



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**THE CYBER OFFENSE-DEFENSE BALANCE
REVISITED: THE VARIABLES TIPPING THE
BALANCE**

by

Daniel P. Gipper

June 2020

Thesis Advisor:
Second Reader:

Ryan Maness
Scott E. Jasper

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2020	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE THE CYBER OFFENSE-DEFENSE BALANCE REVISITED: THE VARIABLES TIPPING THE BALANCE			5. FUNDING NUMBERS	
6. AUTHOR(S) Daniel P. Gipper				
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) Thus far, the efforts to analyze the cyber offense-defense balance have proven unconvincing, driving the need to revisit the discussion. The problems stem from the baseline theory, as the literature suffers from excessive nuance and provides unproductive methods to assess the offense-defense balance. To address these problems, the purpose of this thesis is threefold: (1) offer a robust definition of the offense-defense theory, (2) develop variables that tip the offense-defense balance, creating an analytical framework in the process, and (3) employ that framework to assess the cyber offense-defense balance. This thesis develops a definition of the offense-defense theory that cuts the unnecessary complexity and focuses solely on the offense-defense balance. It is the balance that predicts a heightened chance of conflict, as it identifies a condition that incites aggressive behavior when actors perceive the dominance of offensive strategies. The current literature muddles this clean connection. Next, the theoretical analysis herein reveals six variables that tip the balance: the information advantage, decisive effects, exposure, insulation, criticality, and resilience. This thesis then demonstrates the explanatory power of these six variables by providing case studies in air warfare and irregular warfare. Finally, these variables facilitate an analysis of the cyber offense-defense balance, suggesting that actors perceive offensive strategies to be dominant in cyber conflict.				
14. SUBJECT TERMS offense, defense, balance, cyber, cyber warfare, cyber conflict, air warfare, irregular warfare			15. NUMBER OF PAGES 237	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**THE CYBER OFFENSE-DEFENSE BALANCE REVISITED: THE VARIABLES
TIPPING THE BALANCE**

Daniel P. Gipper
Major, United States Air Force
BS, Michigan State University, 2006
M, Embry-Riddle Aeronautical University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
June 2020**

Approved by: Ryan Maness
Advisor

Scott E. Jasper
Second Reader

Kalev I. Sepp
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Thus far, the efforts to analyze the cyber offense-defense balance have proven unconvincing, driving the need to revisit the discussion. The problems stem from the baseline theory, as the literature suffers from excessive nuance and provides unproductive methods to assess the offense-defense balance. To address these problems, the purpose of this thesis is threefold: (1) offer a robust definition of the offense-defense theory, (2) develop variables that tip the offense-defense balance, creating an analytical framework in the process, and (3) employ that framework to assess the cyber offense-defense balance.

This thesis develops a definition of the offense-defense theory that cuts the unnecessary complexity and focuses solely on the offense-defense balance. It is the balance that predicts a heightened chance of conflict, as it identifies a condition that incites aggressive behavior when actors perceive the dominance of offensive strategies. The current literature muddles this clean connection. Next, the theoretical analysis herein reveals six variables that tip the balance: the information advantage, decisive effects, exposure, insulation, criticality, and resilience. This thesis then demonstrates the explanatory power of these six variables by providing case studies in air warfare and irregular warfare. Finally, these variables facilitate an analysis of the cyber offense-defense balance, suggesting that actors perceive offensive strategies to be dominant in cyber conflict.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PURPOSE.....	4
B.	LITERATURE REVIEW	6
1.	The Problems in Offense-Defense Theory	7
2.	Attempts to Analyze the Cyber Offense-Defense Balance	10
C.	METHODOLOGY	11
D.	MAJOR FINDINGS AND ORGANIZATION	14
 II.	 OFFENSE-DEFENSE THEORY DEFINED	 17
A.	THE ROOTS OF OFFENSE-DEFENSE THEORY	19
1.	Realism.....	19
2.	Offensive and Defensive Realism.....	20
3.	The Originators of Offense-Defense Theory	22
B.	DEFINING THE THEORY.....	24
1.	Conflict, War, Offense, and Defense	24
2.	Causes of War: Origin or Outbreak	28
3.	Preventive Wars and Pre-Emptive Strikes.....	28
4.	Offense-Defense Theory: Definition and Balance.....	30
C.	THE CRITIQUES OF OFFENSE-DEFENSE THEORY.....	32
D.	CUTTING THROUGH THE NUANCE OF OFFENSE- DEFENSE THEORY	36
1.	The Divide Between Perception and Reality	37
2.	Excess Factors Attributed to the Offense-Defense Balance	40
3.	Distinguishing Between Offense and Defense—Not Pertinent to the Balance	43
E.	CONCLUSIONS	46
 III.	 THE CONDITIONS THAT TIP THE BALANCE: THE CURRENT THEORY REVISITED	 49
A.	THE FACTORS OF OFFENSE-DEFENSE THEORY: TECHNOLOGY AND GEOGRAPHY.....	50
1.	Technology.....	51
2.	Geography	54
B.	THE CURRENT VARIABLES EXTOLLED BY OFFENSE- DEFENSE THEORY	57
C.	THE PROPOSED VARIABLES: REFORMATTING OFFENSE-DEFENSE THEORY FOR MODERN CONFLICT	61

1.	Variable 1. The Information Advantage: Enabling Surprise	61
2.	Variable 2. Decisive Effects: The Modern Firepower	64
3.	Variable 3. Exposure: Protection, Duration, and Costs for the Attack.....	66
4.	Variable 4. Insulation from Attack: Fortifications and Buffer Zones	68
5.	Variable 5. Criticality	73
6.	Variable 6. Resilience: The Modern Second-Strike.....	76
D.	THE EXCLUDED VARIABLES	79
1.	Mobility: Insufficient Evidence of Tipping the Balance.....	79
2.	Temporary Weapon Potency: Insufficient Evidence of Tipping the Balance	82
3.	Counterforce and Countervalue Weapons: Inability to Distinguish	83
E.	CONCLUSION	84
IV.	TESTING THE UPDATED OFFENSE-DEFENSE THEORY: AIR WARFARE AND IRREGULAR WARFARE	87
A.	DEFINING AIR WARFARE AND IRREGULAR WARFARE.....	87
B.	CASE SELECTION.....	90
C.	AIR WARFARE.....	96
1.	The Key Attributes of Air Warfare.....	98
2.	Offense in Air Warfare.....	103
3.	Defense in Air Warfare	105
4.	Do the Experts Perceive Air Warfare as Offensive or Defensive?	106
5.	Information Advantage—Air Warfare.....	108
6.	Decisive Effects—Air Warfare	112
7.	Exposure—Air Warfare.....	114
8.	Insulation—Air Warfare.....	117
9.	Criticality—Air Warfare.....	119
10.	Resilience—Air Warfare	120
11.	Conclusion—Air Warfare	121
D.	IRREGULAR WARFARE	122
1.	The Key Attributes of Irregular Warfare	124
2.	Offense in Irregular Warfare	129
3.	Defense in Irregular Warfare	132
4.	Is IW Offensive or Defensive? Expert Opinion and Data	134
5.	Information Advantage—IW.....	136
6.	Decisive Effects—IW	138

