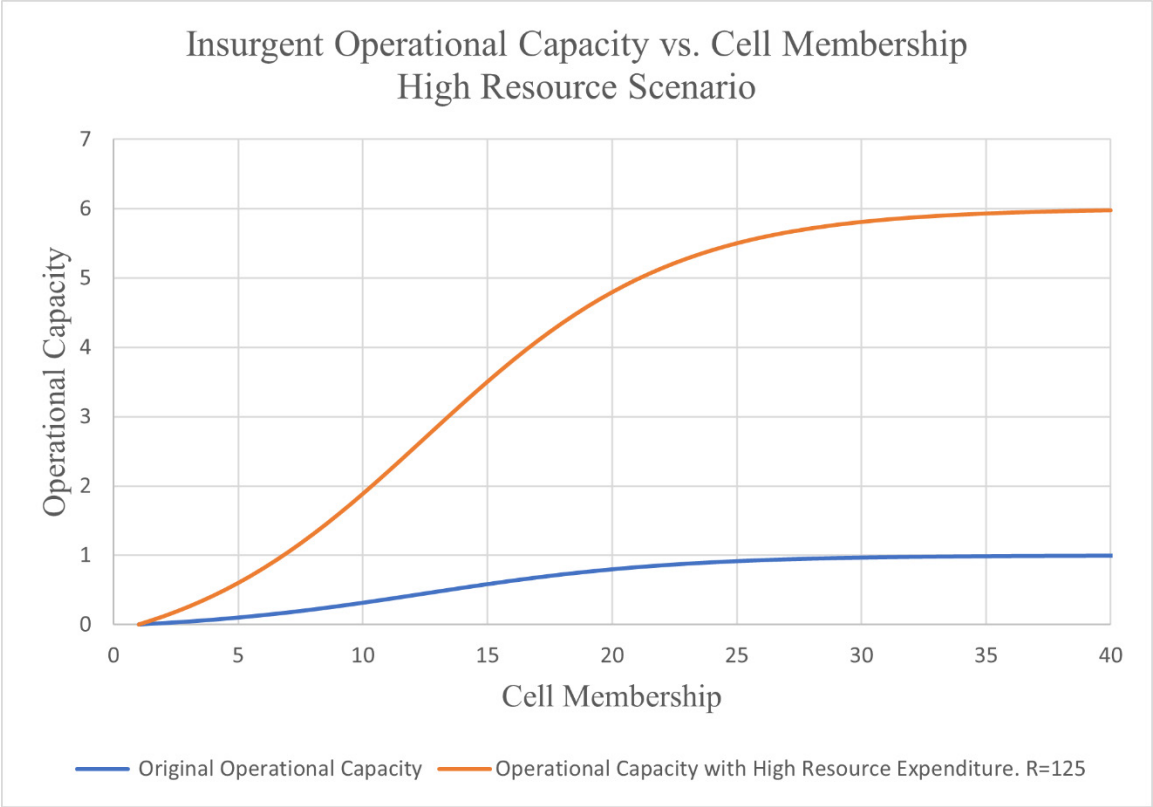

Figure 11. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in High Resource Scenario, R=125

g. Maximum Resource Scenario, R=150

The U.S. (external enabler) has identified an insurgent cell operating within the sovereign territory of a Great Power Competitor. This insurgent cell has conducted a series of successful disruptive attacks against key social and political processes that underly the stability and order of the Great Power Competitor's leadership. This insurgent cell has been labeled a top priority for the U.S. military and intelligence communities and has been allocated 150 units of resource (R), enough to collectively increase the combined values of Q_j and P_j by 1.50—effectively maximizing both. The U.S.' only option, given this spending allotment, is to maximize the region's access to clandestine mediums (C_j) and to maximize its access to protected internet resources (P_j). Figure 12 demonstrates the comparatively superior impact that this strategy has on the operational capacity of the insurgent cell. When compared to all other resource expenditure scenarios, the Maximum Resource Scenario

affirms the positive relationship between resource investments and the received benefit experienced by the supported organization.

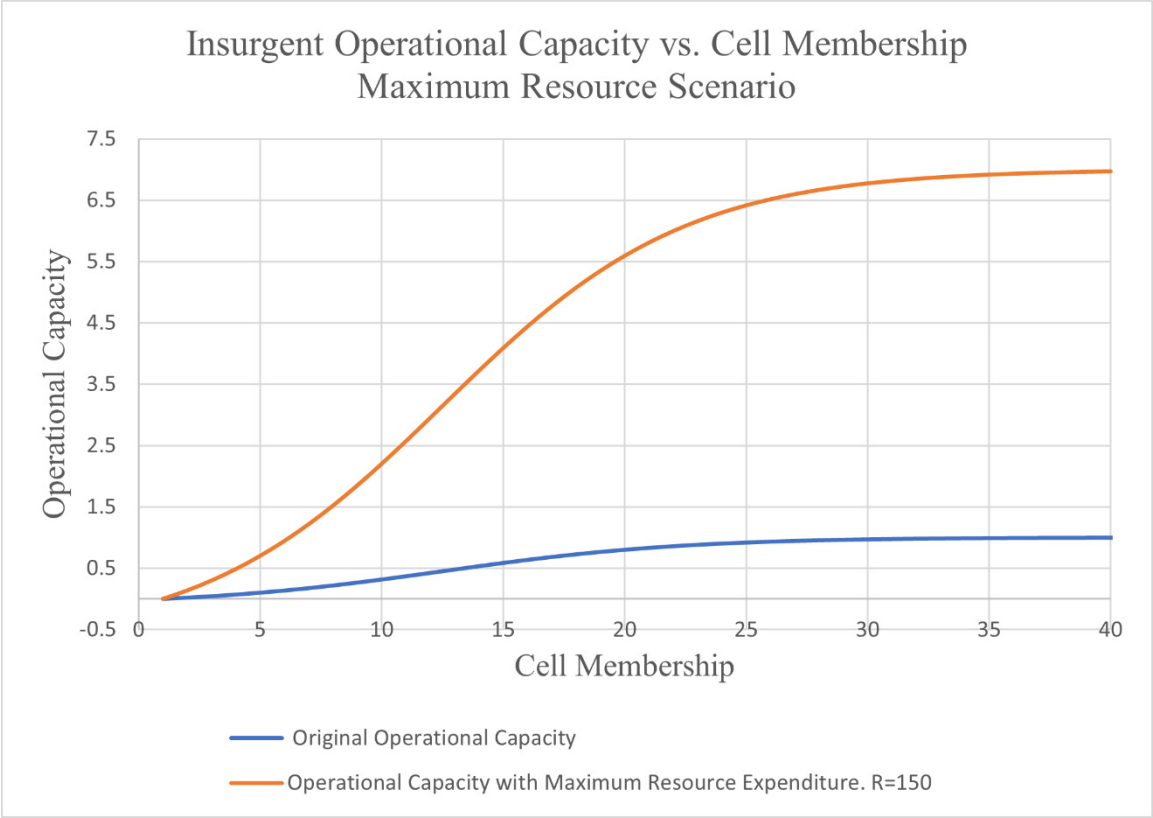

Figure 12. Insurgent Operational Capacity versus Cell Membership. Technology Scaling Impacts in Maximum Resource Scenario, R=150.

For this scenario, the real-world course of action that corresponds to the maximization of C_j would be a cost and labor-intensive influx of protected internet access resources and infrastructure as well as a comprehensive introduction of clandestine medium education and channels to the population of region j. In a maximum spending and strategically paramount operation such as this, it may be expected that the U.S. tasks strategic level assets (like portions of satellite constellations or cyber-specific communication technologies) towards the support and development of the insurgent cell. Additionally, it may be expected that the U.S. provide significant quantities of commercially available communications infrastructure such as satellite communication

downlink terminals, satellite-enabled cellular devices, and subsidized communication subscription services to the population of region j.

3. Modeling Considerations

The hypothetical scenarios and spending combinations addressed in this thesis are by no means comprehensive nor indicative of real-world constraints. While these scenarios demonstrate the operational relationship and hypothesized impact of technology on insurgent operations, there are many more considerations that must be accounted for by operations planners seeking to support insurgent operations. The following section will address key factors that are not explicitly addressed by the modeling efforts provided in this thesis. Among these additional considerations are further analyses of the temporal aspect of current and future operations, the inclusion of McCormick and Owen's aggregate models (demonstrating the summative efficiency of an overall movement vice a single insurgent cell), the potential and likelihood for varied resource costs between clandestine mediums and protected internet resources, and the potential for varying boundary conditions that were not included in this modeling effort.

a. Temporal Considerations

While not addressed in the modeled scenarios, an operation seeking to enable an insurgent cell will likely experience multiple, sequential spending periods or operational cycles and must tailor its resource allocations to consider current operational viability and to prioritize longer-term operational optimization. While an operation may achieve the highest possible operational scaling in a current period with a specific combination of resources, this resource allocation may become suboptimal in future operational periods if total resource allocations do not allow for the maximization of both Q_j and P_j variables. Thus, it may be in the best interest of the insurgent cell and enabling operation to tailor their spending strategies in the current operational period to the overall net expected resource allocations across all periods. This strategy, however, may incur one or more periods of suboptimal enabling operations as the insurgent cell builds its clandestine and protected communications portfolios toward the optimal combination. While this strategy may allow the insurgent cell to maximize its operational capacity in the long run, it may

also jeopardize its short-term viability and solvency. Thus, as third-party planners seek to enable insurgent operations, they must ensure that the insurgent cell remains viable in current periods while also maximizing its total potential by conducting longer-term investments toward an optimized communications portfolio.

b. Aggregate Insurgent Movement Considerations

While the models contained in this thesis address the potential impacts of technological enablement for a single insurgent cell, they do not directly address the impact of technology on the overall insurgent movement. As depicted by McCormick and Owen, the insurgent movement is an aggregation of individual cells working together to achieve a summative level of operational capacity.[52] This aggregative relationship between a total number (n) of cells (j) is depicted below using the operational capacity equation from McCormick and Owen's "Security and Coordination in a Clandestine Organization".[53]

$$Operational\ Capacity\ of\ Overall\ Insurgent\ Movement = \sum_{j=1}^{n} h_j(m_j)$$

As a third-party enabler seeks to support larger-scale resistance movements, it must not only choose to allocate resources to specific communications options but to also choose which insurgent cells to support from an overall population of cells within the movement. Because each cell's operational capacity is also weighted by its strategic and geographic importance (T_j), one approach to maximizing return on resource investment would be to identify insurgent cells with the highest T_j variable values and allocate all available resources to those cells. However, in an effort to generate the greatest possible return on investments, operations planners would benefit from identifying each operational capacitive increase per unit resource per insurgent cell (j) and distributing resources to each cell such that each unit of resource allocated generates the greatest possible impact on the overall movement's operational capacity.

[52] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 177–178.

[53] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 178.

c. Cost Variation Considerations

One critical assumption made by the scenarios in this section is that the costs per percent increase in clandestine channel access (Q_j) and costs per percent increase in protected internet resources (P_j) are equal. This cost equivalency is a driving factor in the maximum available technology scaling variables (C_j) demonstrated in Table 1 and is potentially unrealistic when applied to real-world operations, populations, or geographic regions. From a financial perspective, educating a population on the use of clandestine communications channels may incur different resource costs than providing that same population with the technological infrastructure required to establish protected internet connectivity. Factors such as digital literacy, preexisting communication infrastructures, population age demographics, cellular device penetration rate, local satellite communications markets, digital commerce channels, and population consumption trends may drastically alter the comparative cost per percent increase in either or both Q_j and P_j. As operations planners seek to maximize the operational capacity imparted by external aid, they must evaluate the relative costs of improving the communications options and seek to maximize the impact of resources by allocating them to the area of development where their investment will generate the greatest return to insurgent operational capacity. Similar to the way in which planners must tailor their spending allocations to maximize C_j in an individual cell, they must likewise tailor their resource expenditure based on the costs of each communication option within the contested regions, *j*.

d. Boundary Parameter Considerations

The scenarios in this section employ notional minimums and maximums for the Q_j and P_j variables to demonstrate key characteristics of the relationship between the input variables. Realistically, it must be expected that the minimums and maximums for variables Q_j and P_j will vary based on the demographics and behaviors of populations or regions hosting the insurgent cells. Intuitively, agrarian, rural, or economically disadvantaged populations will likely have lower technological baselines due to the comparatively minimal role that communications technologies play within their social and economic environments. Conversely, highly developed, technologically dependent

populations may have higher baseline values due to their preexisting understanding and employment of technologies that may be repurposed into clandestine or protected communications channels. Operations planners must consider the degree to which technology influences a target population and apply resources accordingly to maximize the effectiveness of their external aid. Because the operational parameters established for a given population and insurgent cell may become limiting factors on the maximum operational capacity of the cell, operations planners must identify insurgent cells with the greatest operational potential and maximize their resources while also identifying insurgent cells with lower operational potential and supporting them with the remaining available resources.

e. Tailoring Models to Real World Scenarios

As irregular warfare practitioners seek to optimize support to an insurgent organization, they must appropriately tailor their models to accurately represent the operational environment in which they seek to cultivate and activate an insurgent guerrilla force. By adapting the models provided by McCormick and Owen's "Security and Coordination in a Clandestine Organization" and the Technology Scaling Variable from this thesis to properly represent the operational gains, losses, and limitations of a specific environment, external players within the insurgent competition may maximize the utility borne of their resource investments. The three-dimensional modeling of a maximization function applied to the Technology Scaling Variable proposed in this thesis would allow an irregular warfare planner or insurgent enabler to visualize the predicted scaling (operational gains) associated with various spending combinations and resource allotments. As seen in Figure 13, the Technology Scaling Variable for a region may be generated as a two-dimensional surface in three-dimensional space, wherein the location on the X and Y axes represents the combination of Q_j and P_j that an external enabler achieves via the investment of resources (R), and the height of the surface on the Z-axis represents the maximum Technology Scaling Variable available given the available combinations of Q_j and P_j.

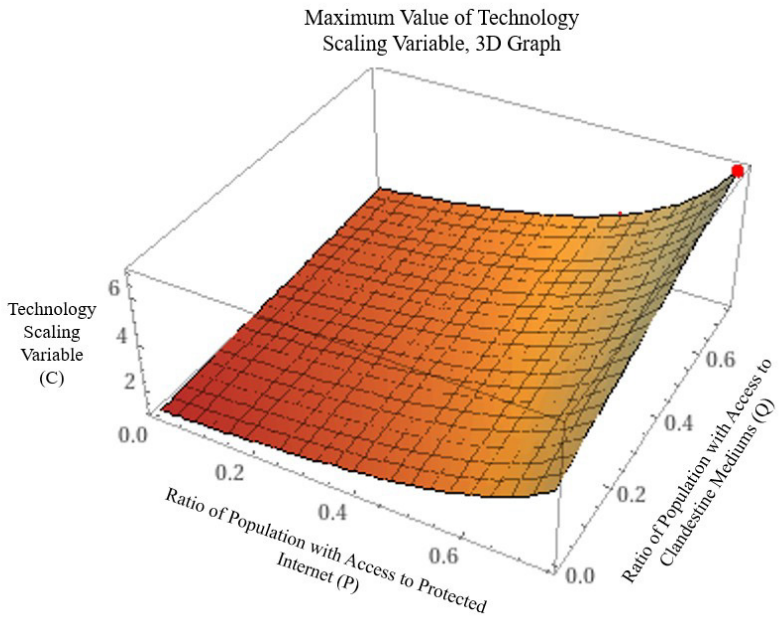

Figure 13. Technology Scaling Variable, Plot in 3-Dimensions. Graph Generated via Wolfram Alpha.

As operations planners and intelligence assets seek to cultivate, weaponize, and employ insurgent organizations, they should likewise seek to maximize the Technology Scaling Variable they impart on an organization. As demonstrated in Figure 13, given the rudimentary set of inputs and limitations provided in this section, at most, an external enabler will be able to achieve a maximum Technology Scaling Variable of 7.0, displayed as the red dot in the top right corner of Figure 13, and as the "Maximum Resource Scenario" provided by Table 1. However, because real-world operations will attempt to model more dynamic scenarios, this thesis also recommends the employment of weighted variables or further scaling within the Technology Scaling Variable equation to account for varied costs, operational returns, and limitations on technologies that may be incurred during support operations to a real-world insurgency or guerrilla movement.

This thesis recommends that operational planners start with the following set of equations as a mathematical starting point for more precise modeling of specific scenarios or operational environments.

$Maximize\ [\frac{(1+AQ_j)}{(1-BP_j)}]$, such that:

$C_{Q,j}Q_j + C_{P,j}P_j \leq R$	Resource Limitations & Cost Scaling
$Q_j \geq L_{Q,j}$	Lower Bound Established for Q in region j
$Q_j \leq U_{Q,j}$	Upper Bound Established for Q in region j
$P_j \geq L_{P,j}$	Lower Bound Established for P in region j
$P_j \leq U_{P,j}$	Upper Bound Established for P in region j
$BP_j \leq 0.99$	Modeling Limitation, Prevents Undefined Output

With Variables:

Q_j	Clandestine Mediums Variable, Percentage of Population
P_j	Protected Internet Variable, Percentage of Population
A	Estimated Operational Importance Scaling Variable for Q_j
B	Estimated Operational Importance Scaling Variable for P_j
$C_{Q,j}$	Cost Per % increase of Q_j, in region j
$C_{P,j}$	Cost Per % increase of P_j, in region j
R	Available Units of Resource
$L_{Q,j}$	Lower Limit on Variable Q_j, in region j, (cannot be negative)
$U_{Q,j}$	Upper Limit on Variable Q_j, in region j, (cannot be greater than 1)
$L_{P,j}$	Lower Limit on Variable P_j, in region j, (cannot be negative)
$U_{P,j}$	Upper Limit on Variable P_j, in region j, (cannot be greater than 1)

IV. EMERGENT COMMUNICATION TECHNOLOGIES

A. INTRODUCTION AND APPLICABILITY CRITERIA FOR COMMUNICATIONS TECHNOLOGIES

Modern insurgent communications technologies have evolved beyond the single-channel radio networks and the courier systems that were foundational to the insurgent organizations of the Global War on Terror, the Vietnam War, and earlier conflicts. While these forms of communication still exist and maintain limited viability in modern conflict, insurgent organizations must develop, employ, and refine modern clandestine and protected mediums of communication in order to limit operational risk against the highly sophisticated and far-reaching surveillance and targeting capacities of Great Power Competitors.

1. Applicability Criteria for Insurgent Communications Options

To compare and evaluate the various clandestine mediums available to a modern insurgency, evaluation criteria for emergent or repurposed communications must be explicitly identified, defined, and applied to potential communications options. This thesis proposes that emergent technologies must meet four general requirements to serve as either clandestine or protected mediums of communication for an insurgent organization. Broadly categorized, these requirements would require a communications technology to be commercially available, employable with minimal education or training, protective or concealing of communicated information, and ultimately a capable medium for the transmission of insurgent guidance, recruitment materials, insurgent education or instruction, or other forms of relevant direction at the discretion of insurgent leadership.

a. Commercial Availability

First, in order for a technology to serve as a medium for insurgent communication, it must be commercially available, technologically compatible, and consumer accessible to the general population and pre-existing physical and digital infrastructures of the targeted region. This requirement of commercial availability ensures that the potential communication technology bears minimal barriers to entry and is as widely available as

possible to both insurgents and members of the local population. Because insurgent operational capacity is positively correlated with insurgent membership, insurgent organizations require communications mediums that allow them to recruit, educate, and coordinate with host populations within their geographic region. The criterion of commercial availability stipulates that any physical hardware, devices, or supporting equipment must be available for purchase in local or regional markets. Furthermore, any required digital software or programming material must be accessible via online marketplaces or the physical delivery of the required software via digital storage devices. Ultimately, in order for an emergent or repurposed medium to be viable as a form of insurgent communication, it must be available to the population of the region hosting the insurgent activity.

b. Low Complexity or Minimal Educational Requirements

Second, similar to the concept of availability, a potential insurgent communication technology must be feasibly accessible to the population. Specifically, the technology or medium must be of low technological complexity or technical sophistication and maintain minimal educational requirements in order to ensure low barriers to operation or employment. The ideal communications platform or medium is one that is readily usable by both insurgent members and the local population as soon as it is purchased or acquired commercially. While ease of use is difficult to quantify and relative to the digital literacy of the region's population, the technology or method itself must minimize the use of complex hardware or sophisticated methodologies that would otherwise prohibit its use by potential insurgent members or supporting members of the civilian population of the region.

However, while minimal complexity or sophistication is required for use by insurgent members seeking to establish communications with their host population, in sensitive use cases, additional protective measures may be added to increase both the protection and concealment of the communications at the cost of increasing the complexity of the communications network or operations. Because sustained and sensitive communications are more likely to occur between members of insurgent cells, the

requirements of lower levels of technological or criminal sophistication do not apply as stringently to insurgency-internal communications networks.

c. Functional Protection or Concealment

Third, a potential insurgent communication technology must—at a minimum – protect the clandestine nature of the insurgent communications it is used to transmit. Specifically, this criterion will require that the potential technology or medium circumvents local or regional cellular infrastructure or conceals the transmission by embedding it within the larger civilian data flows associated with entertainment, online commerce, or other forms of internet-enabled data traffic. This criterion prioritizes the circumvention of local cellular networks in order to enhance the security of an insurgency's communications by avoiding potentially vulnerable hardware or penetrated communications services associated with the telecommunications infrastructures or service providers of a contested region. Additionally, this criterion also prioritizes the use of embedded communications to conceal the nature and existence of insurgent communication activity. By hiding, obscuring, or obfuscating the nature and content of insurgent communications, a potential communication method may limit the probability of detection or exploitation of information associated with the digital transmission of insurgent communications.

Ideally, insurgent communicators would employ a combination of communicative mediums or technologies that provide both confidentiality and availability of transmitted information. While a single communication technology may only provide protection or concealment, two or more technologies or mediums may be employed complementarily in order to provide the greatest level of security to the communicator and recipients. The following sections and case studies will evaluate emergent communicative options individually. However, it is recommended that an insurgent communicator seeks to diversify their communications network and employ multiple methods of concealment, steganographic embedding, and protected connections in order to mitigate the risk of interception, interpretation, and exploitation by an adversarial intelligence effort.

d. Effective Medium for Communication

Last, a potential insurgent communication technology must effectively provide an insurgent organization with the timely ability to transmit protected or concealed data containing insurgent guidance, recruiting material, or other various leadership-generated directions to the population of the region. This criterion will not specify specific data formats, data payload size minimums, or data transmission speeds beyond the qualitative minimum of providing the insurgency with the ability to transmit direction in a timely and usable manner to other members within the organization or externally to the regional population hosting the insurgent cell. While the preceding three criteria may be treated as optional by an insurgent organization, the effective transmission of data is paramount to the viability of a communications technology. An insurgent cell or organization may employ a specialized, non-commercial, sophisticated, or insecure communications medium with the assumption of increased risk or decreased efficiency, but it will not employ a communications technology that fails to meet the communicative needs of the mission.

Ultimately, an insurgent communication technology must be capable of transmitting enough information as fast as necessary in order to meet the needs of the mission about which it is centered. For example, a recruitment-centric form of communication must be capable of the extended staging of recruitment materials, links to exogenous content, and provide insurgent contact information for follow on guidance. Conversely, more time-sensitive operations-oriented communications may require much less data—for example, only a few lines of plain-text information containing the time, location, and guidance for a meeting, rally, or strike—but may require shorter turnaround periods and higher levels of protection from surveillance. Thus, insurgents must seek to tailor their communicative resources to specific mission requirements and threat environments.

The following sections will identify two broad categories of emergent or repurposed communication technology and evaluate them using the criteria established above. Each technology will be cross-examined using all four of the required criteria and will be accompanied by one to two case studies of potential real-world use by the modern insurgent communicator.

V. COMMUNICATIONS VIA VIRTUAL ENVIRONMENTS

A. INTRODUCTION: VIRTUAL ENVIRONMENTS AS COMMUNICATIONS MEDIUMS

Significant technological and cultural changes have been made in the realm of virtual environments since Ryan Rippeon's "Clandestine Message Passing in Virtual Environments (2008)."[54] In the intervening decade and a half, shared virtual environments have become popularized, elevating in status from educational tools and niche entertainment sectors to commonplace mediums for entertainment, education, design, and more. Videogames—the center of this thesis' study of virtual environments as clandestine mediums—have likewise increased in popularity, complexity, and communicative capacity in the intervening years and are thus poised as an emergent medium for concealed and secretive communications between insurgent cells and their civilian host populations.

While the baseline concepts of collaborative virtual environments have not changed in recent decades, the proliferation of high-speed internet availability, handheld computing power, and the industry of mobile streaming entertainment have revolutionized the popularity and use of virtual environments across the global population. The monetization and popularity of the mobile entertainment industry alone have contributed tens of billions of dollars to the development of publicly accessible virtual environments. In the past four years alone, Meta—the organizational successor and rebrand to Facebook—has invested 36 billion dollars into its Reality Division—the internal research and development group responsible for the development of its "metaverse" virtual environment products and virtual reality software.[55] These emerging combinations of popularity, availability, complexity, and communicative capacity in commercially available virtual environments contribute to an ever-growing portfolio of clandestine communications mediums that may be employed by the insurgent cell or supporting population. As the protection and concealment of insurgent communications

[54] Rippeon, "Clandestine Message Passing in Virtual Environments."

[55] Grace Dean, "Meta Has Pumped $36 Billion into Its Metaverse and VR Businesses since 2019," Business Insider, October 29, 2022, https://www.businessinsider.com/charts-meta-metaverse-spending-losses-reality-labs-vr-mark-zuckerberg-2022-10.

are paramount to the survival and operational capacity of an insurgent group, virtual environments may prove to be a critical element of future insurgencies' abilities to communicate in denied or surveilled environments.

One critical advancement in the development of modern virtual environments is the advent and availability of high-definition, open-world, massively multiplayer online role-playing games (MMORPG). Recent market trends in online gaming services have minimized barriers to entry for potential virtual environment users by removing requirements for paid subscriptions and substituting them with advertisements, premium subscription options, and microtransactions for in-game goods or advantages.[56] Thus, as a result of an increasingly popular and free-to-join entertainment market, vast amounts of physical and digital infrastructure have been made available to the insurgent communicator seeking to transmit his or her messages through a denied or adversary-monitored online information environment.

B. APPLICABILITY CRITERIA: VIRTUAL ENVIRONMENT-BASED COMMUNICATIONS

In order for virtual environment-based communications to serve as viable mediums for clandestine insurgent communications, they must meet the four general requirements outlined in this thesis. Virtual environment-based communications must be available, user-friendly, protective or concealing, and viable for the transmission of insurgent leadership, direction, recruiting, or other organizational guidance. The following sections will address broad considerations of the availability and use of virtual environments within the evaluative parameters of the minimum requirements provided in this thesis.

1. Commercial Availability of Virtual Environment-Based Communications

Because virtual environments occupy roles across a broad spectrum of modern entertainment, education, communications, and advertisement sectors, their commercial availability has proliferated in recent decades, and they are available to large portions of the

[56] Dan Singer and Enrico D'Angelo, "The Netflix of Gaming? Why Subscription Video-Game Services Face an Uphill Battle," McKinsey & Company, July 8, 2020. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-netflix-of-gaming-why-subscription-video-game-services-face-an-uphill-battle.

global population. Thousands of virtual environments are available across similarly numerous devices, gaming platforms, software applications, and online-hosted communications venues such as chat rooms, organizational networking software, and telecommunications services. Because virtual environments are available on almost any internet-connected device, an inspiring insurgent communicator can access virtual environments using little more than the mobile phones, internet-connected gaming platforms, and computing devices that are common to households of the developed world.[57] The increasing connectivity of household internet-connected devices has increased the aperture available to clandestine mediums and thus has increased an insurgent's ability to conceal or disguise their communications amidst the data flows associated with the virtual environment's original purpose and role.

Videogames, the subject of this thesis study of virtual environments, are entertainment products and are available commercially in a wide range of consumer markets globally. Broken down into two fundamental categories, virtual environments in the form of video games require two pieces of commercially available items—hardware and software. In order to access virtual environments, users must have the requisite hardware in the form of internet-connected mobile phones, gaming consoles, smart TVs, or streaming devices, as well as having access to the required digital software products like online videogames, gaming applications, or other various communications enabling software applications. For example, virtual environment-enabling hardware like the Xbox and Xbox Live software marketed by the Microsoft Corporation is available globally with exceptions in Cuban, North Korean, Sudanese, Iranian, and Russian markets.[58] Likewise, comparable products made by the Sony Corporation—including the Sony PlayStation and online PlayStation network, are also available globally with similar restrictions on countries currently under trade restrictions

[57] Jingjing Ren et al., "Information Exposure from Consumer IOT Devices: Proceedings of the Internet Measurement Conference," in *2019 Internet Measurement Conference* (Amsterdam: ACM, 2019), 267–79, https://dl.acm.org/doi/10.1145/3355369.3355577.

[58] Microsoft Corporation, "SEC Correspondence: Sale of Microsoft Products," U.S. Security and Exchanges Commission, December 27, 2011. https://www.sec.gov/Archives/edgar/data/789019/000119312512007906/filename1.htm#:~:text=Although%20we%20do%20not%20currently,September%202011%20and%20September%202013.

enacted by the United States.[59] Based on the ubiquitous nature of commercially available virtual environments, under the prescribed evaluation criteria, it may be assumed that an insurgent will feasibly have access to at least one form of virtual environment by which to communicate.

2. User Accessibility of Virtual Environment-Based Communications

For an emergent technology to serve as a broadly utilized communications tool, it must be of minimal technical and educational sophistication. Similar to the entertainment sector's positive impact on commercial availability, the market for internet-enabled video games ensures that they are consumer-oriented and user-friendly. The Entertainment Software Rating Board (ESRB)—the governing body for enforcing industry-adopted guidelines—rates video games using rating categories, Content Descriptors, and Interactive Elements.[60] Specifically, the Interactive Elements category of these ratings includes considerations of unfiltered or uncensored user-generated content, user-to-user communications, and media sharing via gaming networks or connected access to social media. In identifying and selecting potential videogame-based virtual environments for insurgent communications, the ESRB ratings for Interactive Elements provide a streamlined method for identifying games and environments designed to enable user-to-user communications and content generation.[61]

Because video games are developed as entertainment products, they are specifically designed to provide users with entertainment, satisfaction, and curated interaction. Within this construct, video games are designed to contain introductory phases and periods of experimentation intended to introduce users and players to the game's mechanics and controls in a gradual and instructive manner.[62] This initial exposure period serves as a learning curve that ensures users are capable of interacting with each other and the virtual environment in

[59] Taylor Hatmaker, "Sony Suspends PlayStation Store and Console Sales in Russia," TechCrunch, Verizon Media Group, March 10, 2022. https://techcrunch.com/2022/03/09/sony-russia-ps5-gran-turismo-suspended/.

[60] Entertainment Software Ratings Board, "ESRB Ratings Guide," December 16, 2022. https://www.esrb.org/.

[61] Entertainment Software Ratings Board, "ESRB Ratings Guide."

[62] Swapna Krishna, "The Best Games Have the Smartest Learning Curves," Wired – Conde Nast, May 4, 2022. https://www.wired.com/story/video-games-learning-curves/.

concert with the intended milestones built into the game. While video games are not intended for use by insurgent communicators, the learning curve period of gameplay may easily be translated into digital clandestine tradecraft with minimal education by insurgent communicators. Due to the natural acclimation and exposure to virtual environments provided in this initial phase of gameplay, it may be asserted that the communicative aspects of video game-based virtual environments are user-friendly and accessible with minimal technical or educational inputs from the insurgent communicator or enabler.

3. Concealment or Protection Provided by Virtual Environment-Based Communications

Steganography is the science of communicating secret data transmissions via a multimedia carrier such as digital images or audio and video files.[63] The primary protective benefit provided by virtual environments to the clandestine communicator stems from the conversion of insurgent communications into data transmissions of video game play and the digital manipulation of virtual environments. Similar to the traditional forms of digital steganographic concealment of information, the conversion of insurgent communications data into activities or media within a virtual environment results in the translation of communicative data to an alternate form of information or data. By concealing information in the form of virtual environments or curated in-game interactions, insurgent communicators may embed secret communications data in virtual constructions, manipulations of virtual environments or many other forms of interactive steganographic concealments that would prevent an adversarial surveillance effort from intercepting and exploiting their content.

The use of virtual environments as conduits and conversion mediums for insurgent communications may occur in numerous forms. Communications data may be stored in virtual mediums mimicking physical storage, in digitized versions of books, player-to-player messaging functions, voice messages, manipulations of the virtual-physical environment, and

[63] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing* 90, no. 3 (September 6, 2010): 727–52. https://doi.org/10.1016/j.sigpro.2009.08.010.

more.[64] By embedding information in in-game content and interactive functions, an insurgent communicator may conceal their message traffic amidst the comparatively large amount of data traffic supporting the internet-enabled gameplay of the host video game and virtual environment, thus lowering the inherent probability of detection or exploitation by adversarial intelligence or targeting efforts. While these game-internal forms of communication are not entirely immune to interception, surveillance, or exploitation, they provide an additional layer of protection and steganographic concealment to the message traffic they seek to transmit. This conversion of insurgent communications data into in-game messaging media, user-to-user interactions, or digitized environmental phenomenon allows insurgent communicators to protect their information while providing an outlet for information dissemination with access control capabilities.

With the advent of large-scale and high-definition virtual environments comes the opportunity for virtual clandestine tradecraft. This form of data concealment represents a fundamental advancement in the art of clandestine communications and steganographic conversion. Unlike standard forms of digital steganography that require the use of computerized algorithms to decode or extract hidden messages from multimedia carriers, information embedded within virtual environments may be extracted, interpreted, and employed via a human user conducting specific and unique actions within the virtual environment. The following sections of this thesis will address the potential for the development of new methodologies and recreation of historical clandestine communications tradecraft in digitized form, using virtual environments and in-game personas as communicative conduits. Ultimately, the ability of an insurgent communicator to use virtual environments as information conversion and dissemination mediums constitutes the viability of virtual environments as a protective measure for insurgent communications.

[64] Luis Gutierrez and Dan Hammill, "Book and Quill – Minecraft Wiki Guide," IGN Entertainment Incorporated, March 18, 2013. https://www.ign.com/wikis/minecraft/Book_and_Quill; Jared Petty and John Ryan, "Communicating Using the Phone – GTA 5 Wiki Guide," IGN Entertainment Incorporated, November 3, 2016. https://www.ign.com/wikis/gta-5/Communicating_using_the_Phone; Aaron Cook, "How to Make Letters and Numbers in Minecraft," B+C Guides. Brit & Company Guides and Tutorials, September 20, 2021. https://guides.brit.co/guides/make-letters-and-numbers-in-minecraft.

4. Viability of Use in Insurgent Communications for Virtual Environment-Based Communications

Ultimately a virtual environment's ability to provide an insurgent communicator with a commercially available, user-friendly, and data-protective or concealing medium for the transmission of secret communications determines its viability as a method of communication for a clandestine organization. Insurgent organizers and members of the population operating in support of the insurgency's goals may use commercially available entertainment products and services to embed communicative data transmissions below the detection threshold established by adversarial intelligence efforts.

Insurgent actors may employ virtual environments as mediums for the steganographic concealment and transmission of communications, wherein the decoding and interpretation of the message may only be achieved through virtualized completion of tasks or activities within the simulated environment. The following section of this thesis will address this emergent concept of digital clandestine tradecraft and interactive steganography. The subsequent case studies will demonstrate an insurgent communicator's ability to conceal, store, and transmit information through the use of shared virtual environments.

C. VIRTUAL CLANDESTINE TRADECRAFT: METHODS OF COMMUNICATION VIA VIRTUAL ENVIRONMENTS

1. Introduction to Virtual Clandestine Tradecraft

By combining traditional methods of clandestine and covert communication with the interactive capacity provided by virtual environments, insurgent communicators may transmit messages and conduct secret activities under the concealment or guise of online entertainment and data flows. For example, in traditional covert or clandestine communications, a "dead drop" is a form of communication that allows for secure communication by one person leaving and another picking up communicative material—after a predetermined amount of time—at a prearranged location. This method of secret communication limits risk and removes the need for direct contact between participants of the communicative interaction.[65]

[65] Central Intelligence Agency Museum, "Artifacts – Dead Drop Spike," Central Intelligence Agency, accessed January 10, 2023. https://www.cia.gov/legacy/museum/artifact/dead-drop-spike/.

The concept of dead-dropping communications material may be applied to virtual environment-based communications as insurgent communicators may create, hide, and transmit their message data within or through shared virtual environments. Because virtual environments are commonly designed to mimic natural physical environments, many historical models of clandestine communication may be renewed and applied using virtualized conduits.

2. Case Study 1: The Minecraft Dead-Drop

Minecraft is an open-world, sandbox video game that uses fully modifiable three-dimensional building blocks to represent virtual worlds and their components. Originally launched in 2009 by the Mojang company, it has since sold upwards of 200 million copies and has sustained upwards of 125 million monthly active users since 2020.[66] Using virtual avatars, Minecraft players are able to manipulate the virtual environment by building, destroying, or moving pieces of the environment—"blocks"—throughout the virtual playable area—"world" or "realm." Furthermore, beyond simple manipulations of volumetric pieces of the environment, users may leverage the material characteristics of the "blocks" to build virtual structures, functional machinery, artwork, designs, and more.[67] Intended as a collaborative gaming experience, Minecraft servers support the inclusion of anywhere from 1 to 30 players per world simultaneously.[68] Because of the shared and interactive nature of the environment and the modifiable characteristics of the virtual building blocks, Minecraft may be used as a communicative tool for an insurgent cell or organization seeking to conceal message traffic amidst the flow of entertainment-related internet activities. By embedding insurgent message data within manipulations of the Minecraft virtual environment, an insurgent communicator may store and transmit communications material under the guise of online gameplay or general online entertainment activities.

[66] National Park Service, "Information about Minecraft," U.S. Department of the Interior, June 19, 2022. https://www.nps.gov/kewe/learn/education/information-about-minecraft.htm.

[67] National Park Service, "Information about Minecraft."

[68] Minecraft Wiki, "Minecraft Multiplayer Gameplay," Fandom Incorporated, accessed March 9, 2023. https://minecraft.fandom.com/wiki/Multiplayer.

For example, one particularly Minecraft-compatible form of data storage and transmission is the Quick Response Code (QR). QR codes are two-dimensional matrix barcodes originally developed for use in the Japanese automotive sector.[69] Specifically, QR codes are optical labels that store information using numeric, alphanumeric, binary, and kanji encoding modes. QR codes are square-shaped barcodes that use black squares in contrast to a white background to generate a pattern that may be scanned by a camera and interpreted using the patterns in the code's horizontal rows and vertical columns.[70] Because QR codes rely on the use of contrasting squares of colored material or electronic display, they are particularly compatible with the Minecraft virtual environment as players have unlimited virtual access to colored building blocks within the game's digital world. Furthermore, because of the highly interactive and customizable nature of the Minecraft virtual environment, users may not only construct QR codes out of the virtual materials, but they may mask, disguise, or otherwise obscure the constructed QR code so as to require a potential viewer of the code to conduct specific activities, assume a particular vantage point or have some sort of additional knowledge concerning the code in order to be able to access it. This ability to dead-drop information in the form of a virtual QR code is tantamount to the application of clandestine tradecraft and may be used as a tool for an insurgent communicator seeking to avoid detection in a surveilled digital environment. Figure 14 demonstrates the efficacy of embedding QR codes within the virtual environment and the potential for the application of virtual clandestine tradecraft at a rudimentary level.

[69] Leela Prasad Kaki, Chandra Sekhar Musinana, and Somasundara Rao Muppidi, "Message passing using cryptography and steganography," *i-manager's Journal on Cloud Computing* 8 (January 2021): 8–15, https://libproxy.nps.edu/login?url=https://www.proquest.com/scholarly-journals/message-passing-using-cryptography-steganography/docview/2621196897/se-2.

[70] Kaki et al., "Message passing using cryptography and steganography," 8–15.

Figure 14. Minecraft QR Code Viewed from North to South (Left) and South to North (Right) in Virtual Environment.

Because QR codes rely 2-dimensional digital image sensors and programmable processors to evaluate and convert stored information, the medium on which they are stored is not consequential as long as the medium can display the contrasted squares with enough clarity to be interpreted by the receiving digital processor. Because QR codes may be generated virtually, they may serve as virtual data storage repositories or access points for further information or direction. For example, as demonstrated in Figure 14, a QR code may be generated in a Minecraft virtual environment using building blocks of contrasting colors. In this case, "sandstone" blocks and "black cement" blocks have been used to construct a virtual QR code 25 blocks tall, 25 blocks wide, and 2 blocks deep. When presented to an internet-connected device with digital camera capacity, this QR code will be interpreted as a link to the Naval Postgraduate School's website homepage—"https://www.NPS.edu/." Using this technique, an insurgent communicator may employ similar virtual environment-hosted QR codes to redirect message recipients to additional outlets for communications, such as temporary chat servers, private messaging applications, or even physical rendezvous points.