7.	Exposure—IW	140
8.	Insulation—IW	142
9.	Criticality—IW	144
10.	Resilience—IW	146
11.	Conclusion—IW	147
E.	CONCLUDING THOUGHTS ON AIR WARFARE AND IW	147
V.	THE CYBER OFFENSE-DEFENSE BALANCE	151
A.	WHAT IS CYBER CONFLICT?	152
B.	THE KEY ATTRIBUTES OF CYBER CONFLICT	154
1.	Technology in Cyber Conflict	158
2.	Geography in Cyberspace	159
C.	OFFENSE IN CYBER CONFLICT	161
D.	DEFENSE IN CYBER CONFLICT	163
E.	DO THE EXPERTS PERCEIVE CYBER CONFLICT AS OFFENSIVE OR DEFENSIVE?	165
F.	INFORMATION ADVANTAGE—CYBER CONFLICT	166
G.	DECISIVE EFFECTS—CYBER CONFLICT	169
H.	EXPOSURE—CYBER CONFLICT	172
I.	INSULATION—CYBER CONFLICT	173
J.	CRITICALITY—CYBER CONFLICT	175
K.	RESILIENCE—CYBER CONFLICT	178
L.	CONCLUSION—CYBER CONFLICT	180
VI.	CONCLUSION	181
A.	TOWARD RELEVANT DEFINITIONS: OFFENSE-DEFENSE THEORY AND BALANCE	181
B.	THE FACTORS AND VARIABLES OF THE OFFENSE- DEFENSE BALANCE	183
C.	TESTING THE VARIABLES	185
D.	THE CYBER OFFENSE-DEFENSE BALANCE	187
E.	THE IMPLICATIONS AND A LOOK TO THE FUTURE	188
	LIST OF REFERENCES	191
	INITIAL DISTRIBUTION LIST	217

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Depiction of the Methodology Progression in this Thesis.....	12
Figure 2.	The “Four Worlds” as Re-created from Jervis’ 1978 Article	45
Figure 3.	Conti and Raymond’s Chart Depicting the Primary Actors in Cyber Conflict	156

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Consolidated List of the Variables that Impact the Offense-Defense Balance.....	58
Table 2.	The Factors and Variables of Offense-Defense Theory (Developed by This Thesis).....	85
Table 3.	The Factors and Variables of Offense-Defense Theory	185
Table 4.	Offense-Defense Analysis of Air Warfare.....	185
Table 5.	Offense-Defense Analysis of Irregular Warfare	186
Table 6.	Offense-Defense Analysis of Cyber Conflict	188

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMD	air and missile defense
C2	command and control
C4I	command, control, communications, computers, and Intelligence
COIN	counterinsurgency
CSC	Cyberspace Solarium Commission
DCO	defensive cyberspace operations
DOD	Department of Defense
EMS	electromagnetic spectrum
EW	electronic warfare
GPC	great power competition
IADS	integrated air defense system
IR	International Relations
ISR	intelligence, surveillance, and reconnaissance
IW	Irregular Warfare
NATO	North Atlantic Treaty Organization
NSS	National Security Strategy
OCA	offensive counterair
OCO	offensive cyberspace operations
OE	operational environment
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
RADAR	radio detection and ranging
RMA	Revolution in Military Affairs
SAM	surface-to-air missile
SEAD	suppression of enemy air defenses
UAV	unmanned aerial vehicle
UW	unconventional warfare
USAF	United States Air Force
USSOCOM	U.S. Special Operations Command

WWI

World War I

WWII

World War II

ACKNOWLEDGMENTS

I owe an immeasurable debt to my wife, Siri, and our two daughters, Keira and Sydney. Their love and support made this thesis possible. My family also endured my writing process up close during the COVID-19 shelter-in-place order. If not for their patience and understanding through these unusual times, I am certain that I would not have finished.

I would also like to thank my advisors: Dr. Ryan Maness and Dr. Scott Jasper. It was their classes and publications that motivated this thesis. Their encouragement, mentoring, and support guided me across the finish line.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

If America, or U.S. Cyber Command, wanted to wage cyber war, it would do so from inside a glass house.

—Fred Kaplan, *Dark Territory*¹

An unease overshadows our relationship with cyberspace. The connective benefits of the digital world are immeasurable, as connectedness promotes rapid innovation and streamlines financial systems, defense networks, and critical infrastructure. However, the cybersecurity community is sounding a growing alarm. A pervasive neglect for cyber defense has left vast swaths of critical infrastructure exposed, providing an inducement for cyber-attacks. Former Deputy Defense Secretary William Lynn warns that cyberspace’s ever-evolving nature grants cyber offense “the upper hand,” as the endless changes leave the defense perpetually unprepared.² Richard Clarke specifically disparages the cyber defenses throughout the U.S., claiming that our rivals outmatch us in “overall cyber strength” because of our unhealthy dependence on cyberspace and fixation on offensive cyber capabilities.³ Global trends suggest that Clarke and Lynn are correct, as sensitive government networks and critical infrastructure suffer from a steady stream of cyber intrusions.⁴ These intrusions bear all the trappings of an offensive maneuver, as they

¹ Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 216.

² William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs* 89, no. 5 (2010): 99.

³ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat To National Security and What To Do About It*, First ed. (New York: Ecco Publishing, 2010), 147–49.

⁴ To garner a sense of the volume of intrusions, see: Kaplan, *Dark Territory*, 214; James Eng and Wendy Jones, “OPM Chief Says Government Agency Thwarts 10 Million Hack Attempts a Month,” news release, 16 June, 2015, <https://www.nbcnews.com/tech/security/opm-chief-says-government-agency-thwarts-10-million-hack-attempts-n376476>.

involve trespassing in an opponent's domain and threaten stability in the process.⁵ Finally, public intonements of a cyber doomsday—such as Leon Panetta's "cyber Pearl Harbor"—have emerged alongside a spate of disquieting cybersecurity failures, solidifying the world's unease with cyberspace.⁶

These troubling circumstances have unearthed some of the time-tested theories of international relations (IR) to develop insights into the instability spurred by cyberspace. Chief among these re-emergent theories is the offense-defense theory—a natural response to the claims of Lynn and Clarke—the crux of which is that dangerous implications arise when the relative advantage of offensive military strategies outweigh defensive strategies.⁷ The underlying logic is straightforward: when states perceive offense as the dominant strategy, they avoid fulfilling the role of defense by taking steps to capture the offensive role through actions such as a preemptive strike. In peacetime, these circumstances can instigate aggressive behavior and potentially escalate inter-state tensions. Conversely, if states perceive defense as the soundest strategy, the incentive to seize the initiative diminishes, thereby bringing an increased likelihood of peace.⁸ To better explain this

⁵ See the ontology of cyber actions from: Robert Belk and Matthew Noyes, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive U.S. Cyber Policy*, (Cambridge, MA: Harvard University Belfer Center for Science and International Affairs, 2012), 11–24, belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy; One of the pillars of Buchanan's argument is that intrusions threaten: Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford University Press, 2016), 96.