Figure 14 also demonstrates another critical element of virtual environment-based communications: the potential for tradecraft. The QR code in Figure 14 is intentionally built to be two blocks deep. By making one layer entirely out of the light-colored "sandstone" blocks, the QR code has been designed to be viewable only when a user's avatar is standing

North of the QR code and looking North to South in the virtual environment. If viewed from any other angle or viewpoint, the QR code is not readable and will not cause the digital processor to generate an online link or any other form of interpretable data. By design, this QR code forces potential users to conduct a specific set of virtual actions in order to enable the use of the code—in this case, walking, moving, or flying their avatar to a specific portion of the digital world North of the QR code structure. Because virtual environments like Minecraft are built with high levels of modularity and interactable materials, the insurgent communicator may design their QR code to be viewable and useable under specific conditions or after specific virtual actions have been taken. For example, an insurgent communicator may build a set of ten layered QR codes 25 blocks tall, 25 blocks wide, by ten blocks deep, wherein only one of the ten QR code layers correctly directs the viewer to an online repository or communicative outlet. Furthermore, the insurgent communicator may bury this QR code underground or submerge it underwater, or otherwise conceal its virtual location, thus adding an additional layer of controlled access to the information. In designing virtual data storage structures like the QR code in Figure 14 in hidden virtual locations at specific times, an insurgent communicator is essentially conducting a clandestine dead-drop in a virtual environment. Thus, virtual environments may be used as communicative mediums for clandestine message passing and, ultimately, as a tool for the enhancement of an insurgent cell's operational security.

3. Case Study 2: Proximity Chats and Audio Steganography

The second potential method for clandestine communications via virtual environments stems from the communications field of Acoustic Data Transmission (ADT). At its core, ADT is a form of data or information hiding that embeds a data payload into transmitted acoustic media like that commonly seen in music files, or audio accompaniment digital videos. By using one device as a transmitter and another device as a receiver, ADT may be used to communicate information acoustically from one device to another.[71] Because ADT relies on acoustic waveforms as a means of transmission, ADT-based systems operate

[71] N. Lazic, and P. Aarabi, "Communication Over an Acoustic Channel Using Data Hiding Techniques," *IEEE Transactions on Multimedia* 8, no. 5 (2006): 918–24. https://doi.org/10.1109/TMM.2006.879880.

without reliance on additional communication architecture devices like "Bluetooth" or "Zigbee" or "Wi-Fi".[72] Furthermore, because humans experience sound waves with frequencies roughly in the range between 20 Hz and 20 kHz, it is possible to embed and transmit data in acoustic waveforms without users noticing the embedded data within the acoustic content they are viewing.[73] Alone, ADT is currently used in audio watermarking for copyright protection, broadcast monitoring, steganography, and covert communications.[74] However, this thesis proposes that ADT may additionally be used in tandem with virtual environment-based tradecraft in order to enhance the confidentiality of the information exchanges that it may enable.[75] Specifically, acoustic data transmissions may be paired with virtual environment-based acoustic media transmissions like in-game player-to-player communications in ways that limit or control the distribution of the communications payloads.

Figure 15 displays a schematic example of a one-to-one version of a data distribution system leveraging both ADT methodologies and a combination of physical and virtual information delivery mediums. As demonstrated in the schematic flow chart, an insurgent communicator may embed data payloads in acoustic packages that are captured by a video game console's microphone, transmitted via player-to-player interactions in a virtual environment, broadcasted by the receiving video game console's speakers, and received and interpreted by a second device at the recipient's location. Unlike the previous example of virtual environment-based communications, ADT-based communications may be conducted in a shared virtual environment with an audience composed of both witting and unwitting recipients of an acoustic payload. For players receiving an acoustic payload without knowledge of or decryption capabilities, the payload itself will be received as some form of

---

[72] Kiho Cho, Hwan Sik Yun, and Nam Soo Kim, "Robust Data Hiding for MCLT Based Acoustic Data Transmission," *IEEE Signal Processing Letters* 17, no. 7 (2010): 679–82. https://doi.org/10.1109/LSP.2010.2051174.

[73] Manuel Eichelberger et al., "Imperceptible Audio Communication," in *ICASSP 2019 – 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (Zurich: IEEE, 2019) 680–84, https://doi.org/10.1109/ICASSP.2019.8682262.

[74] Kiho Cho, Jae Choi, and Nam Soo Kim, "An Acoustic Data Transmission System Based on Audio Data Hiding: Method and Performance Evaluation." *EURASIP Journal on Audio, Speech, and Music Processing 2015*, no. 1 (2015): 1–. https://doi.org/10.1186/s13636-015-0053-x.

[75] Cho et al., "An Acoustic Data Transmission System Based on Audio Data Hiding: Method and Performance Evaluation."

normal player-to-player audio interaction, such as a music broadcast or verbal conversation. However, for recipients prepared to receive and extract data from an acoustic payload, the transmission of the acoustic payload will be received and interpreted by a secondary device at the recipient's location. Due to the digital embedding of the data payload within an acoustic transmission, ADT-based systems protect sensitive communications by ensuring that only intended recipients of the information will be able to interpret or even notice the transmitted message. Without specific data extraction software and a secondary listening device, surveillance efforts will be unable to detect or interpret the presence of insurgent message traffic as it may be designed to mimic normal message traffic or in-game audio stimuli.

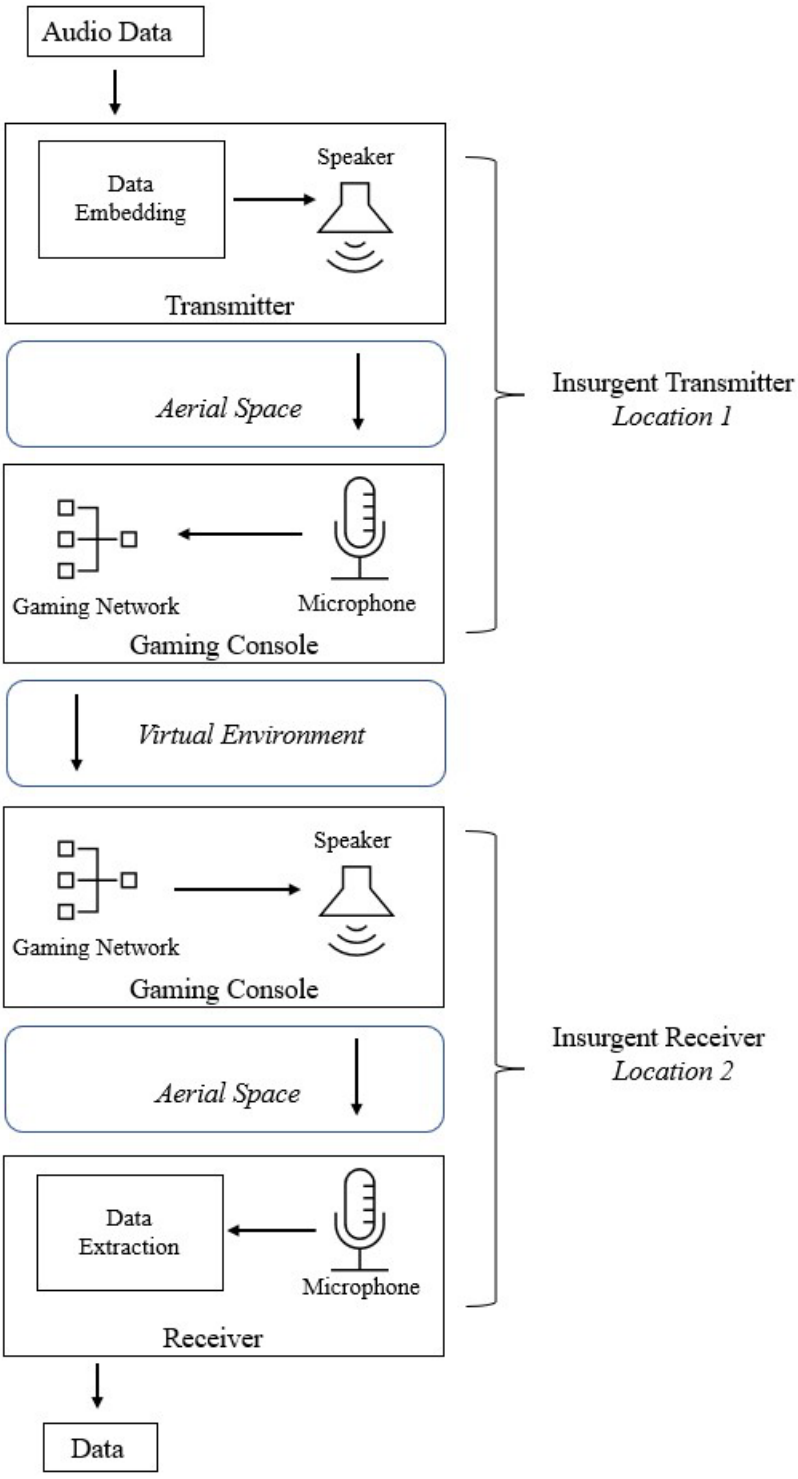

Figure 15. Virtual Environment-Based Acoustic Data Transmission, Schematic Representation.

A key enabler of virtual clandestine tradecraft and acoustic data transmission are emergent "proximity chat" functions within video games. "Proximity chats" are a recent trend in first-person competitive video games wherein certain video games allow individual players to communicate with one another acoustically—IE, verbally through their gaming microphones—when their in-game characters meet specific geographic proximity minimums. For example, in Call of Duty Warzone 2—a first-person competitive shooting game—players may exchange verbal messages when their avatars are within 50 virtual meters of each other on the simulated battlefield.[76] In Call of Duty Warzone 2, once two or more in-game characters are within 50 virtual meters of distance, the "proximity chat" extension of the in-game communication system is initiated, and users may communicate verbally through the microphone-based chat system. Because first-person shooter video games are comparatively dynamic compared to cooperative sandbox-styled cooperative video games, they provide an opportunity for different methods of establishing clandestine channels for communication. This thesis proposes that acoustic data transmissions and proximity chat services within video games may be used complimentarily in order to provide clandestine communicators with the ability to transmit data payloads to select audiences using in-game tactics, techniques, and procedures as virtual forms of clandestine tradecraft. Within this construct, an insurgent communicator may establish a channel for acoustically transmitted data payloads by conducting virtual meetings in games that have proximity chat functions. Because audio transmissions are only possible via proximity chat when in-game characters are within close virtual-geographic proximity, communicators may establish predetermined meeting points within the virtual environment—game map—to be used for short duration transmissions over proximity chat enabled ADT. Additionally, this method of virtual tradecraft may be used to ensure the clandestine nature of the communications as the data payload itself may be embedded in innocuous audio content like music or pre-recorded conversations intended to mimic routine in-game discourse. Without the knowledge of both the virtual meeting location, and access to specific data extraction algorithms, the acoustically transmitted payload is thus protected from unintended recipients or surveillance efforts.

[76] Nat Smith, "How Warzone 2 Proximity Chat Works," PCGamesN – Network-N, November 21, 2022. https://www.pcgamesn.com/call-of-duty-warzone-2/proximity-chat.

In terms of hardware and software compatibility, because ADT modulation techniques such as orthogonal frequency-division multiplexing allow for the imperceptible acoustic embedding of data within human hearable range of 20 Hz to 20 kHz, and because video game audio transmissions are tailored for use in human-to-human interaction, it may be asserted that video game-based acoustic transmission systems may be employed as carriers for use in acoustic data transmission.[77] Furthermore, the availability of proximity chat services within dynamic first-person shooter video games opens the aperture of potential virtual environment-based clandestine tradecraft to include fast paced, dynamic gameplay as a method for screening recipients of ADT transmitted payloads. Similar to the conduct of clandestine activities in the real world, virtual clandestine activities may replicate secret or hidden locations, dynamic venue changes, moving communications, and many other virtual activities that mirror the secretive tradecraft techniques developed by insurgent and intelligence organizations. Thus by requiring potential recipients of insurgent communications to conduct specific activities or demonstrate unique behavior within virtual environments, an insurgent organization may use virtual environment-based ADT as a method of one-to-one or one-to-many payload transmissions with an additional layer of screening or limitations on their distribution.

D. RECOMMENDED USE CASES FOR VE COMMUNICATIONS

Because virtual environment-based communications provide various levels of confidentiality by embedding communications data within publicly transmitted entertainment-related data flows, they are inherently vulnerable to interception by adversarial intelligence and surveillance efforts. While insurgent communications may require specific activities or interactions within the virtual environment, it is still possible that a technologically advanced surveillance effort may intercept and decode the embedded communications in transit, at the origin device, or by impersonating a member of the intended audience. This inherently vulnerable nature limits the recommended use of virtual environments as a means for sensitive communications. Due to the risk associated with disseminating information via a virtual environment and the inherently vulnerable nature of

[77] Eichelberger et al., "Imperceptible Audio Communications," 680.

entertainment-related data flows, this thesis recognizes that insurgent use of virtual environments is optimized when paired with a protective form of internet provision (such as protected satellite communications) or used as a medium for the distribution of insurgent recruitment or educational materials.

As demonstrated in the case studies for this section, virtual environments may serve as mediums for larger-scale information dissemination as well as smaller-scale, one-to-one-styled communications depending on the type of virtual tradecraft that is being employed. Users seeking to establish information caches for use in insurgent recruitment or education may use sandbox-styled video games to store data in the form of visual codes like QR codes. Furthermore, users seeking to conduct shorter duration, higher security communications may leverage additional techniques such as audio steganography in order to provide additional layers of protection to their transmitted information. Because video game-based communications require little criminal or technological sophistication and are conducted through common household entertainment products, they are ideally suited to serve as an informational conduit between insurgent organizations and their host populations. While potentially vulnerable to adversarial surveillance and penetration, virtual environments may be leveraged to provide accessible and protected insurgent data repositories and instructional caches without significantly reducing the operational security of an insurgent organization.

Limiting the transmission of insurgent communications to recruitment and education-related data will likewise limit the incurred operational risk to the insurgent cell responsible for distributing the information. The open availability and access to entertainment-related virtual environments and the availability of online anonymity ensure that virtual environment caches of information are accessible to both friendly and adversary users. Thus, in a contested information environment where online access to insurgent tactics, techniques, procedures, and information is limited, virtual environments may serve as an accessible medium for the transmission of insurgent educational materials. When used as repositories for insurgent educational or recruitment information, virtual environment transmissions limit sustained interaction and user-to-user communications and thus minimize the risk to an insurgent cell's operational security while increasing its effectiveness and communicative capacity. In use cases where sensitive data must be transmitted through a virtual environment medium, it is

recommended that a clandestine communicator leverages the virtual environment in tandem with an additional form of protection, such as the audio steganography addressed previously or the protected internet options addressed in the following sections of this thesis.

E. POTENTIAL FOR MILITARY EMPLOYMENT OF VIRTUAL ENVIRONMENTS

Virtual environments—particularly shared interactive ones—provided by the globally popular video game industry are useful tools for the distribution of clandestine communications. Due to their commercial popularity, video game-based virtual environments are globally available, user-friendly, and potentially useful mediums for the steganographic concealment of insurgent communications. When used alone, virtual environments are optimally suited to serve as mediums for larger-scale information distribution vice sensitive user-to-user communications. Similar to the way that the Office of Strategic Services employed the entertainment-oriented international publishing community to disseminate the fictional novel *The Moon is Down* as an instructional medium for aspiring European saboteurs and resistance fighters in World War 2, the U.S. and its allies may likewise distribute instructional insurgent materials under the guise of online entertainment data and activities.[78]

If the U.S. Department of Defense and its subordinate organizations seek to enable insurgent activities via virtual environment-based communications, they must leverage resources to mitigate the risk incurred by insurgent groups operating in virtual environments. The inherently vulnerable nature of consumer data flows across video gaming networks and unsecured internet connections stipulate that video game-based insurgent communications are both widely accessible and potentially vulnerable mediums. Because an insurgent cell incurs the greatest risk during the prolonged hosting of virtual environment-based data repositories, an external enabler such as the U.S. military may increase the supported insurgent cell's operational security by acting as a risk broker—providing the hosting services from secure geographic locations and protected servers such that insurgents and their host populations alike may access the virtual environments without having to maintain a constant and

[78] Adam Nettina, "How John Steinbeck Inspired the Resistance in WWII," HistoryNet, November 17, 2021. https://www.historynet.com/how-john-steinbeck-inspired-the-resistance-in-wwii/.

vulnerable online presence. Furthermore, the United States may provide additional support to virtual environment-based communications operations by subsidizing or distributing licensed video gaming materials to specific regions hosting insurgent movements. For example, the United States government may coordinate with domestic video game providers and networks to conduct periods of subsidized game distribution in targeted regions under the guise of normal market expansion or advertisement campaigning. Thus, by increasing both the availability and knowledge of clandestine communications capable channels, the U.S. may increase its strategic presence in a contested region via the enablement of an insurgent group or movement.

For higher levels of security, the U.S. may also seek to provide insurgent communicators with access to steganographic embedding and extraction tools. While these tools alone may be indicators of criminal or clandestine activity, they may be likewise concealed as additional features or options within pre-existing communications or entertainment applications that are common to the geographic region hosting the insurgent population. For example, "second screen" applications used by entertainment groups like The Walt Disney Company, a mass media entertainment conglomerate, already provide audio steganographic conversion services to the entertainment industry.[79] As stipulated in the commercial availability criterion, the U.S. must seek to utilize communications options that are commercially available and, ideally, preexistent within the target population's natural communications or entertainment markets. By providing insurgents with access to these tools, the U.S. military and intelligence communities may effectively enhance their ability to enable and communicate with insurgent groups aligned to their missions and goals within the Great Power Competition.

[79] Roman Frigg et al., "Acoustic Data Transmission to Collaborating Smartphones – An Experimental Study," in *2014 11th Annual Conference on Wireless On-Demand Network Systems and Services (WONS)* (Zurich: IEEE, 2014), 17–24, https://doi.org/10.1109/WONS.2014.6814717.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. COMMUNICATIONS VIA PROLIFERATED LOW EARTH ORBIT SATELLITE CONSTELLATIONS

A. INTRODUCTION: PROLIFERATED LOW EARTH ORBIT SATELLITE COMMUNICATIONS

Modern proliferated low Earth orbit satellite constellations have revolutionized global communications networks and will continue to advance in their communicative capacity with each additional satellite launch and technological innovation. With tens of thousands of satellites planned for mega-constellations, companies like Starlink, Amazon Kuiper, and Telesat are establishing massive communications infrastructures in low Earth orbit (LEO). Compared to their predecessors in geosynchronous orbits (GEO) at approximately 37,000 kilometers, LEO satellites orbit between 500 and 2,000 kilometers from Earth and are capable of providing lower latency, higher bandwidth per user, and global coverage using their large constellations of satellites.[80] Driven by a convergence of demand for higher bandwidth connections and advancements in launch capabilities and satellite technologies, the market for pLEO-based satellite communications is experiencing an emergent market for commercially available options by which an insurgent communicator may circumvent the potentially penetrated and vulnerable terrestrial-based communications networks in their region.[81]

Efforts made by Great Power Competitors—Russia and China—have severely increased the threat of surveillance and targeting to insurgent organizations operating on civilian-oriented communications infrastructures or through potentially compromised telecommunications providers. The Russian "Sovereign Internet Laws" introduced in 2019 have created legal frameworks for centralized state management and surveillance of internet-based activities within Russian borders and for online activities conducted by Russian

[80] Chris Daehnick, Ben Maritz, Bill Wiseman, and Isabelle Klinghoffer, "Large LEO Satellite Constellations: Will It Be Different This Time?" McKinsey & Company, accessed May 1, 2023, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time

[81] Daehnick et al., "Large LEO Satellite Constellations: Will It be Different This Time?"

citizens.[82] For example, Article 71 of the Russian Constitution and Government Decree 2385 (December 2020) stipulate that digital telecommunications data on Russian users is subject to regulation, examination, and protection by the Russian government and intelligence agencies. Furthermore, these legislative controls mandate that data on Russian citizens is stored in Russian servers, on Russian soil, beyond the purview of foreign intelligence and information operations entities.[83] Similarly, the Chinese have created the Golden Shield Project ("The Great Firewall of China"), to allow the Chinese Ministry of Public Security to screen, censor, and track digital information flows to and from Chinese users and devices.[84] Likewise, the Chinese have also enacted their own extraterritorial "Personal Information Protection Law" (PIPL) that places all individuals, organizations, and corporations providing communications to Chinese individuals or within Chinese borders under the regulatory scrutiny of the Chinese government.[85]

These trends in legal regulation and intelligence penetration of telecommunication service providers by Great Power Competitors have increased the operational risk borne of an insurgent communicator transmitting data across civilian networks or communications infrastructures. Due to the inherently vulnerable nature of terrestrial-based communications infrastructures, pLEO-based satellite communications may provide an insurgent communicator with a communicative medium that circumvents the use of hazardous networks or exploited infrastructures. By shifting communications—even encrypted ones—from civilian networks to commercial satellite systems, the insurgent communicator may increase their operational security by mitigating risk and exposure to adversarial intelligence and surveillance activities. The following sections of this thesis will evaluate the viability of

[82] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law," German Council on Foreign Relations, January 16, 2020, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[83] Sapranov, "Telecoms, Media, and Internet Report: Russia."

[84] Conrad Chan, Anthony Dao, Justin Hou, Tony Jin, and Calvin Tuong, "Free Speech versus Maintaining Social Cohesion – China's Great Firewall," Stanford Institute of Computer Science, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

[85] Miranda Katz, "The Personal Information Protection Law: China's Version of the GDPR?" Columbia Journal of Transnational Law, February 15, 2022. https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.

pLEO-based satellite communications, provide case study examples from the ongoing Russia-Ukraine War and Iranian Mahsa Amini protests, and will address further recommendations for employment and adoption by the U.S. military and intelligence communities.

B. APPLICABILITY CRITERIA: PROLIFERATED LOW EARTH ORBIT SATELLITE COMMUNICATIONS

For pLEO-based satellite communication systems to serve as viable mediums for clandestine insurgent communications, they must meet the four general requirements proposed in this thesis. pLEO-based communications must be commercially available as both hardware and services with orbital coverage of the region in question, be accessible with minimal technological sophistication, be protective of transmitted information, and be viable for the transmission of insurgent leadership, direction, recruiting, or other organizational guidance. The following sections will address broad considerations of the availability and use of pLEO-based communication networks within the evaluative framework established by this thesis.

1. Commercial Availability of pLEO Satellite Communications

The demand for commercial satellite communications has developed rapidly in recent decades.[86] Specifically, increases in the proliferation and technological capacity of consumer telecommunications networks have driven demands for high data throughput, transmission capacity volumes, reduced latency, and affordable bandwidth services.[87] This increasing consumer demand for satellite communications in concert with recent technological innovations in reusable launch vehicles, has created a growing market for commercially available satellite communications options.[88] This emergent market for globally available satellite communications has increased an insurgent communicator's access to

[86] Olivier Hauw, "The Evolution of Commercial Satellite Communications," Airbus – Secure Communications, 2023, https://securecommunications.airbus.com/en/meet-the-experts/evolution-commercial-satellite-communications.

[87] Hauw, "The Evolution of Commercial Satellite Communications."

[88] Jones, "The Recent Large Reduction in Space Launch Cost."

communicative mediums that supersede or circumvent the potentially hazardous terrestrial telecommunications networks.

pLEO-based satellite communications are now commercially available to civilian consumers, with additional services and brands launching in the near future.[89] SpaceX's Starlink constellation is currently the leading provider of pLEO-based communications services with the highest number of on-orbit satellites and global customers. With over one million active subscribers and three thousand operational satellites in orbit, the Starlink constellation is a prime candidate for insurgent communicators seeking to avoid using compromised telecommunications infrastructure.[90] Furthermore, the Starlink constellation has already been employed in insurgent communications networking in the Russia-Ukraine War and in support of Mahsa Amini protests in Iran.[91] In addition to the currently available Starlink constellation, insurgent communicators will soon be able to connect to Project Kuiper (Amazon) pLEO-based communications services, which are scheduled to come online in the second half of 2024.[92]

Based on the precedent by set by SpaceX's Starlink services, an insurgent communicator may expect to pay anywhere from $500 to $2500 USD for the small aperture terminals—antenna hardware—and between $100 to $500 USD per month for pLEO-based broadband data services.[93] However, due to trends in efficiency, it may be expected that as companies like SpaceX and Amazon streamline production and achieve economies of scale, these hardware and service fees will decrease over time as their products become cheaper to

[89] Amazon, "Here's Your First Look at Project Kuiper's Low-Cost Customer Terminals," March 14, 2023, https://www.aboutamazon.com/news/innovation-at-amazon/heres-your-first-look-at-project-kuipers-low-cost-customer-terminals.

[90] Kate Duffy, "Starlink Has Hit More than 1 Million Users despite a Drop in Download Speeds. Here's What You Need to Know about the Service," Business Insider, December 20, 2022, https://www.businessinsider.com/spacex-starlink-internet-service-elon-musk-all-you-need-know-2021-2.

[91] Duffy, "Starlink Has Hit More than 1 Million Users despite a Drop in Download Speeds. Here's What You Need to Know about the Service."

[92] Amazon, "Here's Your First Look at Project Kuiper's Low-Cost Customer Terminals."

[93] Cara Haynes, "Starlink Internet Review 2023: Plans, Pricing, and Speeds," Satellite Internet Inc, March 20, 2023, https://www.satelliteinternet.com/providers/starlink/#:~:text=Starlink%20costs%20%24110%20per%20month,%242%2C500%20one%2Dtime%20equipment%20fee.

produce and more widely available to consumers.[94] Thus, based on the emergent market and the growing availability of pLEO-based satellite services, it may be asserted that an insurgent will feasibly have access to commercially available PLEO-based communications as a communicative medium.

2. User Accessibility of pLEO Satellite Communications

In order for pLEO-based satellite communications to be a viable medium for an insurgent communicator they must be of minimal criminal and technological sophistication to maximize communications between members of the insurgent organization and the host population. Because pLEO-based satellite communication networks are marketed towards civilian consumers and in direct competition with preexisting telecommunications providers, their services are generally parallel to current standards of service provision.[95] Furthermore, satellite-based communications offer a number of features that that are not readily available via traditional terrestrial microwave, cable, or fiber optic networks. These advantages include distant independent transmission costs, fixed broadcast costs, large information bandwidths, low error rates, and wider availability to diverse user networks.[96] For example, the globally connectable and commercially available Starlink hardware package is comprised of five items, a portable 20-inch Starlink terminal (antenna), antenna stand, router, and two cables.[97] Once configured, the five items in the Starlink residential terminal package act like a common household wireless router—projecting internet availability to up to 128 devices across a maximum of 185 square meters around the terminal apparatus.[98] Once the hardware has been configured, users may connect to the Starlink internet connection via their standard Wi-Fi interfaces on their devices or through a direct Ethernet-wired connection into the Starlink

[94] Amazon, "Here's Your First Look at Project Kuiper's Low-Cost Customer Terminals."

[95] Enrique Dans, "How Starlink Is about to Disrupt the Telecommunications Sector," Forbes Magazine, February 23, 2021, https://www.forbes.com/sites/enriquedans/2021/02/23/how-starlink-is-about-to-disrupt-the-telecommunications-sector/?sh=70ea9f46659a.

[96] Louis J. Ippolito, "Introduction to Satellite Communications." In Satellite Communications Systems Engineering, 2nd ed., 33–34. United States: Wiley, 2017. https://doi.org/10.1002/9781119259411.ch1.

[97] Starlink, "Starlink Residential User Guide." SpaceX, 2022. https://www.starlinkinternet.info/en-us/GettingStartedWithStarlink.

[98] Starlink, "Starlink Residential User Guide."

router.[99] Likewise, Project Kuiper's initial terminal based hardware systems will deploy with similarly user friendly and portable systems in the form of a 1-lb, 7 inch tall terminal that will provide users with similar Wi-Fi interfaced internet connectivity.[100]

Because terminal-based commercial satellite communications operate in direct competition with traditional terrestrial telecommunications services they are designed to minimize operational complexities that would deter potential customers.[101] pLEO-based providers like Starlink and Project Kuiper have designed their systems to operate similarly to preexisting wireless router technologies—providing internet connections through preexisting interfaces on consumer devices. It is highly likely insurgent organizations and their host populations are already employing cellular or wireless internet technologies of equal complexity to the emergent pLEO-based satellite communications. Due to the use of familiar user interfaces and parallels to preexisting communications technologies, this thesis asserts that pLEO-based satellite communications meet the accessibility and usability criteria required of clandestine communications.

3. Concealment or Protection Provided by pLEO Satellite Communications

pLEO-based satellite communications provide an insurgent communicator with communicative channels external to potentially compromised or penetrated local and regional telecommunications providers. Very small aperture terminal connections to pLEO-based internet networks may be rapidly established or installed and allow an insurgent communicator to transmit data independently from terrestrial infrastructure by creating an independent micro-wave relay from mobile terminal locations directly to the proliferated satellite constellation.[102] Unlike previous examples of steganographic data embedding, satellite-based communications provide protection of transmitted data vice concealment. Data

99 Starlink, "Starlink Residential User Guide."

100 Amazon, "Here's Your First Look at Project Kuiper's Low-Cost Customer Terminals."

101 Dans, "How Starlink Is about to Disrupt the Telecommunications Sector."

102 Elbert, Bruce R. *Introduction to Satellite Communication. 3rd ed.* (Boston: Artech House, 2008) 7–12.

transmitted over commercial satellite providers is protected from the potential surveillance or scrutiny incurred in terrestrial telecommunications activity.

Ultimately, the ability of an insurgent communicator to use PLEO-based technologies to circumvent adversarial surveillance and targeting establish the technology as a viable protective measure for clandestine communications. Later portions of this thesis section will address recent and ongoing examples of communicative protection provided by PLEO-based satellite communications.

4. Viability of Use in Insurgent Communications for pLEO Satellite Communications

In addition to their commercial availability and protective qualities, pLEO-based satellite communications also maintain robust data transmission capabilities. The leading providers—SpaceX's Starlink and Amazon's Kuiper Project—both project broadband data transmission speeds between 50–500 megabits per second (MBPS), transmission levels comparable to commonly used household fiber optic-based internet connections.[103] In addition to portable uplink antenna hardware, Starlink pLEO-based systems use orthogonal frequency division multiplexing (OFDM) modulation to efficiently encode digital transmissions into equally spaced frequency range bins and use inverse fast Fourier transforms (IFFT) to transform signals into orthogonal overlapping sinusoids in the time domain to maximize the amount of data that may be transmitted over a fixed amount of bandwidth.[104] Figure 16 demonstrates a visual representation of the 10.7 to 12.7 GHz Starlink downlink signal as reverse-engineered by the University of Texas' Department of Aerospace Engineering and Engineering Mechanics department. By dividing satellite downlink signals into frequency ranges, pLEO-based service providers efficiently divide available bandwidth resources, enabling service provisions to numerous simultaneous users in shared or disparate

[103] Haynes, "Starlink Internet Review 2023: Plans, Pricing, and Speeds."

[104] Mark Harris, "Starlink Signals Can Be Reverse-Engineered to Work like GPS-Whether SpaceX Likes It or Not," MIT Technology Review, October 24, 2022, https://www.technologyreview.com/2022/10/21/1062001/spacex-starlink-signals-reverse-engineered-gps/; MATLAB & Simulink. "What Is OFDM?" 2022. https://www.mathworks.com/discovery/ofdm.html.

regions.[105] In both uplink (transmit) and downlink (receive) scenarios, pLEO-based satellite communications allow for robust data transmissions for insurgent communicators operating in surveilled, denied, or geographically isolated environments. The robust data transmission capabilities and expedient employment options provided by pLEO-based communications systems ensure that they are viable communications options for an insurgent communicator seeking to establish secure but secretive communication links between insurgent cells, the population, and weapons systems or kinetic effects providers.

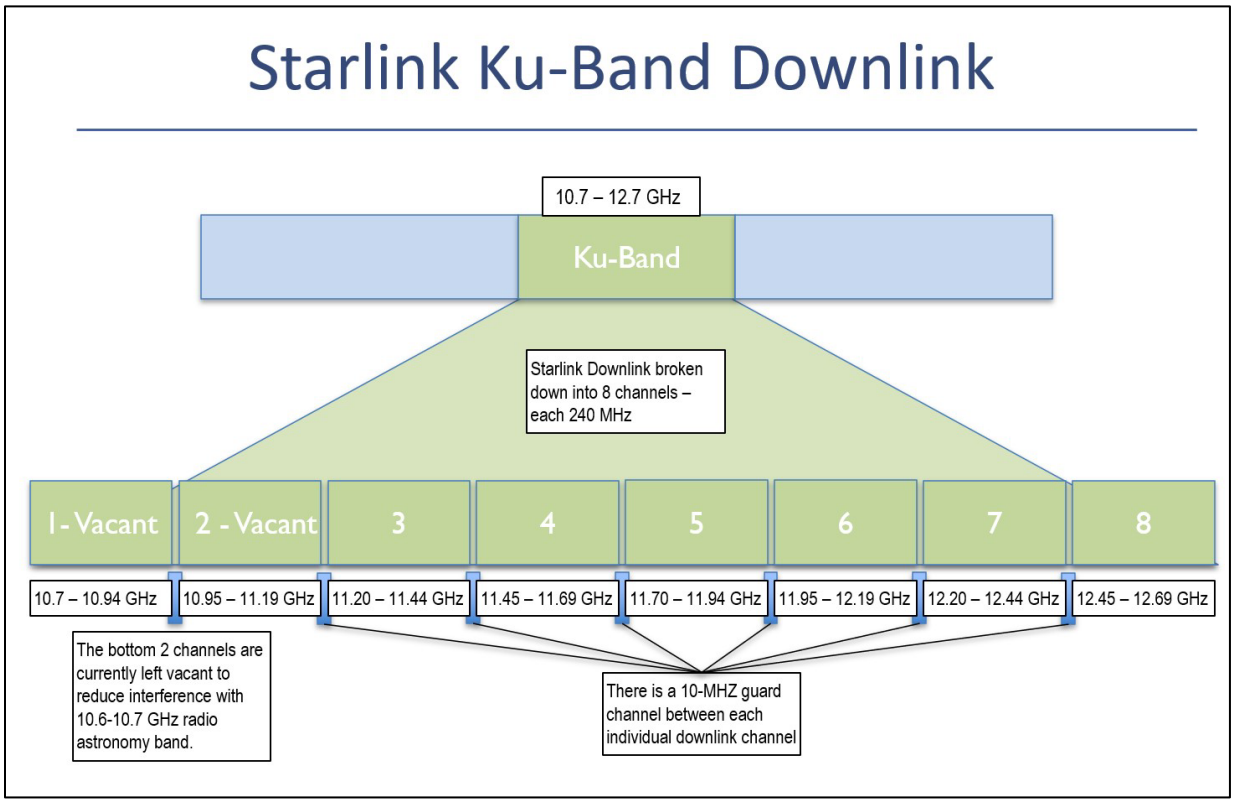

Figure 16. Starlink Ku-Band Downlink Frequency Breakdown Diagram.[106]

Ultimately, using advanced modulation techniques and portable hardware, pLEO-based satellite communications allow insurgent communicators to rapidly establish protected

[105] Todd E. Humphreys, Peter A. Iannucci, Zacharias Komodromos, and Andrew M. Graff, "Signal Structure of the Starlink Ku-Band Downlink," The University of Texas at Austin, 2022. https://doi.org/10.48550/arxiv.2210.11578.

[106] Adapted from Humphreys et al., "Signal Structure of the Starlink Ku-Band Downlink."

communications channels between both insurgent and host population nodes. By transcending terrestrial telecommunications networks, pLEO-based communications may serve as viable methods of protecting and transmitting sensitive and timely data in such a manner that limits operational risk to insurgent organizations while maximizing the efficiency and coordination of insurgent activities in contested regions. The following section of this thesis section will address two case studies of recent pLEO-based insurgent communications and the lessons learned from their employment.

C. PROTECTED INTERNET RESOURCES: METHODS OF COMMUNICATION VIA PLEO SATELLITE COMMUNICATIONS

1. Introduction: Employment of Emergent Satellite Communications Technologies.

Because pLEO-based satellite communications networks are emergent technologies, historical insurgent use cases are limited. However, recent employments of Starlink terminals have been critical enabling factors in two recent and ongoing conflicts in Iran and Ukraine respectively. The following case studies will evaluate the communicative capacity, operational impact, and lessons learned from the employment of pLEO-based Starlink communications networks as they pertain to enabling insurgent activities and maximizing operational capacity. This thesis asserts that PLEO-based communications networks allow insurgent organizations and their host populations to efficiently establish two-way communication channels that transcend the vulnerable terrestrial-based telecommunications infrastructures within their geographic regions. In this light, pLEO-based communications represent a protected form of communication that ensures the confidentiality, integrity, and availability of the transmitted information.

2. Case Study 3: pLEO Communications in the Russia-Ukraine War

The first and ongoing example of pLEO-based satellite communications being leveraged in an asymmetric conflict is currently unfolding in the Russia-Ukraine War. On February 26, 2022—within days of the start of the Russian military offensive into Eastern Ukraine—Ukrainian Vice Prime Minister Mykhailo Fedorov leveraged public messaging via the social media outlet—Twitter—to petition SpaceX's CEO—Elon Musk—directly for

Starlink terminals.[107] This interaction would result in tens of thousands of Starlink terminals being deployed into Ukraine to serve as aids to humanitarian efforts as well as communication channels for the Ukrainian military apparatus during the conflict.[108] Faced with severe conventional military disadvantage and targeting by the robust Russian electronic warfare apparatus, Starlink has provided high-speed internet connections to remote locations and Ukrainian end-users in conflict zones where access is unreliable or denied.[109]

Since the advent of the Russia-Ukraine War in February 2022, Starlink has served as a critical communication stopgap for Ukrainian command, control, and infrastructure elements.[110] Due to the mobile and robust data capabilities provided by Starlink VSAT networks, Starlink as a service has served as a critical gap filler in both combat and noncombat operations. Despite Russian attempts to use precision strike weapons technology against critical Ukrainian infrastructure nodes, the Ukrainian government and military have been able to employ Starlink terminals post-strike to maintain service in targeted or denied areas.[111] Due to the continual targeting and attrition of the Ukrainian telecommunications infrastructure, Starlink has become an integral element in the Ukrainian government, military, and public response to the Russian invasion. With upwards of 150,000 daily users of Starlink-provided Internet, the pLEO-based communication network has become a keystone development in the command, control, communications, intelligence, surveillance, and reconnaissance (C4ISR) of the Ukrainian counter-offensive.[112]

---

[107] Rishi Iyengar, "Why Ukraine Is Stuck with Elon (for Now)," Foreign Policy, November 22, 2022. https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-russia-war/.

[108] Iyengar, "Why Ukraine Is Stuck with Elon (for Now)."

[109] Oleksandra Yeremenko, Oleksandr Lemeshko, M. Persikov, and V. Lemeshko. "ICT Disruptive Technologies: Starlink in Ukraine Case," Kharkiv National University of Radio Electronics, 2022, https://openarchive.nure.ua/server/api/core/bitstreams/9e6ec44a-5b78-4e5d-b98e-d53bb94a6d86/content

[110] Reuters, "Starlink Helped Restore Energy, Communications Infrastructure in Parts of Ukraine – Official," Thomson Reuters, October 12, 2022. https://www.reuters.com/world/starlink-helped-restore-energy-communications-infrastructure-parts-ukraine-2022-10-12/.

[111] Reuters, "Starlink Helped Restore Energy, Communications Infrastructure in Parts of Ukraine – Official."

[112] The Economist, "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare. The Economist – Briefing: A Murmuration of Starlinks," The Economist Newspaper, January 5, 2023, https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

Starlink terminals have also facilitated the emergence of a robust intelligence network that leverages civilian reporting to tip and queue kinetic targeting of Russian military units and personnel in contested regions.[113] By using Starlink-provided internet connections, Ukrainian civilians have been able to upload pictures and report geolocated sightings of Russian military units directly to Ukrainian artillery-battery commanders, who use the data to coordinate fires and shell enemy targets.[114] This method of pairing civilian reporting with military firepower has been leveraged successfully by the Ukrainian counter-offensive to achieve strategic-level success in their efforts to remove Russian elements from contested regions of Eastern Ukraine.[115] For example, small insurgent cells comprised of civilian activists and Ukrainian military intelligence operators were able to provide targeting data on a Russian field hospital, barracks, and food storage facility established in a large electronics store located in the contested Kherson Oblast in Eastern Ukraine.[116] By capturing geolocation-enabled photos and reporting on the daily activities of Russian military units, these insurgent members of the Kherson population would provide critical target data for the military strike operations to come. This civilian-enabled targeting effort would ultimately result in the destruction of the Russian military facility and contribute to the Russian retreat from the Kherson Oblast in late 2022.[117] Figure 17 depicts the location of the Russian military facility following the Ukrainian precision strike operations that rendered the facility inoperable for further hospital, housing, or resource storage operations for the Russian military occupiers.

[113] The Economist, "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare."

[114] The Economist, "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare."

[115] Matthew Luxmoore, "Ukraine's Secret Weapon Is Ordinary People Spying on Russian Forces," The Wall Street Journal, December 15, 2022, https://www.wsj.com/articles/ukraines-secret-weapon-is-ordinary-people-spying-on-russian-forces-11671012147?st=3sak0b2r2zwv95r.

[116] Luxmoore, "Ukraine's Secret Weapon Is Ordinary People Spying on Russian Forces."