⁶ Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012, <https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>; Few failures of cybersecurity have alarmed the public more than the 2017 Equifax data breach: *Examining the Equifax Data Breach: Hearing Before the Committee on Financial Services, U.S. House of Representatives*, Serial No. 115–46, 115th Congress, 1st Session (5 October 2017). <https://www.govinfo.gov/app/details/CHRG-115hhrg30242/CHRG-115hhrg30242>.

⁷ George H. Quester, *Offense and Defense in the International System*, ed. Richard Rosecrance, International Relations Series (New York: John Wiley and Sons, 1977), 1–12; Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (1978): 187, <https://doi.org/10.2307/2009958>; Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security* 22, no. 4 (1998): 7–16, <https://doi.org/10.1162/isec.22.4.5>; Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton, NJ: Princeton University Press, 2010), 74–77.

⁸ A note of caution: the balance analogy evokes the image that offense and defense should be brought into balance. This undermines the concept of the offense-defense theory, defense assists the likelihood of peace, and an equally strong offensive preference could eradicate the push for peace. This thesis covers this more in the coming pages.

concept, most international relations (IR) scholars turn to the analogy evoked by Robert Jervis' seminal description of the theory: the offense-defense balance.⁹ By envisioning the struggle between offense and defense as a traditional-balancing scale that leans toward the heavier side, the central concept of the offense-defense theory becomes apparent. In essence, a virtual balance weights the relative advantage of offensive versus defensive strategies, inducing states to adopt the dominant strategy. The factors that influence military strategy and, consequently, the offense-defense balance are numerous; however, technology and geography represent the predominant factors of offense-defense theory as both have varied over time while producing a noticeable impact on military strategy.

Because technology consistently emerges as a catalyst for new strategies, the digital age has naturally sparked questions about how cyberspace changes the game.¹⁰ If Lynn and Clarke are correct about the dominance of cyber offense, the offense-defense theory describes an unsettling prospect—the incentive to attack is overwhelming in cyber conflict. Some of the noted cyber clashes between states, including Stuxnet, the 2007 Estonian cyber-attacks, and the 2016 U.S. presidential election, all suggest that brinkmanship has become the norm for state interactions in cyberspace. Perhaps, such incidents unfold in cyberspace because the pertinent actors perceive that offense is the dominant strategy. In this regard, applying offense-defense theory to cyber conflict makes sense: does cyberspace promote offensive behavior, and does this impact the stability of the international system?

The implications of these questions have drawn scholars and analysts alike, clamoring to offer their assessment of the cyber offense-defense balance. Unfortunately, the numerous attempts to analyze the cyber offense-defense balance have failed to find widespread agreement or gain any traction thus far.¹¹ As a result, the chief

⁹ Jervis, "Cooperation," 187.

¹⁰ Critics of offense-defense theory may argue that it is strategy and policy that drive military innovation, not technology, implying that aggression emanates from strategy as opposed to technology. However, organizational theory and history suggest otherwise: breakthrough military technologies, like the atomic bomb, tend to originate in civilian minds as opposed to military requirement documents, meaning that technology drives strategy, not the other way around. This point is further emphasized in chapter 2.

¹¹ See the literature review in this introductory chapter.

accomplishments of these attempts is criticism of the offense-defense theory and contradictory analytics, and both provide a guide for this thesis. The criticism highlights the need to address foundational problems of the offense-defense theory, and the inconsistent analytics suggest a methodology issue.

In other words, an analysis of the cyber offense-defense balance first demands two vital steps: a review of the core theory and a new method to assess the balance. Because a sound theory is necessary to derive meaningful insights into cyber conflict, this thesis aims to undertake that task. The analytical task of reconfiguring the offense-defense balance exposes the core argument of this thesis: despite the creative efforts to blur the lines of offense and defense in the international system, the overall distinctions are still discernible and remain a valuable tool in conflict analysis. The distinction enables analysts to recognize the growing origins of war, as the relative balance between offensive and defensive strategies can presage aggressive behavior when offensive strategies appear dominant. The aggressive behavior that arises from offensive strategies is, in part, a function of perceptions, and perceptions lean on a qualitative understanding of the world. This theoretical argument guides the restructuring of the offense-defense theory herein and shows how the modern instruments of war can incite conflict.

A. PURPOSE

The overarching aim of this work centers on analyzing the cyber offense-defense balance in order to understand the stability of cyberspace. However, a review of the literature reveals a fundamental problem; namely, the offense-defense theory requires significant overhaul before an assessment of the balance is undertaken. The theory lacks grounding and consistency, and its many versions often fail to tie into the offense-defense balance. Furthermore, how might one assess the balance? The typical approach involves calculating a net ratio of the offensive costs needed to claim territory versus the corresponding defensive costs.¹² While these calculation may provide some practical use,

¹² Charles L. Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and How Can We Measure It?," *International Security* 22, no. 4 (1998): 46, <https://doi.org/10.2307/2539240>; Glaser, *Rational Theory of International Politics*, 140.

the insinuation that a simple ratio is symbolic of the offense-defense balance does not follow the premise of the underlying theory.¹³ A balance measurement that relies on a cost ratio implies that actors on the international stage primarily care about the financial costs of war. It is true that costs often play a role in strategy development; however, when it comes to wartime decisions, most actors prioritize something else: winning.¹⁴ Hence, this study argues that the theory should center on perceptions and an effort to determine the drivers of perception in military strategy. In the case of changes within technology and geography driving the offense-defense balance, what variables generate offensive inclinations?

As a result, the purpose of this thesis becomes threefold: (1) offer a robust *definition* of the offense-defense theory, (2) *develop variables* that incite offensive strategies to produce an analytical framework for the offense-defense balance, and (3) employ that framework to *assess the cyber offense-defense balance*. While the methodology covers the intervening steps between these purposes, these goals constitute the deliverables of this thesis. Because the current literature presents a wave of critiques and perplexing nuance, the definition of offense-defense theory must aim to shed these problems. This thesis develops a set of variables that captures the conditions which, in turn, alter strategic perceptions and drive preferences for either offensive or defensive strategies, producing an analytical framework for the offense-defense balance in the process.¹⁵ Collectively, a coherent definition of the theory and a framework for offense-defense analysis build a reasoned evaluation of the cyber offense-defense theory.

¹³ Keir A. Lieber, "Mission Impossible: Measuring the Offense-Defense Balance with Military Net Assessment," *Security Studies* 20, no. 3 (2011): 452, <https://doi.org/10.1080/09636412.2011.599193>.

¹⁴ The 2014 QDR reveals how a constrained budget can impact strategic decision-making: Charles T. Hagel, *Quadrennial Defense Review* (Washington, DC: Office of the Secretary of Defense, 2014), <https://dod.defense.gov/News/Special-Reports/QDR/>; The 2018 NDS mirrors the more common defense goals of deterring aggression and winning if necessary, as opposed to saving money: James N. Mattis, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, 2018), 1, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

¹⁵ The variables reflect a similar approach used in determining innovation diffusion termed "Roger's Five Factors." This is addressed further in methodology: Everett M. Rogers, *Diffusion of Innovations*, Fifth ed. (New York: Free Press, 2003), 255–85.