[117] Luxmoore, "Ukraine's Secret Weapon Is Ordinary People Spying on Russian Forces."

Figure 17. Activists Sent Photos of an Electronics Store Russian Forces Used in Kherson to the Ukrainian Military.[118]

In addition to serving as a linkage between pro-Ukrainian insurgent cells and conventional Ukrainian military forces, Starlink has additionally served to enhance small-scale insurgent attack and sabotage techniques. By configuring the lightweight Starlink terminals to work as the datalink for unmanned aerial vehicles—specifically smaller quadcopter-style drones—Ukrainian resistance fighters are able to extend the range and duration of drone-based surveillance or attack operations. Figure 18 demonstrates the smaller-scale weaponization options available to VSAT technologies like Starlink. By affixing explosive devices like 82mm mortar rounds and a Starlink terminal to an unmanned aerial vehicle, an insurgent or military organization may deliver explosive munitions or conduct extended periods of surveillance beyond the 5–12 kilometer transmission range provided by

[118] Source: Serhii Korovayny, "Activists Sent Photos of an Electronics Store Russian Forces Used in Kherson to the Ukrainian Military, Which Destroyed the Store." The Wall Street Journal, December 15, 2022, https://www.wsj.com/articles/ukraines-secret-weapon-is-ordinary-people-spying-on-russian-forces-11671012147?st=3sak0b2r2zwv95r.

radio frequency-based drone controls.[119] Thus, by employing emergent communicative capacities in tandem with pre-existing strategies, an insurgent cell may enhance its operational capacity with minimal additional hardware or adaptations to previous methods of weapons employment.

Figure 18. Photo of a Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces.[120]

The Ukrainian population's employment of Starlink VSAT terminals as weapon enhancements and quick response reporting channels for targeting data demonstrates the utility of pLEO-based forms of communication. Because Starlink satellite communications allow insurgent intelligence gatherers to clandestinely report the location and activities of enemy units or increase the effective range of their improvised weapons systems, they are a force multiplier for an insurgent cell's operational capacity and a link to external resources

[119] Mark Rutherford, "The Issues with Jamming Drone Frequencies," D-Fend Solutions, February 12, 2023, https://d-fendsolutions.com/blog/issues-with-jamming-drone-frequencies/#:~:text=Frequency%20Bands,-Commercial%20drones%20operate&text=Most%20of%20the%20more%20expensive,some%20as%20far%20as%2012km; Rob Lee, "Photo of a Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces." Twitter post, March 25, 2023. https://twitter.com/RALee85/status/1639749679079383042/photo/1

[120] Source: Lee, "Photo of a Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces."

and weaponeering. By providing intelligence networks and weapons systems with the ability to transmit targeting data quickly, secretly, and securely, commercial pLEO-based satellite communications are critical enablers of an insurgent organization's ability to coordinate, strike, and remain concealed during operations against an asymmetrically advantaged adversary. Given the modeling framework provided by McCormick and Owen's "Security and Coordination in a Clandestine Organization," the inclusion of this thesis' proposed technology scaling variable, and open source reporting on the number of Starlink terminals currently operating in Ukraine, Figure 19 demonstrates the positive impact that protected pLEO communications may impart pro-Ukrainian insurgents operating cells operating in the contested Ukrainian terrain.[121] Recent statements made by SpaceX's founder and CEO Elon Musk claim that there are approximately 25,000 Starlink terminals operating in Ukraine, and, operating at maximum capacity each of these 25,000 terminals may support up to 128 users simultaneously—up to 3.2 million users if employed in a maximum use scenario.[122][123] Furthermore, if all Starlink terminals operating in Ukraine were allocated to the oblasts declared "annexed" by the Russian Federation—Luhansk Oblast, Donetsk Oblast, Zaporizhzhia Oblast, and the Kherson Oblast, these 3.2 million users would represent roughly 36% of the regional population (8.79 million).[124][125] Using the technology scaling variable provided in the modeling section of this thesis, this 36% employment rate of protected communications would result in a technology scaling variable value of 1.56. Figure 19 demonstrates the net positive impact that this technology scaling function would impart on the operational capacity of the Ukrainian insurgent forces operating in enemy controlled territory. Note, Figure 19 adheres to the notional baseline parameters of $k = 0.1$, $a = 0.2$, and $C_j = 1$ from the "Updated Modeling" section of this thesis.

---

[121] McCormick and Owen, "Security and Coordination in a Clandestine Organization," 178.

[122] Mike Wall, "1,300 SpaceX Starlink Terminals with Ukraine's Military Went Offline Due to Funding Shortfall: Report," Space.com, November 8, 2022. https://www.space.com/ukraine-spacex-starlink-terminals-offline-funding-shortfall.

[123] Starlink, "Starlink Residential User Guide."

[124] Steven Pifer, "The Russia-Ukraine War and Its Ramifications for Russia," Brookings Institute, February 24, 2023, https://www.brookings.edu/articles/the-russia-ukraine-war-and-its-ramifications-for-russia/.

[125] Statista Research Department, "Total Population of Ukraine as of February 1, 2022, By Region," March 6, 2023, https://www.statista.com/statistics/1295222/ukraine-population-by-region/

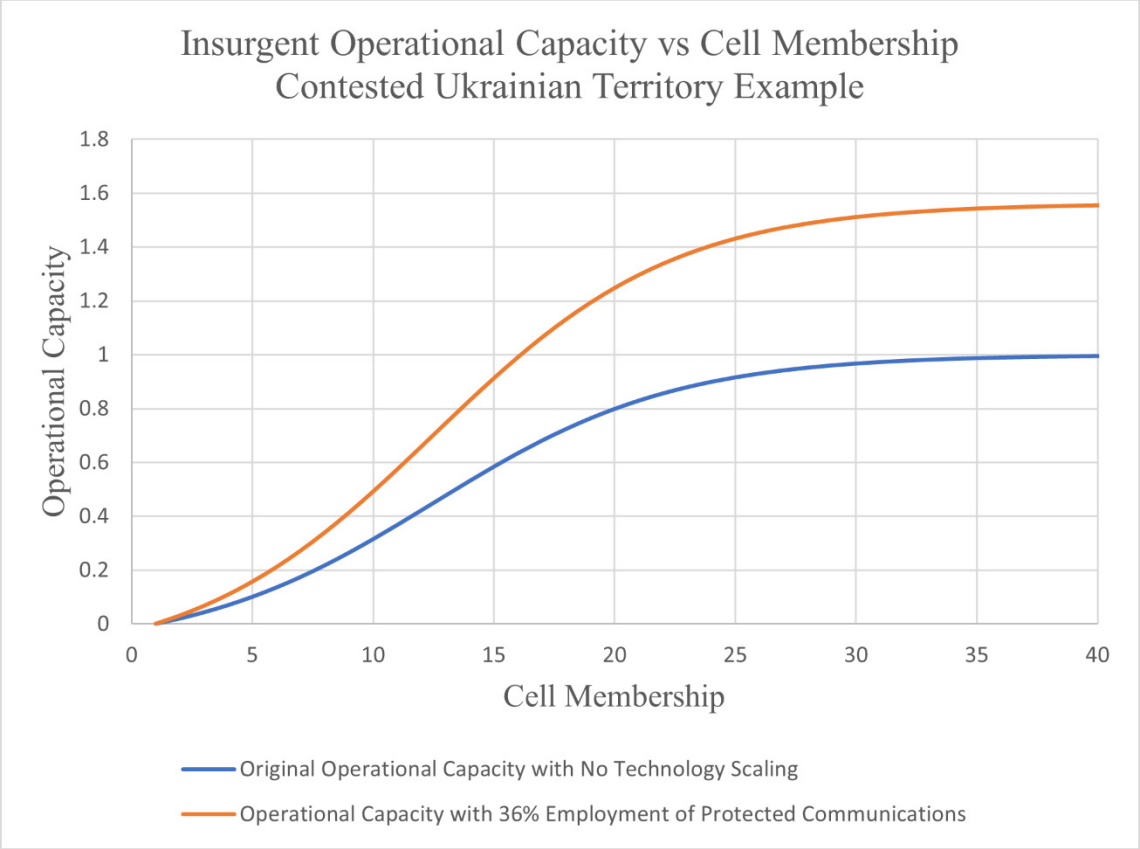

Figure 19. Operational Capacity Gains for 36% Adoption of Protected Communications Technologies. Application of Insurgent Modeling to Contested Ukrainian Oblasts.

While satellite communications technologies like that provided by Starlink are not invulnerable to enemy jamming and targeting efforts, they provide an insurgent communicator with an additional avenue for data transmission and impose additional surveillance requirements on an adversary seeking to limit the operations of an insurgent organization. Because satellite communications are owned and operated by often geographically and politically independent providers and act as an alternative layer to the terrestrial telecommunications infrastructure, they may serve as highly effective communications tools for insurgencies operating in regions in the periphery of Great Power Competitors with robust intelligence apparatuses. The Ukrainian employment of Starlink technologies as an enabler for intelligence networks and precision strike operations demonstrates the tactical and strategic opportunity provided by pLEO-based communications technologies in kinetic operations. Despite disadvantages in conventional military capacity,

the communications advantages provided by satellite communications may allow insurgent organizations and asymmetrically disadvantaged organizations to leverage intelligence and strike capabilities in kinetic conflict. Later portions of this section will address potential methods of support, both operationally and financially, that the U.S. may employ to maximize the distribution and employment of pLEO-based technologies by cells operating in favor of U.S. interests within the Great Power Competition.

3. Case Study 4: pLEO Communications in the "Mahsa Amini" Protests in Iran

The second case study oriented on the insurgent employment of proliferated low earth orbit satellite communications comes from recent use in antigovernment protests that occurred in late 2022 in Iran. Following the death of 22-year-old Iranian Mahsa Amini at the hands of Tehran's "Gasht-e Ershad" morality police in September 2022, large-scale antigovernment protests erupted across Iranian cities and social media outlets.[126] Immediately following Amini's death and the initiation of protest activities, the Iranian government exercised its control over the three mobile and one wireline telecommunications companies that provide over 85% of network traffic to Iranian users to restrict data usage and impose digital curfews on the Iranian public.[127][128] The desired end state of these restrictions on consumer data flows was inferably to deny access to social media and digital messaging applications in an attempt to curb the coordination of further civil unrest and dissemination of anti-governmental materials.[129] Figure 20, a graphic developed by Cloudflare—a U.S.-based network service and cloud-based cybersecurity firm—demonstrates the control leveraged by the Iranian government against its domestic telecommunications providers by outlining the immediate decline in network availability occurring between the 16th and 17th of September—the day

[126] Reuters, "Events in Iran since Mahsa Amini's Arrest and Death in Custody," December 12, 2022. https://www.reuters.com/world/middle-east/events-iran-since-mahsa-aminis-arrest-death-custody-2022-10-05/.

[127] Reuters, "Events in Iran since Mahsa Amini's Arrest and Death in Custody."

[128] James Allworth, "Two Months Later: Internet Use in Iran during the Mahsa Amini Protests," Cloudflare Inc, December 12, 2022, https://blog.cloudflare.com/two-months-later-internet-use-in-iran-during-the-mahsa-amini-protests/.

[129] Allworth, "Two Months Later: Internet Use in Iran during the Mahsa Amini Protests."

of and day after Mahsa Amini's death in police custody.[130] Specifically, the graphic depicts the Iranian government's ability to restrict consumer data flow by conducting comprehensive coverage blackouts across the primary telecommunications providers—Mobile Communication Company of Iran (MCCI-AS), IranCell, Rightel, and IranTel.[131]

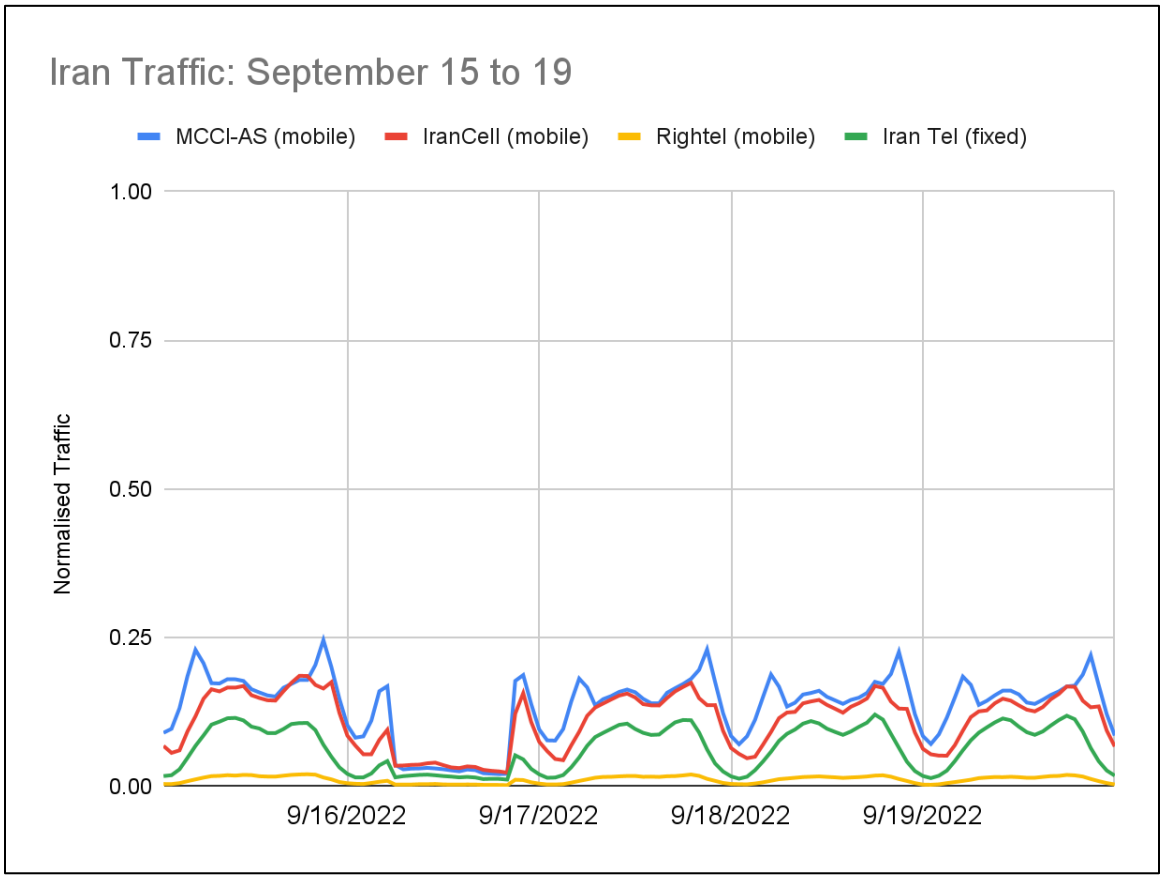

Figure 20. Iranian Network Traffic from September 15–19, 2022.[132]

In addition to the blunt methods of state-levied data censorship, the Iranian Communications Regulatory Authority also maintains a computer-based surveillance and control system called "SIAM" that allows the Iranian government to conduct a broad set of

[130] Allworth, "Two Months Later: Internet Use in Iran during the Mahsa Amini Protests."

[131] Allworth, "Two Months Later: Internet Use in Iran during the Mahsa Amini Protests."

[132] Source: Allworth, "Two Months Later: Internet Use in Iran during the Mahsa Amini Protests."

surveillance, remote-access, and service denial activities against any device connected to Iranian telecommunications networks.[133] At its core the SIAM system is a surveillance and censorship tool that allows Iranian intelligence and law enforcement operators to alter, disrupt, and monitor Iranian cellular data traffic.[134] The SIAM suite of tools comprehensively denies the Iranian public from maintaining the confidentiality, integrity, and availability of their transmitted data by controlling data connection speeds, breaking encryptions on voice and text messaging, tracking device movements, and producing detailed metadata target devices and networks of individuals.[135] Thus, even when internet-enabled communications are available to Iranian data users, there is a significant possibility of those communications being used as targeting data for the authoritarian state's intelligence, military, and law enforcement apparatus. Iranian protestors and insurgents are thus forced to operate in data-deprived environments or in exploited networks that increase their risk of targeting and attrition.

Following the internet blackouts imposed by the Iranian national government, the United States Treasury Department issued a license to allow U.S. companies with the ability to "expand the range of internet services available to Iranians" with the further explicit intent to help "the Iranian people be better equipped to counter the government's efforts to surveil and censor them."[136] This circumvention of standing sanctions preventing U.S. corporations from doing business in Iran allowed U.S.-based SpaceX to begin providing Starlink internet services to Iranian civilians and resulted in the infiltration and activation of approximately 100 Starlink terminals within Iranian borders by December 2022.[137] Similar to the protected communications used by Ukrainian Starlink users, Iranian protestors have likewise begun

[133] Sam Biddle, and Murtaza Hussain, "Hacked Documents: How Iran Can Track and Control Protesters' Phones," The Intercept, October 28, 2022, https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/.

[134] Biddle and Hussain, "Hacked Documents: How Iran Can Track and Control Protesters' Phones."

[135] Biddle and Hussain, "Hacked Documents: How Iran Can Track and Control Protesters' Phones."

[136] Wall Street Journal Editorial Board, "Opinion | Elon Musk Has a Better Iran Idea," The Wall Street Journal, September 25, 2022, https://www.wsj.com/articles/elon-musk-has-a-better-iran-idea-starlink-protests-mahsa-amini-11663883982.

[137] Reuters, "Elon Musk Says around 100 Starlinks Now Active in Iran," December 27, 2022. https://www.reuters.com/technology/elon-musk-says-around-100-starlinks-now-active-iran-2022-12-26/.

employing Starlink internet services as a stopgap and bypass mechanism for their heavily restricted and surveilled local telecommunications infrastructure.[138]

While a small number of clandestinely employed Starlink terminals does not constitute a comprehensive pLEO-based coverage network, they may serve as critical nodes, providing a distributed network of touchpoints through which larger portions of the Iranian protestor population may receive guidance from insurgent organizers or news from the global community.[139] Additionally, Starlink terminals have provided the Iranian public with a channel to the outside world where their texts, videos, and social media posts may be used to generate global political and financial support for their protests and cause.[140] As protests and civil rights movements continue in Iran, it may be expected that further infiltration and activation of pLEO-based networks will continue. As demonstrated in the Technology Scaling Variable equation provided in earlier sections of this thesis, as more and more portions of the population adopt protected communications, the insurgent operational capacity in the region will increase exponentially. Widespread adoption and employment of protected communications assets like pLEO-based VSAT technologies will saturate adversarial surveillance capacities and limit their ability to target insurgent actors. While the Iranian government may be able to identify and target insurgents via the tracking and surveillance of a hundred terminals, their surveillance efforts will become much more resource intensive and much less scrutable against a network of potentially thousands of terminals and tens of thousands of users.

As a proof of concept, the use of Starlink terminals in a denied information environment against an established and highly capable authoritarian regime demonstrates the efficacy and utility of pLEO-based communications as enabling technologies for non-militarized insurgent movements. Starlink-provided internet access is not beholden to the Iranian Communications Regulatory Authority and is not host to the spying eyes of surveillance programs like SIAM. The Mahsa Amini protest movement's employment of

138 Karl Vick, "How Activists Get Elon Musk's Starlink to Iran's Protesters," Time – World News – Iran, January 25, 2023, https://time.com/6249365/iran-elon-musk-starlink-protests/.

139 Vick, "How Activists Get Elon Musk's Starlink to Iran's Protesters."

140 Vick, "How Activists Get Elon Musk's Starlink to Iran's Protesters."

limited pLEO-based networking resources demonstrates the large impact that a relatively small amount of physical hardware and commercial services can provide. Starlink has been a critical enabler for communications internal to the Mahsa Amini protest movement in Iran, but also as a generative factor for global attention, solidarity, and financial support for the movement as well.[141] The following section of this thesis will address recommended use cases for U.S. military support to insurgent organizations through the provision and employments of emergent technologies like those seen in the Mahsa Amini protest. Ultimately, the successes and failures of Iranian protestors and insurgent communicators serve to outline the viability of commercial satellite communications for insurgent movements as well as refine the tactics, techniques and procedures that will enable future insurgents and warfighters alike.

D. RECOMMENDED USE CASES FOR PLEO-BASED COMMUNICATIONS

Because pLEO-based satellite communications provide insurgent organizations with a commercially available, globally accessible internet connection that transcends the potentially hazardous telecommunications providers and infrastructures in their region, they are uniquely suited to serve as a scalable communications solution for an insurgent organization throughout its operational life cycle. As demonstrated in the Mahsa Amini protests and the Russia-Ukraine war, pLEO-based communications can provide resilient communications to both large and small-scale operations in both kinetic and non-kinetic environments. As protective mediums, pLEO-based communications channels provide confidentiality, integrity, and availability of communicative data transmissions regardless of legal control or intelligence penetration of local telecommunications providers. Due to the significant mitigation of risk provided by pLEO-based communications, this thesis recommends that pLEO-based satellite communications be leveraged to the maximum extent possible in accordance with the available hardware resources in a given region. In addition to the significant security provided by commercial satellite communications, the consumer-oriented designs of emergent VSAT technologies ensure that they are viable channels of communications both internally to the insurgent organization and externally between the

141 Vick, "How Activists Get Elon Musk's Starlink to Iran's Protesters."

general population as well. In this light, pLEO-based communications may serve as viable communications channels for sensitive and timely intra-insurgency communications as well as for coordination, recruitment, and education efforts with the host population.