B. LITERATURE REVIEW

The literature connecting the offense-defense theory to cyber conflict reveals the problems in the core theory and the disagreements about the stability of cyberspace. In terms of theorists who believe that there exists a propensity for cyber offense, Joseph Nye, Jr. makes a compelling case for the dominance of offense in cyberspace: “Because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense.”¹⁶ Ben Buchanan reaches a similar conclusion in his 2016 book, which argues that the necessity of intrusions in cyberspace operations can ensnare states in a series of escalations.¹⁷ Meanwhile, other academics argue that cyber offense may not exhibit the dominant properties that everyone fears, and the balance may favor the defense. For instance, Rebecca Slayton points to cost considerations, while Eric Gartzke and Jon Lindsay emphasize the fortifying role that deception plays in cyber defense.¹⁸ Finally, without directly referencing offense-defense theory, some authors caution that the literature exaggerates the instability of cyberspace, as the predominant feature of cyber conflict is actually restraint. For example, Thomas Rid argues that cyber capabilities act as a replacement for violent tools—thereby making the world less prone to conventional war—and notions of cyberwar are overblown.¹⁹ Similarly, Valeriano, Jensen, and Maness conclude that cyberspace has demonstrated an inability to produce escalations that spill outside the cyber domain thanks to interceding diplomacy.²⁰ The growing debate over offense and defense in cyberspace offers a rich exploration into its place in strategy and policy.

¹⁶ Joseph S. Nye Jr, *The Future of Power* (New York: Public Affairs Press, 2011), 115.

¹⁷ Buchanan, *Cybersecurity Dilemma*.

¹⁸ Rebecca Slayton, “What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment,” *International Security* 41, no. 3 (2016), https://doi.org/10.1162/ISEC_a_00267; Erik Gartzke and Jon R. Lindsay, “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,” *Security Studies* 24, no. 2 (2015), <https://doi.org/10.1080/09636412.2015.1038188>.

¹⁹ Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), xiv.

²⁰ Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), 203.

Some theorists question the merits of describing cyber conflict in terms of the offense-defense balance. For instance, John Arquilla cautions that historical attempts to identify the offensive or defensive properties of weapons to guide strategy have proven tragically inaccurate.²¹ Furthermore, Keir Lieber points to the failure of cyber advocates to demonstrate the potency of cyber-attacks, which he argues undermines a basic tenet of offense-defense theory.²² The critics of applying offense-defense theory, in general, worry that the theory oversimplifies the problem or leans on unhealthy assumptions. Concerns from authors such as Arquilla and Lieber raise the vital question that guides this thesis: what is the definition of offense-defense theory, and what aspects of warfare tip the offense-defense balance one way or the other? It is this question that led to the offense-defense literature.

1. The Problems in Offense-Defense Theory

The underlying principles of the offense-defense theory suggest that there are important implications when opponents perceive that conditions favor either an offensive or defensive strategy. Two scholars often credited with being at the forefront of the theory—George Quester and Robert Jervis—argue that conditions favoring offensive action raise the likelihood of escalation.²³ Following in the footsteps of Quester and Jervis, the IR theorists Charles Glaser, Stephen Van Evera, and Jack Snyder further develop the theory by identifying pertinent factors, offering a means to measure the balance, and presenting the implications.²⁴ Unfortunately, the intervening years since Quester and Jervis also brought a plethora of debates on the offense-defense theory, presenting a difficult roadblock to further theoretical development. Broadly speaking, the offense-defense theory

²¹ John Arquilla, “From Blitzkrieg to Bitskrieg: The Military Encounter with Computers,” *Communications of the ACM* 54, no. 10 (2011): 61–62, <https://doi.org/10.1145/2001269.2001287>.

²² Keir A. Lieber, “The Offense-Defense Balance and Cyber Warfare,” in *Cyber Analogies*, ed. John Arquilla and Emily O. Goldman (Monterey, CA: Naval Postgraduate School, 2014), 103, <https://calhoun.nps.edu/handle/10945/40037>.

²³ Quester, *Offense and Defense*; Jervis, “Cooperation.”

²⁴ William C. Wohlforth, “Realism,” in *The Oxford Handbook of International Relations*, ed. Christian Reus-Smit and Duncan Snidal (Oxford, UK: Oxford University Press, 2008), 142, <https://doi.org/10.1093/oxfordhb/9780199219322.003.0007>.

broadly now lacks two essential elements that would otherwise facilitate the purpose of this thesis: (1) a consistent definition within the IR community, and (2) an analytical framework to assess the offense-defense balance in cyberspace. Both problems directly contribute to the strategic inattention that stakeholders pay to the theory and its implications.

Since offense-defense theory entered IR vernacular in the 1970s, its logic has remained consistent. However, as scholars have sought to refine the theory in the intervening years, they invariably assign tenets and nuance to the theory to the point of being counterproductive instead of insightful. By introducing each of the excessive tenets and nuance, the offense-defense theory often confuses instead of clarifies, and its excess complexity does not allow for robust applications. The complexities arise on multiple fronts: the inability to distinguish between offense and defense, the perceptual and reality-based versions of the balance, and the multiple factors that could impact the balance. The weight-balance scale analogy, itself, also sparks misunderstanding at times, as the purpose of a balancing scale is to find equilibrium—to balance the two sides—instead of favoring one side: defense. As is made clear throughout this thesis, finding equilibrium in offensive and defensive strategies was never the intention of the analogy. Instead, only the comparison implied by the balance matters. A system comprised of equal perceptions concerning offense and defense can still pose a heightened risk of conflict due to some states being prone to aggression. Moreover, an equally strong belief in a defensive strategy may exacerbate the situation. Hence, such confusion and excess nuance detract from the theory.

Also, importantly, offense-defense literature does not offer an effective means of analyzing the offense-defense balance, and the predominant method—a net assessment of offensive and defensive cost-ratios to determine the balance—suffers from logical flaws. The clearest articulation of the net assessment method surfaces in the works of Glaser and his colleague Chaim Kaufmann. To measure the offense-defense balance, they recommend computing “the ratio of the cost of the forces that the attacker requires to take territory to

the cost of the defender's forces."²⁵ This method is appealing for two reasons: costs do play a central role in war decisions, and a ratio offers an easily-digested comparison for policy-makers. Unfortunately, calculating these ratios is also an immensely difficult task, offering numerous opportunities for programming or subjective errors.²⁶ Further, the notion of cost is subjective in and of itself. In his landmark study of American strategy, Russell Weigley produces a compelling case that U.S. policy and military strategy has evolved into pursuits of enemy annihilation while minimizing cost.²⁷ Though Weigley does not explicitly define "cost," the idea emerges time and again in his book that the employment and arming of U.S. forces over time betrays an underlying effort to minimize the time and lives lost in war, not the dollars required to wage it. After Weigley, additional studies of the American strategic culture reveal the same idea: the United States prefers to achieve victory quickly and with minimal casualties, through marshaling overwhelming and precise firepower.²⁸ In other words, Americans measure cost in time, casualties, and objectives. The goal is to win decisively—not fight a revenue-neutral war.

In terms of an alternate means to assess the offense-defense balance, the literature does offer specific properties that weapons and geography may possess that tip the balance; unfortunately, the current literature falls short in offering properties—or variables—that apply to modern conflict. An overview of the technological and geographic conditions that past offense-defense theorists argue as impactful to the offense-defense balance seem to have either (1) arisen from a myopic bias for land warfare, or (2) suffered from Cold War and twentieth-century World War orientations. Chapter III of this thesis captures these outdated variables, which reveals both an unfocused spread of efforts and the influence that

²⁵ Glaser and Kaufmann, "What Is the Offense-Defense Balance," 46.

²⁶ Lieber, "Mission Impossible," 452.

²⁷ Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy*, 1977 Paperback ed. (Bloomington, IN: Indiana University Press, 1973), xxii-xxiii.

²⁸ Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel* (Stanford, CA: Stanford University Press, 2010), 86; Colin S. Gray, *Another Bloody Century: Future Warfare* (New Haven, CT: Phoenix Press, 2007), 59; Theo Farrell, "Strategic Culture and American Empire," *The SAIS Review of International Affairs* 25, no. 2 (2005), <https://doi.org/10.1353/sais.2005.0033>.

the two World Wars exerted on the theory. In short, the theory is outdated and not suited to analyze the cyber offense-defense balance.

2. Attempts to Analyze the Cyber Offense-Defense Balance

Despite some of the shortcomings in the offense-defense theory, several attempts in scholarship have emerged to address the cyber offense-defense balance. The predominate approach hinges on Glaser and Kaufmann's recommendation of calculating the cost-ratio of offense and defense—a method already disputed in this thesis.²⁹ In the case of cyber conflict, these calculations have ultimately proven inconsistent, alternating between proclamations of offense and defense as the dominant strategy. The numerical calculations of the cyber offense-defense balance only underscore the subjectivity of the task. For instance, are foreign intelligence and network analysis offensive or defensive tasks? Does calculating the political and social fall-out of cyber-attacks warrant consideration? The laudatory efforts of the Naval Postgraduate School thesis by Patrick Malone and the security scholar Rebecca Slayton are the prime examples of these contradictions.³⁰ Their papers both produce a cost-ratio of the cyber offense-defense balance vis-à-vis a Stuxnet case study but ultimately disagree over the relative dominance of offense versus defense. Further, Stuxnet represents a unique case in its cost and scope, employing four costly zero-day exploits and jumping a secure "air gap" to target a highly-sensitive national system.³¹ Relying on Stuxnet as the sole measure for the cyber offense-defense balance does not capture the breadth of cyber conflict, especially given the atypical nature of the attack.³²

²⁹ Glaser and Kaufmann, "What Is the Offense-Defense Balance," 46; Ben Garfinkel and Allan Dafoe, "How Does the Offense-Defense Balance Scale?," *Journal of Strategic Studies* 42, no. 6 (2019), <https://doi.org/10.1080/01402390.2019.1631810>.

³⁰ Patrick J. Malone, "Offense-Defense Balance in Cyberspace: A Proposed Model" (Graduate Thesis, Naval Postgraduate School, 2012), 55–61, <http://hdl.handle.net/10945/27863>; Slayton, "What Is the Cyber Offense-Defense Balance?," 98.

³¹ Slayton, 95–101.

³² While Slayton's analysis focuses solely on Stuxnet, Malone also analyzes the 2007 DDOS attack on Estonia and finds an offense to defense cost ratio of 1:131: Malone, "Offense-Defense Balance in Cyberspace," 47–53.

Lieber and Ilai Saltzman both employ a different approach, leaning on two of the enduring variables that offense-defense theorists suggest are impactful to the balance: mobility and firepower.³³ Saltzman updates these recurring variables into the cyber-centric terms of “versatility” and “byte power” to produce an analysis of the offense-defense balance.³⁴ This approach, however, is insufficient as the offense-defense literature also purveys a compelling backlash against mobility and firepower, suggesting that new efforts ought to consider different variables. Furthermore, Saltzman’s approach is problematic as updating the past variables to versatility and byte power does not capture enduring properties of military capability that may incite aggressive behavior. For instance, byte power is a narrowly-focused term unlikely to offer useful insights in any application outside of cyber conflict. The offense-defense theory is simply at a point that necessitates an overhaul, and minor adjustments do not generate any lasting insights.

C. METHODOLOGY

To avoid the same fate as past assessments of the cyber offense-defense balance, this thesis undertakes a different approach— a return to the literature to derive variables pertinent to the balance, and apply those variables to cyber conflict.³⁵ Unfortunately, the literature review exposes a significant hurdle to this method; namely, the variables within the literature do not exhibit sufficient relevance to modern warfare. Thus, this method requires new variables. However, the approach in this thesis is not to wholly discount the

³³ Lieber, “The Offense-Defense Balance and Cyber Warfare,” 100–04; Ilai Saltzman, “Cyber Posturing and the Offense-Defense Balance,” *Contemporary Security Policy* 34, no. 1 (2013): 42–45, <https://doi.org/10.1080/13523260.2013.771031>.

³⁴ Saltzman, “Cyber Posturing,” 43–44.

³⁵ Keir Lieber does briefly do this in his analysis of the cyber offense-defense balance; however, he focuses on just a few attributes: Lieber, “The Offense-Defense Balance and Cyber Warfare,” 100–01; Ilai Saltzman also does this by “cybernating” offense-defense theory (“From Mobility to ‘Versatility,’ and From Firepower to ‘Byte Power’), however, he does not consider some of broader variables offered by the literature, e.g., surprise: Saltzman, “Cyber Posturing,” 42–45; Most literature on the cyber offense-defense balance focuses on the telling aspects of cyber conflict, anecdotes, or heuristics of cyber offense and cyber defense: Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security* 38, no. 2 (2013), https://doi.org/10.1162/ISEC_a_00138; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 153–56; Rid, *Cyber War Will Not Take Place*, 167–70.

variables already present in the literature, as past theorists have demonstrated their explanatory power in determining the balance. As a result, the offense-defense literature provides an apt starting point for the development of an analytical framework in modern warfare. The goal is to provide a lasting set of variables that do not wither along with cyber conflict.

To reach this goal, the methodology to assess the cyber offense-defense balance and how it may tip unfolds in four parts: refine the definition, develop the variables, test the variables for robustness, and then apply the variables to cyber conflict. To succinctly capture this process, Figure 1 provides a visual representation. The first step, refining the definition, involves returning to the literature and refocusing the theory toward the impacts and assessment of the offense-defense balance, as the current definition fails on both accounts. Next, to develop offense-defense variables for the assessment, the literature also provides a starting block as the current variables speak to conventional war, and the aim is to achieve a generalizable theory. This thesis applies four general tests to develop and propose new variables of the offense-defense balance: logical assessment, doctrine, short examples, and significant arguments. These tools refine the variables to produce an analytical framework for the offense-defense balance. To verify the robustness of the resulting variables, this thesis tests those variables in two modern forms of conflict: air warfare and Irregular Warfare (IW). Finally, the variables and analytical framework from this thesis come to bear on the topic at hand—assessing the cyber offense-defense balance.