Ultimately, an insurgency's employment of pLEO-based communications will be defined by its ability to acquire terminals and fund the requisite data subscription services to use them. For large-scale employment scenarios with thousands of available terminals and subscriptions, commercial satellite communications may be used to create a shadow network of communications infrastructure as well as provide redundancy for strategic-level operations and activities. Given thousands of terminals and access for hundreds of thousands of users, pLEO-based networks like those used by the Ukrainian resistance forces may be leveraged to extricate a population from its vulnerable terrestrial telecommunications infrastructure and provide robust protected communications resources directly to large portions of the population. Likewise, in small-scale employment scenarios with hundreds of terminals and potentially thousands of subscribers, pLEO-based networks like those used in the Mahsa Amini protests may be leveraged to create information distribution networks. In smaller use case scenarios, terminals may serve as critical nodes in a sparser network connecting an isolated movement to insurgent leadership or support from the outside world.

pLEO-based communications allow insurgents to communicate freely and securely with a lower risk of exploitation, surveillance, or denial by adversarial electronic warfare capabilities or intelligence operations. Due to the protective nature of commercial satellite communications, this thesis recommends that pLEO-based communicative mediums be prioritized for use based on the timeliness and sensitivity of the communications and the availability of commercial hardware and subscriptions. In limited resource scenarios, insurgents should seek to reserve pLEO-based channels for their most important or time-sensitive communications. Given the large bandwidth capacity and uninterrupted coverage provided by commercial pLEO terminals, it is recommended that insurgents maximize available data allocations while maintaining "emissions control" procedures.

While insurgent communicators and sympathizers should maximize the communicative capacity provided by pLEO-based satellite communications, they must establish and adhere to electronic protection (EP) measures known as "emissions control." By

reducing physical, technical, and administrative signatures associated with the use of their commercial satellite services, insurgents may further minimize the risk of detection and targeting by adversarial electronic warfare elements.[142] Among other environment-specific techniques for maintaining the concealment of communications networks, this thesis recommends that, at a minimum, VSAT users employ a modified version of the ten tenets of radio emissions control established by the Marine Corps Intelligence Training Enhancement Program. Table 2 demonstrates the recommended 10 techniques and guidelines for reducing the electromagnetic emissions associated with pLEO-based networking in order to avoid being located and targeted by enemy signals intelligence and reconnaissance assets.

[142] Brian Alcorn, Garrett Boyce, Brian Walsh, Tom Haluska, Evan Kolodziejczak, Kent Johnson, Nick Pugh, Biran Kerg, Nolan Sheahan, and Philip Burtt-Henderson, *EP EMCON SOP: A Guide to Reduce Technical Signature*, (Virginia Beach, VA: Marine Corps Intelligence Schools (MCIS) Intelligence Training Enhancement Program (ITEP), 2020), https://brushbeater.org/wp-content/uploads/2021/03/EP-EMCON-SOP.pdf

Table 2. The Ten Tenets of Reducing VSAT Detectability.[143]

The Ten Tenets of Reducing VSAT Detectability		
	Technique	Guidelines
1	Transmit Less	Transmit only mission-critical information. Avoid Voice-Over-Internet (VOIP) transmissions when text based transmissions are available.
2	Move	Employ a transmit-move-transmit-move cycle of communications to avoid detection and targeting by adversarial direction finding (DF) assets.
3	Brevity	Employ text-based chat applications. Establish brevity codes for locations, activities, and cells/groups.
4	Establish Local Networks	Establish local networks near but not collocated with VSAT terminals. Distance users from the terminal using ethernet connections to nearby routers. Do not attempt to establish a longstanding network in the immediate vicinity of terminal hardware.
5	Mask Terminals	Modify terminals to minimize visual detection. Remove or cover light or reflective materials. Place VSAT hardware (terminals) behind barriers, in dug-out holes, on adjacent rooftops, or behind other pieces of concealing terrain or vegetation to minimize exposure to adversarial surveillance or reconnaissance.
6	Reduce Power	Shut off terminals, routers, and power supplies when not actively configuring networks or transmitting. Minimize electromagnetic leakage.
7	Use Protected Applications	When using VSAT technology with cellular devices, do not transmit data or information on compromised communications applications. Use encrypted-chat applications.
8	Use Multiple Channels	Employ multiple channels for communication based on availability. Seek to build networks of multiple brands of satellite communications providers if/when hardware and subscription services are available. Establish and use rolling communications plans, cycling to secondary and tertiary resources when needed.
9	Proliferate	Maximize non-military use of satellite communications. Mix insurgent data transmissions into civilian and infrastructure-use terminals. More terminals operating in an area increases intelligence/surveillance requirements for the adversary.
10	Randomize	Employ variation in communication schedules, usage patterns, an any other identifiable patterns of use. Share and exchange terminals when operationally possible to disrupt targeting efforts.

E. POTENTIAL U.S. SUPPORT TO AND EMPLOYMENT OF PLEO-BASED COMMUNICATIONS NETWORKS

The employment of pLEO-based communications networks by insurgent organizations may be facilitated by external actors such as the U.S. government and military. These facilitating activities include the leveraging of domestically based satellite communications providers, using military and intelligence personnel or operations to infiltrate required terminal hardware into denied or contested regions, and establishing a

143 Adapted from Alcorn et al., *EP EMCON SOP: A Guide to Reduce Technical Signature*.

financial support base to fund the hardware, software, and subscription services designated for use by members of the insurgent population. By conducting these three supporting activities, the U.S. may effectively introduce and support clandestine communication networks in contested regions and in support of its national interests abroad.

The first supporting activity, leveraging domestic satellite communications providers, requires the U.S. government to maintain cooperative relationships with its private sector as well as legal flexibility with regard to international export laws and limitations. The Mahsa Amini protests demonstrate this need for legal flexibility, as previous sanctions leveraged against the Iranian national government would have otherwise prevented the U.S.-based Starlink from being able to provide services to terminals to users in Iran.[144] Under the initial trade embargoes levied against Iran, most U.S. firms would have been prohibited from trading with, providing services to, or investing in Iran.[145] However, in accordance with the updated "Iranian Transactions Regulations: Guidance on the Provision of Internet Connectivity Services" issued by the Office of Foreign Assets Control, "Internet connectivity services to civilian customers in Iran can be authorized on a case-by-case basis by specific license, provided that the main purpose is to benefit the people of Iran through increased access to information."[146] Further legislation would additionally be leveraged to authorize U.S.-based software service providers to export software services that are "incident to the exchange of personal communications over the Internet, such as instant messaging, chat and email, social networking, sharing of photos and movies, and web browsing."[147] The flexibility demonstrated by the U.S. Treasury Department regarding Iranian sanctions and embargoes highlights the needs for a legally adaptable system that would allow U.S. commercial providers to facilitate insurgent communications and keep pace with emergent technology

144 Zachary Laub, "International Sanctions on Iran," Council on Foreign Relations, July 15, 2015, https://www.cfr.org/backgrounder/international-sanctions-iran.

145 Laub, "International Sanctions on Iran."

146 Office of Foreign Assets Control (OFAC), "Iranian Transactions Regulations: Guidance on the Provision of Internet Connectivity Services (2003)," https://ofac.treasury.gov/media/7896/download?inline.

147 Office of Foreign Assets Control (OFAC), "Iranian Transactions Regulations: Interpretive Guidance and Statement of Licensing Policy on Internet Freedom in Iran (2012)," https://ofac.treasury.gov/media/7891/download?inline

opportunities. As it is likely the U.S. will need to foster insurgent elements in the geographic periphery of or potentially within the borders of a Great Power Competitor, legal flexibility and effective coordination between the government and private industry is a critical requirement for the successfully employment of commercial clandestine communications.

The second supporting activity, leveraging U.S. military and intelligence assets to support device or service infiltration, requires that the U.S. intelligence community and military—particularly elements of special forces command and cyber command—maintain the presence and training required to introduce satellite communications hardware and software to insurgent movements and host populations in potentially denied environments. As demonstrated in the Russia-Ukraine War, private and national postal services may be unavailable or subject to intrusive inspections or screenings that would prevent the delivery of hardware to the desired recipients.[148] Likewise, in denied or surveilled information environments, the availability and transmission of clandestinely capable communications applications may be restricted or hazardous to the accessor.[149] As outlined in the Irregular Warfare Joint (IW) Joint Operating Concept (JOC), U.S. Special Forces Command and the U.S. Marine Corps must be capable of conducting stabilizing irregular warfare activities to develop enabling capacities such as communications in non-state partners as a form of irregular warfare.[150] While many recent applications of irregular warfare activities have been centered on destabilizing activities associated with counter-terrorism operations and counter-insurgency campaigns, this thesis posits that irregular warfare practitioners must also prepare to conduct clandestine and constructive activities such as communication network construction and material support to non-state actors like insurgent movements abroad.

[148] Vick, "How Activists Get Elon Musk's Starlink to Iran's Protesters."

[149] Cybersecurity and Infrastructure Security Agency (CISA), "Russia Cyber Threat Overview and Advisories," United States Department of Homeland Security, 2023, https://www.cisa.gov/russia.

[150] Joint Chiefs of Staff, *Irregular Warfare (IW) Joint Operating Concept (JOC),* (Washington, DC: Joint Chiefs of Staff, 2011), https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v1.pdf

Lastly, external actors seeking to support or enable the development of a pLEO-based satellite communications network for an insurgent movement should seek to establish lines of funding, financier organizations, or other means of ensuring the financial viability of a commercially procured network. As seen in the Russia-Ukraine war, large-scale networking of commercial assets would require potentially thousands of terminals and monthly subscriptions—costs that for the Ukrainians have amounted to over a hundred million U.S. dollars in 2022 alone.[151] Similarly, even in smaller-scale insurgencies or protest movements, the financial burdens of individual terminals may be prohibitive to insurgent users and may be externally supported through activist-provided funds, global fundraising campaigns, or private financiers with shared interests in the movement's goals or cause.[152] By leveraging larger-scale governmental organizations like the United States Agency for International Development (USAID), nonmilitary elements of the U.S. government may themselves become significant contributors to the development and sustainment of global clandestine communications networks.[153] By classifying and providing pLEO-based communications services like SpaceX's Starlink networks as civilian foreign and development assistance resources, USAID has provided upwards of 5,000 Starlink terminals to the Government of Ukraine in support of their defense against the 2022 Russian invasion.[154]

Ultimately, commercial proliferated low earth orbit satellite communications may incur significant financial and logistical obstacles to employment when opposed by an autocratic regime or when supplied to contested or adversary-controlled regions. As external enablers, the U.S. government, military, and intelligence communities must seek

[151] Grace Kay, "Elon Musk's Starlink Satellite Internet Is Reportedly Raising Prices in Ukraine," Business Insider, November 30, 2022, https://www.businessinsider.com/elon-musk-spacex-starlink-internet-raising-prices-in-ukraine-2022-11#.

[152] Vick, "How Activists Get Elon Musk's Starlink to Iran's Protesters."

[153] U.S. Agency for International Development (USAID), "USAID Safeguards Internet Access in Ukraine through Public-Private-Partnership with SpaceX: Press Release," February 10, 2023. https://www.usaid.gov/news-information/press-releases/apr-05-2022-usaid-safeguards-internet-access-ukraine-through-public-private-partnership-spacex.

[154] U.S. Agency for International Development (USAID), "USAID Safeguards Internet Access in Ukraine through Public-Private-Partnership with SpaceX: Press Release."

to mitigate barriers to employment by allowing commercial providers with the legal ability to provide services, leveraging military and intelligence capabilities to deliver requisite technologies, and establishing financial bases to support the potentially cost prohibitive nature of commercial communications solutions. If the U.S. can provide an insurgency with the hardware, software, and financial ability to employ emergent VSAT technologies, insurgencies globally will benefit from the increases in operational capacity and operational security afforded by protected communications channels. The following sections of this thesis will address how insurgent movements may be employed in tandem with emergent operational doctrine from U.S. Special Forces Command and The United States Marine Corps within the Great Power Competition framework.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CLANDESTINE COMMUNICATIONS AND EMERGENT MILITARY DOCTRINE

A. INTRODUCTION AND HISTORICAL VIGNETTE

Competition and kinetic conflict between globally powerful nations is not a novel concept, nor is the employment of insurgent organizations as secretive means of conducting warfare or war-related support activities. Insurgent organizations have historically served as significant force multipliers for combat operations, logistical enablers for forward-deployed basing efforts, and instruments of international influence in contested political domains.[155] By enabling, equipping, and coordinating with U.S. and allied-aligned insurgent organizations, elements of the U.S. military may maximize their own operational capacity and lethality in contested domains like those of the South China Sea, Ukraine, and other regions in the geographic periphery of Great Power Competitors. Emergent military doctrines such as the NATO Comprehensive Defense Manual and the Marine Corps Expeditionary Advanced Base Operations (EABO) Manual both incorporate the employment of indigenous forces as critical enablers for conventional and special military activities. In adversary-controlled or denied environments, the employment of indigenous supporting forces requires the cultivation and operationalization of dark networks and secret organizations comprised of insurgent forces capable of accomplishing the supporting tasks outlined in the aforementioned emergent military doctrine.

The cultivation and activation of insurgent networks in support of large-scale or forward deployed military campaigning is also not a novel concept. The Allied Intelligence Bureau (AIB), activated under General Douglas MacArthur's General Headquarters (GHQ) in July of 1942, consisted of a vast multinational network of intelligence and indigenous operatives that were leveraged to obtain and report information, weaken the enemy by sabotage, and provide assistance to local resistance movements that were aligned

[155] Michael E. Bigelow, "Allied Intelligence Bureau Plays Role in World War II," U.S. Department of the Army, September 1, 2016. https://www.army.mil/article/174480/allied_intelligence_bureau_plays_role_in_world_war_ii.

with Allied force objectives in the Pacific and beyond.[156] Under the Allied Intelligence Bureau, four distinct sub-organizations were developed to conduct four separate supporting efforts to the overall Allied strategy in the South Pacific. Labeled Sections A, B, C, and D, these four organizations within the AIB would be responsible for the conduct of sabotage, intelligence, surveillance, and propaganda, respectively.[157] Despite the unique operational goals of each section of the AIB, they all would, in some manner, employ both clandestine communications and insurgent enablers throughout their secret participation in the Allied efforts to wrest the Pacific from Imperial Japan.[158]

Section A of the AIB, the section responsible for obtaining information on Japanese military activities and conducting acts of sabotage, would be especially reliant on the use of indigenous and insurgent forces. Having been forced out of the Philippines in the early months of 1942, the Allied forces under General MacArthur would rely heavily on an AIB-facilitated network of guerrillas, spies, and saboteurs to maintain a foothold in the critical yet enemy-controlled terrain of the Philippine islands.[159][160] By co-opting support from escaped American prisoners of war and the indigenous Hukbalahap guerrilla fighters, the "United States Forces in the Philippines" (USFIP) initially organized and equipped over six thousand Filipino guerrillas and used them to conduct a myriad of attacks against Imperial Japanese military outposts throughout the Philippines.[161] Using the guerrilla forces of the USFIP, the AIB directed attacks against Japanese military convoys, destroyed critical infrastructure like bridges and telephone lines, burned food storage facilities, and

156 Bigelow, "Allied Intelligence Bureau Plays Role in World War II."

157 Alan Powell, "Beginnings." Essay. In *War by Stealth: Australians and the Allied Intelligence Bureau, 1942–1945*, (Carlton South, Vic, Australia : Melbourne University Press, 1996) 20–31.

158 Powell, War by Stealth: Australians and the Allied Intelligence Bureau, 1942–1945, 20–31.

159 Derek Van Abbe, and Allison Ind, "Allied Intelligence Bureau – Book Review," *Pacific Affairs* 33, no. 4 (1960): 405–6. https://doi.org/10.2307/2753409.

160 William B. Breuer, "Guerrillas, Spies, and Saboteurs," Essay. In *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945*, (New York: St. Martin's Press, 1987), 11–23.

161 Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945*. 11–23.

captured enemy weaponry and ammunition.[162] Additionally, the AIB would leverage the negative sentiment of the Filipino public against the Imperial Japanese presence to create a large-scale, urban network of espionage centered on the Japanese military leadership in Manila. This intelligence-centric network of insurgent collectors would allow the AIB to track Japanese military leadership presence in Manila, report Japanese shipping tonnages via clandestinely transmitted radio codes, and identify top-secret camouflaged underground ammunition storage facilities that would be targeted and destroyed upon the return of American air power to the Philippines.[163] By the middle of 1944, every major island and several smaller islands within the Philippines would be host to elements of what had become a guerrilla organization of upwards of 182,000 guerrillas, 126 clandestine radio stations, and 27 weather reporting facilities.[164]

By leveraging insurgent organizations as instruments of intelligence and sabotage, the U.S. and AIB effectively capitalized on the opportunity provided by clandestine organizations located in denied or enemy-controlled environments. As a blueprint for future operations, the support provided to the Filipino guerrillas operating under the USFIP banner will undoubtedly serve as an example of successful force multiplication through the use of insurgent proxies. By taking lessons learned from critical enabling factors provided by the AIB to Filipino guerrillas and taking a modernized approach to the education, weaponization, and supply of friendly guerrilla organizations, the U.S. military may enhance its lethality in forward-deployed environments. Where the AIB leveraged American submarine flotillas to deliver weapons, ammunition, explosives, and medical supplies to the Filipino guerrillas, future U.S. military operations may employ satellite-connected unmanned aerial vehicles to establish clandestine supply lines to insurgent

[162] Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23.

[163] Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23.

[164] Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23.

organizations in denied environments.[165] Where the AIB established chains of clandestine radio retransmission sites across the South Pacific, future U.S. intelligence operations may host virtual environment-based communications servers to be used by insurgents communicating in denied information environments.[166] Where the AIB employed Filipino guerrilla fighters to set conditions and maintain critical targeting data for the U.S. and Allied Pacific campaign's return and victory over the Imperial Japanese in the Philippines, future insurgent organizations may likewise be critical and deciding factors in the next era of strategic competition.

Ultimately, the employment and successes of insurgent organizations under the Allied Intelligence Bureau in World War 2 serve as case studies in the application of insurgencies as instruments of power projection and international influence. As the U.S. and its allies return to an era of conventional military parity, specifically in the Pacific, insurgent organizations will likely once again become critical operational enablers in denied, degraded, or enemy-controlled environments. The following sections of this thesis will address the roles and responsibilities of the U.S. Marine Corps and U.S. and NATO Special Forces in the cultivation and activation of insurgent networks in support of national and international military strategies for establishing forward deployed military positions and protecting the sovereignty of nations occupying regions in the periphery of Great Power Competitors.

B. EXPEDITIONARY ADVANCED BASE OPERATIONS

Naval Doctrine Publication 1 "Naval Warfare" highlights sea control, power projection, deterrence, maritime security, and sealift materiel support as the enduring functions by which the U.S. Navy pursues national objectives in both peace and war.[167]

---

[165] Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23; Josh Luckenbaugh, "Drones Modified for Medical Supply Drops in Ukraine," National Defense – International News, August 22, 2022. https://www.nationaldefensemagazine.org/articles/2022/8/22/drones-modified-for-medical-supply-drops-in-ukraine; AeroVironment. "Vapor® UAS: Helicopter Drone with Drop Delivery," 2023, https://www.avinc.com/uas/vapor.

[166] Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23.