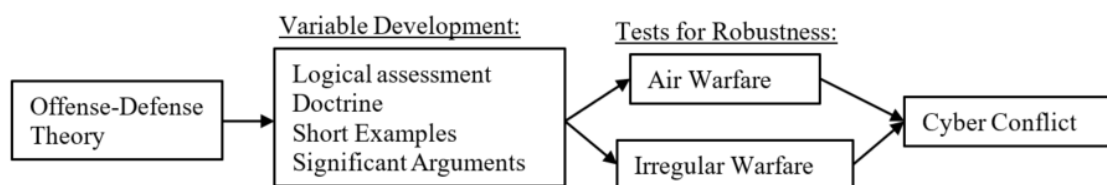


Figure 1. Depiction of the Methodology Progression in this Thesis

To produce an effective analytical framework for the offense-defense balance, this thesis models the offense-defense variables on a successful approach in business literature:

Everett Rogers' "five factors" of innovation diffusion.³⁶ Innovations, much like military strategy, take hold and diffuse, or spread, throughout a targeted social system based on the perceptions that the population holds toward the innovation. For context, Rogers' five factors are (1) relative advantage, (2) compatibility, (3) complexity, (4) trialability, and (5) observability.³⁷ How strongly people ascribe Rogers' five factors to emerging innovations determines whether diffusion occurs. The crux is that if emerging innovations can exhibit potential through an analysis of Rogers' five factors, its chances for adoption are high. This same model can apply to the perceptions underlying the offense-defense balance. If a set of technological and geographic factors sufficiently alter perceptions that offense or defense is a dominant strategy, then the actors adopt the corresponding strategy. Importantly, there is never just one variable that sways perceptions—a point underscored by Rogers' theory on innovations. It is a net assessment of the main perceptual issues, and, ultimately, this thesis arrives at six variables, creating an analytical framework to assess newer modes of conflict, much as a framework for assessing innovation emerges from Rogers' five factors.

Conducting an analysis of the offense-defense balance through air warfare and IW also raises the issue of case selection. Why lean on air warfare and IW to test the developed variables in this thesis? The primary reason rests with the modern applicability of both modes of conflict while also "bridging the offense-defense theory gap" from land warfare to cyber conflict. This "gap" in theory refers to the predominant focus that offense-defense theorists pay to traditional forms of conflict, particularly land warfare, then forego any concerted efforts to improve the theory until cyber conflict. Thus, air warfare and IW have *received only sparing attention in the current offense-defense literature* while emerging as *highly relevant modes of conflict*. Additionally, these two modes of conflict *possess analytical features similar to those of cyber conflict* in three ways: all are inherently disparate, all possess asymmetric qualities, and all fail to conform to traditional battleground geometries. In other words, air warfare, IW, and cyber conflict all share

³⁶ Rogers, *Diffusion of Innovations*, 255–85.

³⁷ As an important aside, while Rogers uses the term "factors" to describe the attributes of innovations, this thesis uses "variables" given the developing nature of the concept.

similarities that do not readily meet the eye; thus, the considerations for offense and defense ultimately prove similar, as well, providing analogous insights during the study. Finally, air warfare and IW both coincide with a rich literature, with case studies and expert opinions readily available to underscore the theoretical conclusions. Chapter IV further explores these points in finer detail to reinforce the points of this paragraph.

D. MAJOR FINDINGS AND ORGANIZATION

Through the proffered methodology, this thesis establishes a pertinent definition of the offense-defense theory, provides a framework to examine the offense-defense balance, then employs this framework on cyber conflict. To facilitate clear organization, the Chapter breaks mirror this progression. First, Chapter II presents the definition offense-defense theory with the underlying aim of cutting through the excess nuance, ensuring validity to modern warfare, and tying the theory to the balance. An essential part of determining the definition is a return to the parent disciplines—IR studies and the realist school of thought—to draw out the theoretical underpinnings. In terms of the theoretical definition, three key recommendations emerge. First, to keep the definition focused on perceptions and conflict management, the objective, or reality-based, version of the offense-defense balance is discarded. Second, to keep the focus on the balance and prediction offensive inclinations, the definition herein excludes differentiation. Third, the pertinent factors that vary through history and thus motivate offensive or defensive strategies are technology and geography.³⁸ Chapter III starts with the variables from the offense-defense literature then moves through the process of developing the offense-defense variables that constitute an analytical framework. As a result of this analysis, this thesis finds that the offense-defense balance tips as the result of six variables pertaining to technology and geography: the information advantage, decisive effects, exposure, insulation, criticality, and resilience.

In the second half of this thesis, the variables and analytical framework from this thesis come to bear on the topic at hand. Chapter IV shows the test for robustness through air warfare and IW by first establishing the key issues and definitions before assessing both

³⁸ Quester, *Offense and Defense*, 2; Jervis, “Cooperation,” 194.

modes of conflict through the lens of each offense-defense variable. Testing of the variables developed in Chapter III against air warfare and IW suggests that they exhibit sufficient explanatory power, as the tests align with expert views and trends. Finally, Chapter V summons the lessons from the previous Chapters to assess the cyber offense-defense balance. When applying the six variables to cyber conflict, the analysis in this thesis suggests that cyber offense-defense balance favors the offense. This finding hinges on four particular variables tipping the balance:

1. The information advantage that one can gain through offensive cyber actions,
2. The complete lack of exposure enjoyed by attacking units in OCO,
3. The perception that critical assets are targetable through cyberspace, and
4. The lackluster insulation of passive cyber defense.

Another important factor that ties the last two variables together and inhibits the defense is that the private sector owns and operates many of the attractive targets in cyberspace, resulting in a low-level of insulation and increased vulnerability of critical assets. Prominent voices in the U.S. Government are raising concerns over the poor cyber defenses that haunt the United States and its allies, giving hope to the goal that the world may quell the welling conflict of cyberspace.³⁹

³⁹ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, (Arlington, VA: The Cyberspace Solarium Commission, 2020), vi, <https://www.solarium.gov/>.

THIS PAGE INTENTIONALLY LEFT BLANK

II. OFFENSE-DEFENSE THEORY DEFINED

Pure defense, however, would be completely contrary to the idea of war, since it would mean that only one side was waging it. Therefore, defense in war can only be relative, and the characteristic feature of waiting should be applied only to the basic concept, not to all of its components.

—Carl von Clausewitz, *On War*⁴⁰

Why do states go to war? Whole forests have fallen to print literature on this question, and because the offense-defense theory identifies a causal factor in war, it, too, plays a role in the deforestation. Offense-defense theory describes a condition that incites aggressive behavior between states, and aggressive behavior leads to an increase likelihood that states may choose conflict over cooperation. As Chapter I explains, the aggressive behavior arises when actors perceive that the relative balance of offense and defense favors the offense, causing the actors to adopt offensive strategies. The offense-defense theory continues to evolve while sparking healthy academic debate, which is indicative of both its appeal and limitations. Constructive debate is a necessary part of theoretical development, as examining theory through a skeptical lens bolsters the theoretical explanatory power, while also finding and limitations.⁴¹ It is the limitations of the offense-defense theory that are the focus of this chapter and the next. As it stands, the theory does possess many of the attributes that science typically upholds as crucial. Chief among these attributes is explanatory power—a theoretical trait that Van Evera argues offense-defense theory possesses, as his book leverages the offense-defense balance to identify the origins of

⁴⁰ Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret, Indexed ed. (Princeton, N.J: Princeton University Press, 1984), 357.

⁴¹ Kenneth Waltz identifies this as his goal at the onset of his pioneering work in international political theory: Kenneth N. Waltz, *Theory of International Politics*, First ed., Addison-Wesley Series in Political Science (Reading, MA: Addison-Wesley Publishing Company, 1979), 18.

numerous wars.⁴² Unfortunately, the offense-defense theory also needs refinement, as it suffers from the detracting attributes addressed in the Literature Review of Chapter I. This chapter and the next comprehensively addresses these problems.

Simply put, the offense-defense theory currently does not provide the tools to conduct the assessment that this thesis aims to offer: an assessment of the cyber offense-defense balance through analyzing the pertinent factors that offense-defense theory identifies.⁴³ It currently lacks two essential elements that would otherwise facilitate the purpose of this thesis: (1) a consistent definition within the IR community, and (2) an analytical framework to assess the offense-defense balance in cyberspace. This chapter focuses on the first problem, and the next chapter focuses on the second. Fixing these two issues enables an analysis of the balance in cyberspace.

In sum, the purpose of this chapter is to offer a definition of offense-defense theory that is applicable across multiple forms of conflict. To reach such a definition, this chapter focuses on the salient parts of the theoretical definition, including its tenets, then identifies and discards the unnecessary complexity that renders the theory ineffectual. First, this necessitates a basic understanding of the roots of the offense-defense theory, paying particular attention to the realist school of thought and its contemporary divide between offensive and defensive realism. Second, this chapter defines the concepts of war, offense, and defense, and provides the definition of offense-defense theory leveraged throughout this thesis. Importantly, this definition focuses solely on the offense-defense balance, as the balance identifies conditions in the international system that may lead to war. Next, this chapter addresses some of the important critiques that scholars have raised concerning the offense-defense theory, which helps to shape the theoretical limits of the theory. Finally,

⁴² For a sampling of well-regarded views on “good” theory, see: Peter Kosso, *Reading the Book of Nature: An Introduction to the Philosophy of Science* (New York: Cambridge University Press, 1992), 27–50; Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research* (Princeton, NJ: Princeton University Press, 1994), 19–23; Stephen Van Evera, *Causes of War: Power and the Roots of Conflict*, ed. Robert J. Art, Robert Jervis, and Stephen M. Walt, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 1999), 185–92.

⁴³ This approach is different from prominent works that have emerged thus far on the cyber offense-defense. See the literature review of Chapter I.

this chapter pairs away the complexity brought on by excess nuance within the literature, which has confounded the theory and has confused analysts looking to apply it. By discarding the unnecessary complexity from the theory, a version of the theory emerges that facilitates the goal of this thesis: analyzing the cyber offense-defense balance.

A. THE ROOTS OF OFFENSE-DEFENSE THEORY

The roots of offense-defense theory provide two primary benefits for the reader: the theoretical context and clarity on the conceptual offerings of the theory. It is from the realist IR tradition and its prominent subschools—offensive and defensive realism—that offense-defense theory emerged.⁴⁴ Understanding realism and its subschools helps bring the theory into focus.

1. Realism

Realism is an IR school of thought that begins with certain axioms about the anarchical international state system and analyzes their causes and consequences.⁴⁵ The principle goal of IR realists is to identify those variables that can lead to either conflict or cooperation in the international system. According to realism, the chief enabler of any violent or aggressive state behavior is the anarchy that defines the international system.⁴⁶ Within the international anarchy, realists believe that power is the focal explanatory tenet of state action, which is a point that Hans Morgenthau makes in his “six principles of political realism.”⁴⁷ Because realism centers on power, many of its theories emanate from the assumption that actors—including states—gravitate to Realpolitik methods to achieve their interests, meaning that they attempt to align those forces needed to gain and maintain

⁴⁴ Wohlforth, “Realism,” 138–42.

⁴⁵ For an in-depth understanding of realism and its philosophy, see: E. H. Carr, *The Twenty Years' Crisis, 1919–1939: An Introduction to the Study of International Relations*, 1981 Printing of the Second ed. (London, UK: Macmillan Press, 1946), 10.

⁴⁶ Kenneth N. Waltz, “The Origins of War in Neorealist Theory,” *The Journal of Interdisciplinary History* 18, no. 4 (1988): 620, <https://doi.org/10.2307/204817>.

⁴⁷ Morgenthau refers to power as the “signpost” of policy: Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, Fifth ed. (New York: Alfred A. Kopf, 1978), 4–15.

power.⁴⁸ Kenneth Waltz provides one of the most straightforward and encompassing definitions of Realpolitik, writing that its elements are these: “The ruler’s, and later the state’s, interest provides the spring of action; the necessities of policy arise from the unregulated competition of states; calculation based on these necessities can discover the policies that will best serve a state’s interests; success is the ultimate test of policy, and success is defined as preserving and strengthening the state.”⁴⁹ Part of the policy that best serves the interest of a state is military strategy. Military strategy—often referred to as doctrine—forms and then changes based on a variety of factors, leading states to adopt policy befitting their respective circumstances.⁵⁰ The underlying motivations in the interplay of power, doctrine, and state policy has since sparked much debate within realism.

2. Offensive and Defensive Realism

As a result of these debates, realism spawned two distinct subschools: offensive and defensive realism.⁵¹ The basic point of contention between the two is a disagreement over the motivations that guide international actors toward either conflict or cooperation. Offensive realism holds that states act in a fashion that is expansionist in nature and seek to protect their interests through gaining additional power, thereby causing conflict.⁵² Meanwhile, defensive realism centers its arguments on the belief that states seek to

⁴⁸ The states of the anarchic Westphalian system often operate as the “groups” in this definition.

⁴⁹ Waltz, *Theory of International Politics*, 117.

⁵⁰ Barry Posen offers one of the seminal works exploring factors that impact doctrine. He specifically explores the impacts of organizational and international balancing issues in the interwar years in Europe: Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*, ed. Robert J. Art and Robert Jervis, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University of Press, 1984).

⁵¹ The more accurate terminology here is “offensive and defensive neorealism.” “Realism” is used here for the sake of simplicity. Neorealism arose as an evolutionary step within realism influenced primarily by the work of Kenneth Waltz: Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis*, 2001 ed. (New York: Columbia University Press, 1959); Waltz, *Theory of International Politics*; On Waltz’s impact on realism and neorealism: Wohlforth, “Realism,” 135–39.

⁵² Wohlforth, “Realism,” 138–39.

entrench their security out of a sense of fear, and only changes to the system interrupt that status quo and force states into war.⁵³

Today, both subschools benefit from a few prominent works that encapsulate the views of both camps. First, John Mearsheimer's *The Tragedy of Great Power Politics* plays an immense role in offensive realism, a book in which he contends that the historical behavior of states reveals a prevailing desire of the powerful to gain and grow a hegemony.⁵⁴ According to Mearsheimer, while it may appear that powerful states often act out of greed, they actually act out of fear—fear of losing what they have gained. Mearsheimer makes the case that a historical review reveals that hegemonies behave more aggressively as they gain power, and their policy betrays a fear of losing that power.⁵⁵

Mearsheimer's argument that a state will not stay content once secure runs counter to the status quo argument of defensive realism. The concepts that underpin defensive realism appear prominently in Waltz's writing: "In anarchy, security is the highest end...The first concern of states is not to maximize power but to maintain their positions in the system."⁵⁶ He makes this point through highlighting the tendency of states to follow both internal and external balancing behaviors, meaning that states act to quell any rising power that threatens to disrupt the present balance of power, or status quo.⁵⁷ A state's internal balancing involves strengthening its economic or military disposition, while external balancing most often involves tailoring alliances to keep rising powers in check. Other defensive realists have taken his argument a step further by contending that the international anarchy punishes aggressive behavior, which suggests that most states are

⁵³ Wohlforth, 138–39.