[167] Department of the Navy. *Naval Warfare*, NDP 1 (Washington, DC: Department of the Navy, 2020), https://cimsec.org/wp-content/uploads/2020/08/NDP1_April2020.pdf

Nested within these enduring functions of naval warfare is the Marine Corps emergent doctrine of Expeditionary Advanced Based Operations (EABO). At its core, EABO is a subset of the naval power projection and sea control enduring functions as amphibious Marine units are explicitly identified as providers of manpower ashore in forward-deployed littoral environments.[168] EABO is a form of expeditionary warfare that involves the employment of mobile, low-signature, persistent, and sustainable naval expeditionary forces from a series of austere and temporary locations ashore within potentially contested maritime areas.[169] Under the EABO construct, U.S. Marine Corps' assets and personnel serve as providers of critical fleet sustainment activities as well as instruments of power projection and sea control within a potentially contested littoral environment.[170]

Absolutely critical to the establishment of these forward-deployed capabilities is the Marine Corps concept of "stand-in" forces. As defined in the Tentative Manual for EABO (TM-EABO), stand-in forces are mobile, low-signature, persistent, and maintainable organizations capable of operating within the enemy's weapon engagement zone (WEZ), supporting host-nation sovereignty, and engaging enemy forces in a close-range battle.[171] While the Tentative Manual for EABO does not explicitly identify indigenous, insurgent, or clandestine organizations as providers or elements of the stand-in forces, this thesis postulates that, like the United States Forces in the Philippines (USFIP) of World War 2, forward-deployed military assets in contested or denied domains will benefit from the employment and integration of local, U.S.-aligned guerrilla organizations. The TM-EABO likewise does not explicitly acknowledge its origins within the operations of the Allied Intelligence Bureau, however, its characteristics and definitions demonstrate the parallels between the future U.S. Marine Corps stand-in forces and those of the USFIP in the Philippines. According to the TM-EABO, stand-in forces would provide the U.S.

168 Department of the Navy. *Naval Warfare*, NDP 1.

169 Department of the Navy. *Tentative Manual for Expeditionary Advanced Base Operations,* TM-EABO (Washington, DC: Department of the Navy, 2021), https://mca-marines.org/wp-content/uploads/TM-EABO-First-Edition-1.pdf

170 Department of the Navy. Tentative Manual for Expeditionary Advanced Base Operations, TM-EABO.

171 Department of the Navy. Tentative Manual for Expeditionary Advanced Base Operations, TM-EABO.

naval element with engagement capabilities throughout the competition continuum including competition below the threshold of violence, partner engagements, and shaping of the theater for future operations.[172] Much like the sabotage-and-espionage networks established by the AIB throughout the South Pacific in World War 2, stand-in forces will ideally become a network of operationally capable insurgent cells operating in support of U.S. military assets and basing efforts in contested geographic terrain.[173]

At their core insurgent organizations are fundamentally compatible with the concept of stand-in forces. As the Marine Corps strives to create stand-in forces that are mobile, persistent, low signature, cost effective, and integral to an operational framework, it will not find a better option than that provided by a friendly-aligned clandestine organization.[174] However, despite the potential for operational compatibility, the U.S. Marine Corps is critically lacking in its ability to cultivate, communicate with, weaponize, and employ irregular or insurgent partner forces. Despite longstanding bilateral training exercises like "Cobra Gold" with Thai Navy, "Kamandag" with the Philippine Marine Corps, and "Iron Fist" with the Japan Ground Self-Defense Force (JGSDF), U.S. Marine Corps activities in the Pacific are largely confined to large-scale, conventional military integration with a focus on live fire exercises, air support integration, and joint maneuvering of ground forces.[175] If the U.S. Marine Corps truly seeks to adapt and employ EABO doctrine in future conflicts, it must likewise adapt its international training regimen to include the participation and employment of non-state irregular forces.

---

[172] Department of the Navy. Tentative Manual for Expeditionary Advanced Base Operations, TM-EABO.

[173] Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23.

[174] Department of the Navy. Tentative Manual for Expeditionary Advanced Base Operations, TM-EABO.

[175] Jonathan Coronel, "Cobra Gold 20: Thai, U.S. Marines Strengthen Bonds for Another Year," Department of the Navy – Headquarters Marine Corps, March 9, 2020, https://www.marines.mil/News/News-Display/Article/2105579/cobra-gold-20-thai-us-marines-strengthen-bonds-for-another-year/;3rd Marine Division, "U.S. Marines Simultaneously Launch Major Bilateral Exercises with Japan, Philippines," of the Navy – Headquarters Marine Corps, September 29, 2022. https://www.marines.mil/News/News-Display/Article/3174227/us-marines-simultaneously-launch-major-bilateral-exercises-with-japan-philippin/; Dzirhan Mahadzir, "U.S. Marines, Japan Self Defense Force Kick Off Iron Fist Exercise in Western Pacific," U.S. Naval Institute, February 20, 2023, https://news.usni.org/2023/02/19/u-s-marines-japan-self-defense-force-kick-off-iron-fist-exercise-in-western-pacific.

In addition to its current rotation of participation in bilateral conventional military exercises, the U.S. Marine Corps must man, train, and equip its forces in preparation for the conduct of large-scale integration with indigenous stand-in forces. Like the clandestine radio retransmission sites established for the AIB's Coastwatcher surveillance program, or the maritime infiltration of weapons and ammunition to guerrilla forces fighting under the USFIP banner, the U.S. Marine Corps must be prepared to establish clandestine infrastructure or provide materiel support to insurgent organizations acting as persistent stand-in forces in contested or denied terrain.[176] The communications technologies identified in this thesis represent two forms of commercially available and cost effective methods of communication for insurgent organizations. As the U.S. Marine Corps seeks to cultivate, weaponize, and activate future insurgent organizations as stand-in forces, it must itself adopt methods of communication that would allow it to communicate beyond the current boundaries of conventional military-to-military cooperation seen in bilateral exercises. As a low-cost, low-hardware option, virtual environment-based communication mediums would allow forward deployed U.S. forces to establish secretive information distribution networks between U.S. personnel, members of an insurgency, and elements of the broader public without incurring significant logistical or financial obligations. Furthermore, for more sensitive or data-intensive applications, the U.S. Marine Corps may procure, distribute, activate, and employ networks of satellite communication nodes to critical elements of an insurgent or partner nation force. As seen in the technology scaling variable provided in the earlier sections of this thesis, a multi-channel network of clandestine communications—both protected and concealed—will hypothetically yield the greatest returns to operational capacity and, in turn, increase the lethality of an irregular partner force. In order to better prepare itself for future peer-level conflict and the potential requirement for irregular warfare activities, the U.S. Marine Corps must adopt commercial communications technologies, incorporate irregular warfare training and activities into its international exercise rotation, and develop its intelligence and special operations assets to serve as critical enablers for future insurgent-conventional pairings.

176 Feldt, Eric A. *The Coastwatchers* (New York, NY: Oxford University Press, 1946); Breuer, *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945.* 11–23.

The Marine Corps is currently unmanned, untrained, and ill-equipped to conduct the large-scale intelligence operations and irregular warfare activities required to overcome conventional military disadvantages in operating environments like the South Pacific. By adapting historical methodologies like those employed by the Allied Intelligence Bureau and by harnessing emergent weapons and communications technologies, the U.S. Marine Corps may effectively and efficiently execute the operational goals established in its plans for Expeditionary Advanced Base Operations. The U.S. Marine Corps may no longer rest on the laurels of its historic victories in the Pacific. With the emergent threat of a peer-level navy in the Chinese People's Liberation Army-Navy, the U.S. Navy and Marine Corps must adopt and employ all available force multiplicative technologies, strategies, and partnerships. Insurgent organizations and the employment of guerrilla movements will be critical enablers for future military operations in the contested or denied terrains of the next major conflict.

C. NATO'S COMPREHENSIVE DEFENSE STRATEGY

In addition to solely U.S. emergent doctrine concerning the cultivation and employment of indigenous and potentially insurgent forces, irregular warfare techniques are also present in emergent allied doctrines like NATO's Comprehensive Defense Strategy. Under the Comprehensive Defense structure, nations located on the periphery or in the geographic direction of an asymmetric adversary's trajectory may seek to establish a whole-of-society defense that is consistent with international law and accepted norms.[177] Within this construct, a participating nation develops a layered defensive force comprised of its national military, a secondary "Home Guard" of reservist volunteers, and a tertiary clandestine "Asymmetric Defense Component" built from a mobilized civilian population.[178] Modeled after an operationalized insurgency, the Asymmetric Defense Component (ADC) of a nation's comprehensive defense structure would retain a compartmentalized, operational cell-based structure that would allow the irregular force to

[177] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* (Brussels, Belgium: NATO Special Operations Headquarters, 2021). https://portal.nshq.nato.int/Library/DownloadFile/25e65162-e2f3-1d38-dd99-b7574e421d3f

[178] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 43.

be divided into functional units, limit the targeting vulnerabilities associated with interconnected organizations, all while allowing the insurgent network to be efficiently directed by the overarching government or military organization.[179] As deterrent and resistant forces, the Home Guard and Asymmetric Defense Component are critical pieces of the Comprehensive Defense Strategy as they seek to presuppose the presence of a large-scale, weaponized civilian resistance force capable of intelligence, sabotage, and limited conventional military operations against potential incursions by an asymmetric aggressor.[180] Foundational to the effective employment of a Home Guard or Asymmetric Defense Component is the existence and use of a resilient and potentially secretive communications network. Without the ability to communicate and coordinate between all three militarized elements of a Comprehensive Defense posture, any national effort to employ the secondary and tertiary layers of the defense will be at best inefficient or at worst counterproductive.

The Comprehensive Defense Handbook stipulates that organizations within the Comprehensive Defense structure must employ communications security measures in a balanced manner to ensure operational capacity and organizational security.[181] Furthermore, the Comprehensive Defense Handbook assumes that all electronic communications will be monitored by adversarial intelligence in times of peace, crisis, and war, recommending that its insurgent advisees seek to employ numerous technical and non-technical means of communications to mitigate the risk of compromise.[182] This thesis recommends that virtual environment-based and proliferated low Earth orbit satellite communications may be leveraged in support of elements of the Comprehensive Defense Strategy.

Designed to mimic an operationalized insurgent organization, an Asymmetric Defense Component leverages the support of a nation's public population to generate

[179] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 44–46.

[180] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 43.

[181] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 44.

[182] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 45.

operational capacity in the form of distributed operational cells. Because the Asymmetric Defense Component maintains minimal military protection or conventional military infrastructure, it relies on secrecy to maintain the security of its members. However, despite the lack of conventional military equipment or presence, the Asymmetric Defense Component is still considered an official, government-led organization.[183] Because the Asymmetric Defense Component requires the large-scale distribution of insurgent material and guidance without the formal allocation of communications infrastructure, this thesis recommends that virtual environment-based communications serve as critical mediums for the storage and transmission of defense-oriented communications for an Asymmetric Defense Component. Because virtual environments are globally popular and accessible in the form of online entertainment, they provide almost universal access to communications as long as an insurgent communicator has an internet connection and an internet-connected device like a cell phone or gaming console. Additionally, this thesis recommends that insurgent communicators seeking to employ virtual environments as mediums for secret communications use, innovate, and adapt methods like those outlined in the "Virtual Clandestine Tradecraft" section of this thesis to enhance the concealment and protection of their transmitted data.

Compared to the insurgency-oriented Asymmetric Defense Component, the Home Guard element of a Comprehensive Defense is a more robust, funded, professional reserve defense force. As a secondary to the national military, the Home Guard is a part-time professional force of trained, on-call citizens.[184] Because the Home Guard maintains formal military sustainment and funding, it is a prime candidate for commercial communications technologies such as pLEO-based satellite communications. By including portable and resilient pLEO-based satellite communications in the suite of issued equipment to a Home Guard organization, a nation seeking to enhance its defense posture and the effectiveness of its layered military may do so quickly, efficiently, and at a reasonable cost. Additionally, by employing commercial communications technologies, a

[183] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 44.

[184] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 37.

nation participating in the Comprehensive Defense structure would streamline its ability to receive external aid and material support as external enablers within the NATO alliance would simply be able to purchase, activate, and sustain commercial communications solutions for their Home Guard.

The Comprehensive Defense Strategy seeks to enhance the defensive and deterrent posture of asymmetrically disadvantaged nations against the potential aggressions of a Great Power Competitor or regional adversary. At its core, the Comprehensive Defense Strategy seeks to employ the non-governmental 98% of a nation's population to directly contribute to its safety, security, and right to self-determination.[185] Within the Comprehensive Defense Strategy, commercially available clandestine communications may serve as defining factors in a nation's ability to effectively leverage a whole-of-society approach to defense. While operationally and logistically unlikely, a nation that fully achieves the 98% participation envisioned in the Comprehensive Defense Strategy would experience a military capacity much greater than that of an un-mobilized and disconnected population. Adhering to the notional baseline parameters of $k = 0.1$, $a = 0.2$,. and $C_j = 1$ from the "Updated Modeling" section of this thesis, Figure 21 demonstrates the hypothetical positive impact that an insurgent defense force would achieve if it were able to maintain a populational 98% access to concealed and protected forms of communication. The observed difference between the original operational capacity with no technology scaling and the hypothesized operational capacity with 98% access to concealed or protected communications is a hundredfold increase in the operational capacity of the insurgent cell or collective organization. This thesis asserts that commercial clandestine communications are a critical enabler for modern insurgent organizations and are thus also critical to any nation's effort to establish a Comprehensive Defense posture.

[185] NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* 15.

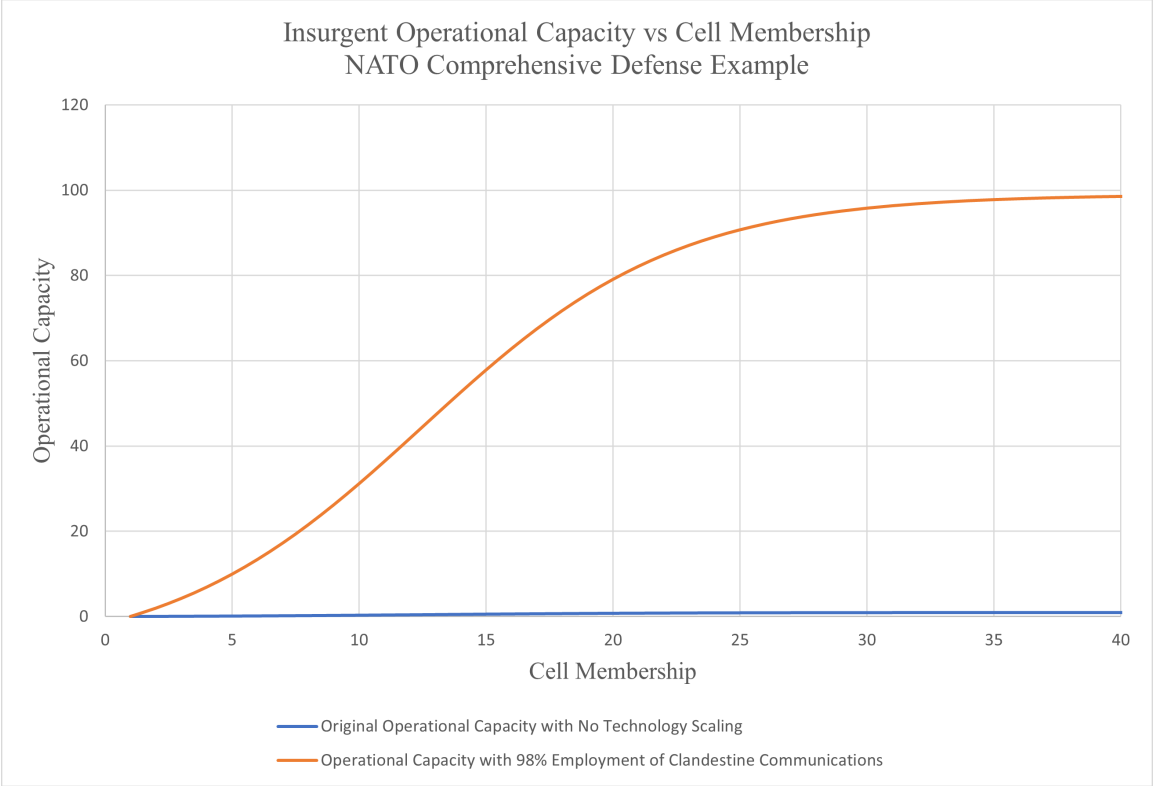

Figure 21. Operational Capacity Gains for a 98% Adoption of Clandestine Communications Technologies vs. No Adoption/Employment. Application of Insurgent Modeling to an Asymmetric Defense Component Organization.

VIII. CONCLUSION

As instruments of international power and operational capacity, insurgent organizations and guerrilla forces may serve as critical enablers for future operations. This thesis asserts that advances in commercial communications and entertainment technologies may be leveraged to increase the operational capacity of an insurgent organization in its competition against a regional adversary, the military forces of an aggressive neighbor state, or within the construct of the Great Power Competition. The emergent peer-level threat of the Chinese People's Liberation Army and Navy has highlighted the need for force multiplicative strategies and partnerships. Key among these strategic and doctrinal opportunities is the use of insurgent organizations and emergent technologies to generate or multiply relative combat power, intelligence gathering capabilities, and resilient communications networks.

Specifically, this thesis posits that the proliferation of video game-based virtual environments and proliferated low earth orbit satellite communications may serve as ideal mediums for concealed or protected insurgent data transmission. As the U.S. and its allies seek to enable insurgent organizations or guerrilla movements on the periphery or within the borders of adversary nations, it may employ these emergent technologies to increase the security and coordination of its insurgent partners. The Technology Scaling Variable equation set provided in this thesis is a baseline proposal for the mapping and optimization of material support given to clandestine organizations. As planners seek to allocate resources to direct and indirect lines of support to non-state forces like U.S.-aligned insurgent organizations, the mathematical models provided by McCormick and Owen's "Security and Coordination in a Clandestine Organization" are useful tools for the visualization and evaluation of available potential operational capacity. Furthermore, by employing additional models to evaluate the specific impacts and trade-offs between supporting technologies, planners may optimize the use of their resources to generate the highest amount of operational capacity in support of their strategic or operational goals.

The need for irregular warfare activities like insurgent-conventional military pairings is not a novel concept and is foundational to emergent military doctrine like that

seen in NATO's Comprehensive Defense strategies or the U.S. Marine Corps Expeditionary Advanced Base Operations. If the U.S. and its allies truly seek to maximize their deterrent posture and power projection capabilities, insurgent organizations must be employed to maximize the impact borne of their investments in strategically important regions and operationally capable populations. Insurgent organizations have historically served as critical providers of intelligence and strategic operational capacity in denied environments like those seen in the 1940s Imperial Japan-controlled Philippines. As the U.S. faces yet another peer-level threat in the Pacific, it must once again adopt irregular warfare doctrine within its conventional planning and cultivate operationally capable insurgent partners abroad.

LIST OF REFERENCES

12th Chinese National People's Congress, National Intelligence Law of the People's Republic (2017). https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

3rd Marine Division. "U.S. Marines Simultaneously Launch Major Bilateral Exercises with Japan, Philippines." Department of the Navy – Headquarters Marine Corps, September 29, 2022. https://www.marines.mil/News/News-Display/Article/3174227/us-marines-simultaneously-launch-major-bilateral-exercises-with-japan-philippin/.

AeroVironment. "Vapor® UAS: Helicopter Drone with Drop Delivery." 2023. https://www.avinc.com/uas/vapor.

Alcorn, Brian, Garrett Boyce, Brian Walsh, Tom Haluska, Evan Kolodziejczak, Kent Johnson, Nick Pugh, Biran Kerg, Nolan Sheahan, and Philip Burtt-Henderson. *EP EMCON SOP: A Guide to Reduce Technical Signature,* Virginia Beach, VA: Marine Corps Intelligence Schools (MCIS) Intelligence Training Enhancement Program (ITEP), 2020, https://brushbeater.org/wp-content/uploads/2021/03/EP-EMCON-SOP.pdf

Allworth, James. "Two Months Later: Internet Use in Iran during the Mahsa Amini Protests." Cloudflare Inc, December 12, 2022. https://blog.cloudflare.com/two-months-later-internet-use-in-iran-during-the-mahsa-amini-protests/.

Amazon. "Here's Your First Look at Project Kuiper's Low-Cost Customer Terminals," March 14, 2023. https://www.aboutamazon.com/news/innovation-at-amazon/heres-your-first-look-at-project-kuipers-low-cost-customer-terminals.

Bell, J. Bowyer. "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem." *International Journal of Intelligence and Counterintelligence* 3, no. 1 (1989): 15–43. https://doi.org/10.1080/08850608908435089.

Biddle, Sam, and Murtaza Hussain. "Hacked Documents: How Iran Can Track and Control Protesters' Phones." The Intercept. October 28, 2022. https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/.

Bigelow, Michael E. "Allied Intelligence Bureau Plays Role in World War II." U.S. Department of the Army, September 1, 2016. https://www.army.mil/article/174480/allied_intelligence_bureau_plays_role_in_world_war_ii.

Breuer, William B. "Guerrillas, Spies, and Saboteurs." Essay. In *Retaking the Philippines: America's Return to Corregidor and Bataan, October 1944-March 1945*, 11–23. New York: St. Martin's Press, 1987.

Canadian Security Intelligence Service. "China's Intelligence Law and the Country's Future Intelligence Competitions." Government of Canada, May 17, 2018. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html.

Central Intelligence Agency Museum. "Artifacts – Dead Drop Spike." Central Intelligence Agency. Accessed January 10, 2023. https://www.cia.gov/legacy/museum/artifact/dead-drop-spike/.

Chan, Conrad, Anthony Dao, Justin Hou, Tony Jin, and Calvin Tuong. "Free Speech versus Maintaining Social Cohesion – China's Great Firewall," Stanford Institute of Computer Science, 2011. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital Image Steganography: Survey and Analysis of Current Methods." *Signal Processing* 90, no. 3 (September 6, 2010): 727–52. https://doi.org/10.1016/j.sigpro.2009.08.010.

Cho, Kiho, Hwan Sik Yun, and Nam Soo Kim. "Robust Data Hiding for MCLT Based Acoustic Data Transmission." *IEEE Signal Processing Letters* 17, no. 7 (2010): 679–82. https://doi.org/10.1109/LSP.2010.2051174.

Cho, Kiho, Jae Choi, and Nam Soo Kim. "An Acoustic Data Transmission System Based on Audio Data Hiding: Method and Performance Evaluation." *EURASIP Journal on Audio, Speech, and Music Processing* 2015, no. 1 (2015): 1–. https://doi.org/10.1186/s13636-015-0053-x.

Cook, Aaron. "How to Make Letters and Numbers in Minecraft." Brit & Company Guides and Tutorials, September 20, 2021. https://guides.brit.co/guides/make-letters-and-numbers-in-minecraft.

Coronel, Jonathan. "Cobra Gold 20: Thai, U.S. Marines Strengthen Bonds for Another Year." Department of the Navy – Headquarters Marine Corps, March 9, 2020. https://www.marines.mil/News/News-Display/Article/2105579/cobra-gold-20-thai-us-marines-strengthen-bonds-for-another-year/.

Cybersecurity and Infrastructure Security Agency (CISA). "Russia Cyber Threat Overview and Advisories." United States Department of Homeland Security, 2023. https://www.cisa.gov/russia.

Daehnick, Chris, Ben Maritz, Bill Wiseman, and Isabelle Klinghoffer. "Large LEO Satellite Constellations: Will It Be Different This Time?" McKinsey & Company. Accessed May 1, 2023. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time.

Dans, Enrique. "How Starlink Is about to Disrupt the Telecommunications Sector." Forbes Magazine, February 23, 2021. https://www.forbes.com/sites/enriquedans/2021/02/23/how-starlink-is-about-to-disrupt-the-telecommunications-sector/?sh=70ea9f46659a.

Dean, Grace. "Meta Has Pumped $36 Billion into Its Metaverse and VR Businesses since 2019." Business Insider. October 29, 2022. https://www.businessinsider.com/charts-meta-metaverse-spending-losses-reality-labs-vr-mark-zuckerberg-2022-10.

Department of the Navy. *Naval Warfare*, NDP 1 (Washington, DC: Department of the Navy, 2020), https://cimsec.org/wp-content/uploads/2020/08/NDP1_April2020.pdf

Department of the Navy. *Tentative Manual for Expeditionary Advanced Base Operations,* TM-EABO (Washington, DC: Department of the Navy, 2021), https://mca-marines.org/wp-content/uploads/TM-EABO-First-Edition-1.pdf

Duffy, Kate. "Starlink Has Hit More than 1 Million Users despite a Drop in Download Speeds. Here's What You Need to Know about the Service." Business Insider. December 20, 2022. https://www.businessinsider.com/spacex-starlink-internet-service-elon-musk-all-you-need-know-2021-2.

Edelman, Eric and Gary Roughead. *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* Washington, DC: National Defense Strategy Commission, 2018. https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

Eichelberger, Manuel, Simon Tanner, Gabriel Voirol, and Roger Wattenhofer. "Imperceptible Audio Communication." In *ICASSP 2019 – 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 680–84. Zurich: IEEE, 2019. https://doi.org/10.1109/ICASSP.2019.8682262.

Elbert, Bruce R. *Introduction to Satellite Communication. 3rd ed.* 7–12. Boston: Artech House, 2008.

Elburn, Darcy. "Low Earth Orbit (LEO) Economy." NASA. February 2022. https://www.nasa.gov/leo-economy/faqs.

Entertainment Software Ratings Board. "ESRB Ratings Guide." December 16, 2022. https://www.esrb.org/.

Epifanova, Alena. "Deciphering Russia's 'Sovereign Internet Law." German Council on Foreign Relations, January 16, 2020. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

Feldt, Eric A. *The Coastwatchers*. New York, NY: Oxford University Press, 1946.

Freeman, Michael, Hy S. Rothstein, and Greg Wilson. "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines." Essay. In *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, 15–20. Monterey, CA: Naval Postgraduate School, Department of Defense Analysis, 2011.

Frigg, Roman, Giorgio Corbellini, Stefan Mangold, and Thomas R. Gross. "Acoustic Data Transmission to Collaborating Smartphones – An Experimental Study." In *2014 11th Annual Conference on Wireless On-Demand Network Systems and Services (WONS)*. 17–24. Zurich: IEEE, 2014. https://doi.org/10.1109/WONS.2014.6814717.

Gutierrez, Luis, and Dan Hammill. "Book and Quill – Minecraft Wiki Guide." IGN Entertainment Incorporated, March 18, 2013. https://www.ign.com/wikis/minecraft/Book_and_Quill.

Hallex, Matthew, and Travis Cottom. "Proliferated Commercial Satellite Constellations – Implications for National Security." *Joint Forces Quarterly*, (April 2020): 20–30. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_20-29_Hallex-Cottom.pdf?ver=2020-03-31-130614-940.

Harris, Mark. "Starlink Signals Can Be Reverse-Engineered to Work like GPS-Whether Spacex Likes It or Not." MIT Technology Review, October 24, 2022. https://www.technologyreview.com/2022/10/21/1062001/spacex-starlink-signals-reverse-engineered-gps/.

Hatmaker, Taylor. "Sony Suspends PlayStation Store and Console Sales in Russia." TechCrunch. Verizon Media Group, March 10, 2022. https://techcrunch.com/2022/03/09/sony-russia-ps5-gran-turismo-suspended/.

Hauw, Olivier. "The Evolution of Commercial Satellite Communications." Airbus – Secure Communications. 2023. https://securecommunications.airbus.com/en/meet-the-experts/evolution-commercial-satellite-communications.

Haynes, Cara. "Starlink Internet Review 2023: Plans, Pricing, and Speeds." Satellite Internet Inc, March 20, 2023. https://www.satelliteinternet.com/providers/starlink/#:~:text=Starlink%20costs%20%24110%20per%20month,%242%2C500%20one%2Dtime%20equipment%20fee.

Humphreys, Todd E, Peter A. Iannucci, Zacharias Komodromos, and Andrew M. Graff, "Signal Structure of the Starlink Ku-Band Downlink." The University of Texas at Austin, 2022. https://doi.org/10.48550/arxiv.2210.11578.

Ippolito, Louis J. "Introduction to Satellite Communications." In Satellite Communications Systems Engineering, 2nd ed., 33–34. United States: Wiley, 2017. https://doi.org/10.1002/9781119259411.ch1.

Iyengar, Rishi. "Why Ukraine Is Stuck with Elon (for Now)." Foreign Policy, November 22, 2022. https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-russia-war/.

Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02. Washington, DC: Joint Chiefs of Staff, 2010. https://dcsg9.army.mil/assets/docs/dod-terms.pdf.

Joint Chiefs of Staff, *Irregular Warfare (IW) Joint Operating Concept (JOC),* Washington, DC: Joint Chiefs of Staff, 2011. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v1.pdf

Harry W. Jones, "The Recent Large Reduction in Space Launch Cost." In *48th International Conference on Environmental Systems,* 1–10. Albuquerque: ICES, 2018. https://ttu-ir.tdl.org/bitstream/handle/2346/74082/ICES_2018_81.pdf.

Kaki, Leela Prasad, Chandra Sekhar Musinana, and Somasundara Rao Muppidi. "Message passing using cryptography and steganography." *i-manager's Journal on Cloud Computing* 8 (January 2021): 8–15. https://libproxy.nps.edu/login?url=https://www.proquest.com/scholarly-journals/message-passing-using-cryptography-steganography/docview/2621196897/se-2.

Katz, Miranda. "The Personal Information Protection Law: China's Version of the GDPR?" Columbia Journal of Transnational Law, February 15, 2022. https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.

Kay, Grace. "Elon Musk's Starlink Satellite Internet Is Reportedly Raising Prices in Ukraine." Business Insider, November 30, 2022. https://www.businessinsider.com/elon-musk-spacex-starlink-internet-raising-prices-in-ukraine-2022-11#.

Korovayny, Serhii. "Activists Sent Photos of an Electronics Store Russian Forces Used in Kherson to the Ukrainian Military, Which Destroyed the Store." The Wall Street Journal, December 15, 2022. https://www.wsj.com/articles/ukraines-secret-weapon-is-ordinary-people-spying-on-russian-forces-11671012147?st=3sak0b2r2zwv95r.

Krishna, Swapna. "The Best Games Have the Smartest Learning Curves." Wired – Conde Nast, May 4, 2022. https://www.wired.com/story/video-games-learning-curves/.

Laub, Zachary. "International Sanctions on Iran." Council on Foreign Relations, July 15, 2015. https://www.cfr.org/backgrounder/international-sanctions-iran.

Lazic, N., and P. Aarabi. "Communication Over an Acoustic Channel Using Data Hiding Techniques." *IEEE Transactions on Multimedia* 8, no. 5 (2006): 918–24. https://doi.org/10.1109/TMM.2006.879880.

Lee, Rob. "Photo of a Ukrainian UAV Used to Drop 82mm Mortar Rounds Equipped with a Starlink Terminal Captured by Russian Forces." Twitter post, March 25, 2023. https://twitter.com/RALee85/status/1639749679079383042/photo/1

Luckenbaugh, Josh. "Drones Modified for Medical Supply Drops in Ukraine." National Defense – International News, August 22, 2022. https://www.nationaldefensemagazine.org/articles/2022/8/22/drones-modified-for-medical-supply-drops-in-ukraine

Luxmoore, Matthew. "Ukraine's Secret Weapon Is Ordinary People Spying on Russian Forces." The Wall Street Journal, December 15, 2022. https://www.wsj.com/articles/ukraines-secret-weapon-is-ordinary-people-spying-on-russian-forces-11671012147?st=3sak0b2r2zwv95r.

Lynk Global Incorporated. "Lynk Proves Direct Two-Way Satellite-to-Mobile-Phone Connectivity." September 29, 2021. https://lynk.world/lynk-proves-direct-two-way-satellite-to-mobile-phone-connectivity.

Lynk Global Incorporated. "Lynk Shannon Satellite Narrative Statement." Federal Communications Commission. 2020. https://apps.fcc.gov/els/GetAtt.html?id=266627&x=.

Mahadzir, Dzirhan. "U.S. Marines, Japan Self Defense Force Kick Off Iron Fist Exercise in Western Pacific." U.S. Naval Institute, February 20, 2023. https://news.usni.org/2023/02/19/u-s-marines-japan-self-defense-force-kick-off-iron-fist-exercise-in-western-pacific.

MATLAB & Simulink. "What Is OFDM?" 2022. https://www.mathworks.com/discovery/ofdm.html.

McCormick, Gordon H, and Frank Giordano. "Things Come Together: Symbolic Violence and Guerrilla Mobilisation." *Third World Quarterly* 28, no. 2 (2007): 295–320. https://doi.org/10.1080/01436590601153705.

McCormick, Gordon H., and G. Owen. "Security and Coordination in a Clandestine Organization." *Mathematical and Computer Modelling 31*, no. 6–7 (May 2000): 175–92. https://doi.org/10.1016/s0895-7177(00)00050-9.

McCormick, Gordon H. "The Shining Path and Peruvian Terrorism." *Journal of Strategic Studies* 10, no. 4 (1987): 114. https://doi.org/10.1080/01402398708437317.

Microsoft Corporation. "SEC Correspondence: Sale of Microsoft Products." U.S. Security and Exchanges Commission, December 27, 2011. https://www.sec.gov/Archives/edgar/data/789019/000119312512007906/filename1.htm#:~:text=Although%20we%20do%20not%20currently,September%202011%20and%20September%202013.

Minecraft Wiki. "Minecraft Multiplayer Gameplay." Fandom Incorporated. Accessed March 9, 2023. https://minecraft.fandom.com/wiki/Multiplayer.

Molnar, Andrew R. "Definitions of Clandestine and Covert Behavior." Essay. In *Human Factors Considerations of Undergrounds in Insurgencies*, 101–2. Washington, DC: U.S. Army Headquarters, 1966.

National Aeronautics and Space Administration (NASA). "NASA Space Science Data Coordinated Archive – Starlink 1010." 2022. https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2019-074D

National Park Service. "Information about Minecraft." U.S. Department of the Interior, June 19, 2022. https://www.nps.gov/kewe/learn/education/information-about-minecraft.htm.

NATO Special Operations Headquarters, *Comprehensive Defense Handbook Volume 1.* Brussels, Belgium: NATO Special Operations Headquarters, 2021. https://portal.nshq.nato.int/Library/DownloadFile/25e65162-e2f3-1d38-dd99-b7574e421d3f

Nettina, Adam. "How John Steinbeck Inspired the Resistance in WWII." HistoryNet. November 17, 2021. https://www.historynet.com/how-john-steinbeck-inspired-the-resistance-in-wwii/.

Office of Foreign Assets Control (OFAC). Iranian Transactions Regulations: Guidance on the Provision of Internet Connectivity Services (2003)." https://ofac.treasury.gov/media/7896/download?inline.

Office of Foreign Assets Control (OFAC). "Iranian Transactions Regulations: Interpretive Guidance and Statement of Licensing Policy on Internet Freedom in Iran (2012)." https://ofac.treasury.gov/media/7891/download?inline

Petraeus, David H., James F. Amos, and John A. Nagl. "Targeting." Essay. In *The U.S. Army/Marine Corps Counterinsurgency Field Manual U.S. Army Field Manual No. 3–24: Marine Corps Warfighting Publication No. 3–33.5*, 191–96. Chicago, IL: University of Chicago Press, 2007.

Petty, Jared, and John Ryan. "Communicating Using the Phone – GTA 5 Wiki Guide." IGN Entertainment Incorporated, November 3, 2016. https://www.ign.com/wikis/gta-5/Communicating_using_the_Phone.

Pifer, Steven. "The Russia-Ukraine War and Its Ramifications for Russia." Brookings Institute, February 24, 2023. https://www.brookings.edu/articles/the-russia-ukraine-war-and-its-ramifications-for-russia/.

Powell, Alan. “Beginnings.” Essay. In *War by Stealth: Australians and the Allied Intelligence Bureau, 1942–1945*, 20–31. Carlton South, Vic, Australia : Melbourne University Press, 1996.

Ren, Jingjing, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, and Hamed Haddadi. “Information Exposure from Consumer IOT Devices: Proceedings of the Internet Measurement Conference.” In *2019 Internet Measurement Conference,* 267–79. Amsterdam: ACM, 2019. https://dl.acm.org/doi/10.1145/3355369.3355577.

Reuters. “Elon Musk Says around 100 Starlinks Now Active in Iran.” December 27, 2022. https://www.reuters.com/technology/elon-musk-says-around-100-starlinks-now-active-iran-2022-12-26/.

Reuters. “Events in Iran since Mahsa Amini’s Arrest and Death in Custody.” December 12, 2022. https://www.reuters.com/world/middle-east/events-iran-since-mahsa-aminis-arrest-death-custody-2022-10-05/.

Reuters. “Starlink Helped Restore Energy, Communications Infrastructure in Parts of Ukraine – Official.” Thomson Reuters, October 12, 2022. https://www.reuters.com/world/starlink-helped-restore-energy-communications-infrastructure-parts-ukraine-2022-10-12/.

Rippeon, Ryan. “Clandestine Message Passing in Virtual Environments.” Master’s thesis, Naval Postgraduate School, 2009. https://calhoun.nps.edu/handle/10945/3967

Rutherford, Mark. “The Issues with Jamming Drone Frequencies.” D-Fend Solutions, February 12, 2023. https://d-fendsolutions.com/blog/issues-with-jamming-drone-frequencies/#:~:text=Frequency%20Bands,-Commercial%20drones%20operate&text=Most%20of%20the%20more%20expensive,some%20as%20far%20as%2012km.

Sapranov, Walter. “Telecoms, Media, and Internet Report: Russia.” ICLG.com. International Comparative Legal Guides, Accessed: May 1, 2023. https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/Russia

Schroeder, Ralph. “Defining Virtual Worlds and Virtual Environments.” *Journal For Virtual Worlds Research* 1, no. 1 (July 2008). https://doi.org/10.4101/jvwr.v1i1.294.

Shalf, John. “The Future of Computing Beyond Moore’s Law.” *The Royal Society Publishing – Mathematical, Physical And Engineering Sciences* 378, no. 2166 (January 2020). http://doi.org/10.1098/rsta.2019.0061.

Singer, Dan, and Enrico D'Angelo. "The Netflix of Gaming? Why Subscription Video-Game Services Face an Uphill Battle." McKinsey & Company. July 8, 2020. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-netflix-of-gaming-why-subscription-video-game-services-face-an-uphill-battle.

Smith, Nat. "How Warzone 2 Proximity Chat Works." PCGamesN – Network-N, November 21, 2022. https://www.pcgamesn.com/call-of-duty-warzone-2/proximity-chat.

Starlink. "Starlink Residential User Guide." SpaceX, 2022. https://www.starlinkinternet.info/en-us/GettingStartedWithStarlink.

Starlink, "Starlink WiFi Router Specifications." SpaceX. Accessed January 8, 2023. https://www.starlink.com/specifications.

Statista, "Number of Active Satellites from 1957 to 2021." 2022. https://www.statista.com/statistics/897719/number-of-active-satellites-by-year/#:~:text=This%20statistic%20illustrates%20the%20number,3%2C291%20active%20satellites%20in%202020.

Statista, "Number of Smartphone Subscriptions Worldwide from 2016 to 2021." 2022. https://www.statista.com/outlook/dmo/digital-media/video-games/online-games/worldwide#analyst-opinion.

Statista Research Department, "Total Population of Ukraine as of February 1, 2022, By Region," March 6, 2023. https://www.statista.com/statistics/1295222/ukraine-population-by-region/.

The Economist. "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare. The Economist – Briefing: A Murmuration of Starlinks." January 5, 2023. https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

Tse-Tung, Mao. "What Is Guerrilla Warfare?" Essay. In *On Guerrilla Warfare – Translated and with an Introduction by Brigadier General Samuel B. Smith USMC (Ret.)*, 43–51. New York, NY: Praeger, 1961.

U.S. Agency for International Development (USAID). "USAID Safeguards Internet Access in Ukraine through Public-Private-Partnership with SpaceX: Press Release." February 10, 2023. https://www.usaid.gov/news-information/press-releases/apr-05-2022-usaid-safeguards-internet-access-ukraine-through-public-private-partnership-spacex.

U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States*. Washington, DC: 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Van Abbe, Derek, and Allison Ind. “Allied Intelligence Bureau – Book Review.” *Pacific Affairs* 33, no. 4 (1960): 405–6. https://doi.org/10.2307/2753409.

Vick, Karl. “How Activists Get Elon Musk’s Starlink to Iran’s Protesters.” Time – World News – Iran. January 25, 2023. https://time.com/6249365/iran-elon-musk-starlink-protests/.

Wall, Mike. “1,300 SpaceX Starlink Terminals with Ukraine’s Military Went Offline Due to Funding Shortfall: Report.” Space.com. November 8, 2022. https://www.space.com/ukraine-spacex-starlink-terminals-offline-funding-shortfall.

Wall Street Journal Editorial Board. “Opinion | Elon Musk Has a Better Iran Idea.” The Wall Street Journal, September 25, 2022. https://www.wsj.com/articles/elon-musk-has-a-better-iran-idea-starlink-protests-mahsa-amini-11663883982.

Wilson, Greg, and Hy Rothstein. “The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines .” Essay. In *Gangs and Guerrillas – Ideas from Counterinsurgency and Counterterrorism*, edited by Michael Freeman, 15–21. Monterey, CA: Naval Postgraduate School, 20111.

Yeremenko, Oleksandra, Oleksandr Lemeshko, M. Persikov, and V. Lemeshko. ““ICT Disruptive Technologies: Starlink in Ukraine Case,” Kharkiv National University of Radio Electronics, 2022, https://openarchive.nure.ua/server/api/core/bitstreams/9e6ec44a-5b78-4e5d-b98e-d53bb94a6d86/content

Yonekura, Emmi, Brian Dolan, Moon Kim, Krista Romita Grocholski, Raza Khan, and Yool Kim. *Commercial Space Capabilities and Market Overview: The Relationship Between Commercial Space Developments and the U.S. Department of Defense*. RR 578–2 . Santa Monica, CA: RAND, 2022. https://www.rand.org/pubs/research_reports/RRA578-2.html.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California