⁵⁴ John J. Mearsheimer, *The Tragedy of Great Power Politics*, Updated ed. (New York: W. W. Norton & Company, 2014), 29–46.

⁵⁵ Mearsheimer, *Tragedy of Great Power Politics*, 332–33.

⁵⁶ Waltz, *Theory of International Politics*, 126.

⁵⁷ Waltz, 118.

security seekers.⁵⁸ Since the international system generally punishes those that act aggressively, aggressive behavior does not often arise but for three reasons: domestic political issues, the fear of aggression from others, or perceptions that conditions favor aggression.⁵⁹ Because defensive realism tends to view these perceptions as a causal factor of aggressive behavior, most theorists attribute offense-defense theory to defensive realism.

3. The Originators of Offense-Defense Theory

It is difficult to pin down the originator of offense-defense theory; thus, it is best to credit two authors: George Quester and Robert Jervis. Both conceive of the theory in a fashion that resembles other defensive realist theories—as a phenomenon grounded in the realities of the international system and its security-seeking nations. The primary difference between the two authors is that Quester wrote about the theory primarily as a means of crafting sensible arms controls, while Jervis noted its impact on a theory known as the “security dilemma.” Quester’s approach arose, in part, from Schelling and Halperin’s *Strategy and Arms Control*, in which they recommend that the international community enact initiatives reducing the advantage that attackers stand to gain through surprise attacks or the initiative.⁶⁰ Seizing on this idea in his 1974 book, *The Continuing Problem of International Politics*, Quester suggests that the international community may have success in arms control efforts by differentiating between offensive and defensive weapons, much

⁵⁸ “At least in the long run, the balance of power that arises out of international anarchy punishes aggression; it does not reward it. Consequently, strategies of security through expansion violate the basic principles of international politics,” Jack L. Snyder, *Myths of Empire: Domestic Politics and International Ambition*, ed. Robert J. Art, Robert Jervis, and Stephen M. Walt, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 1991), 11; “In fact the structure of international power provides more disincentives than incentives for aggression. Aggressors are more often punished than rewarded...Aggressor states usually are contained or destroyed,” Van Evera, *Causes of War*, 9.

⁵⁹ Jack L. Snyder and Keir A. Lieber, “Defensive Realism and the ‘New’ History of World War I,” *International Security* 33, no. 1 (2008): 184.

⁶⁰ Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control* (New York: The Twentieth Century Fund, 1961), 12.

as it had attempted in the Disarmament Conference of 1932.⁶¹ Then, in 1977, he published *Offense and Defense in the International System*, in which he identifies offensive advantages as a distinct variable that raises the likelihood of war.⁶²

For Jervis, the offense-defense balance arose as a key to the puzzle posed by another theory in the realist tradition—the security dilemma. The basic principle of the security dilemma is that when an actor attempts to bolster its defenses, that action can paradoxically degrade the actors security as the surrounding actors then face an incentive to also increase their defenses, which often includes a measure of offensive capability.⁶³ The IR scholar John Herz is often credited with coining the phrase in a 1950 article: “there has arisen what may be called the ‘security dilemma’ of men...Striving to attain security from attack [s], they are driven to acquire more and more power in order to escape the impact of the power of others. This, in turn, renders the others more insecure and compels them to prepare for the worst.”⁶⁴ A problem with the security dilemma theory is that, by itself, it suggests a world in which international cooperation is a near impossibility. In answer to this puzzle, Jervis’ 1978 article, “Cooperation Under the Security Dilemma,” introduces the offense-defense balance into neorealist theory and demonstrates how the balance can dampen the effects of the security dilemma. The difficulty for cooperation under the security dilemma arises due to its self-reinforcing dynamics that result in escalations that can “spiral” out of control.⁶⁵ Jervis argues that the balance offers conditions in which states can expand their security without threatening their neighbors. According to Jervis, when the balance of

⁶¹ George H. Quester, *The Continuing Problem of International Politics* (New York: The Dryden Press, 1974), 51–55; One of the foremost tellings of the Disarmament Conference of 1932 can be found in: Marion W. Boggs, *Attempts to Define and Limit “Aggressive” Armament in Diplomacy and Strategy*, ed. H. M. Belden et al., The University of Missouri Studies (Columbia, MO: University of Missouri, 1941), 7–17.

⁶² Quester, *Offense and Defense*, 10.

⁶³ The IR scholar Shiping Tang offers a thorough definition of the security dilemma that he derived from Herz, Butterfield, and Jervis. I, in turn, derive this shortened definition from Tang. Shiping Tang, “The Security Dilemma: A Conceptual Analysis,” *Security Studies* 18, no. 3 (2009): 594, <https://doi.org/10.1080/09636410903133050>; Herbert Butterfield, *History and Human Relations* (London, UK: Collins Clear-Type Press, 1951), 19–22; John H. Herz, “Idealist Internationalism and the Security Dilemma,” *World Politics* 2, no. 2 (1950): 157, <https://doi.org/10.2307/2009187>; Jervis, *Perception and Misperception*, 76.

⁶⁴ Herz, “Idealist Internationalism and the Security Dilemma,” 157.

⁶⁵ Jervis, “Cooperation,” 175; Tang, “The Security Dilemma: A Conceptual Analysis,” 592.

military power favors defensive strategies, states may increase their security without sparking a security dilemma; hence, states may cooperate while the security dilemma theory still offers explanatory power.⁶⁶ Though Jervis does not discount the practical uses of offense-defense theory that Quester puts forth, his primary argument is that the theory possesses theoretical value.

Thus, offense-defense theory aligns with defensive realist thinking and provides practical and theoretical use. It is primarily from Quester and Jervis that the offense-defense theory and the balance entered the neorealist lexicon, and its message was clear in the Cold War—the United States and Soviets should both be wary of the offensive capability that both sought. The link between offense-defense theory and defensive realism begins with the common assumption that states generally avoid war unless provoked, which aligns with the notion that a perceived offensive advantage in the system may elicit aggressive behavior in otherwise secure states. Following the theoretical work of Quester and Jervis, other defensive realists sought to consider what sways the balance and the implications, including Glaser, Van Evera, and Snyder.⁶⁷

The quest to identify war-causing conditions ties back to the central task of this thesis—determine if cyberspace entices aggressive behavior as a result of the cyber offense-defense balance. By knowing what conditions spark aggression in the cyber realm, we can identify when the likelihood of conflict emerges. Unfortunately, the debate surrounding offense-defense theory has bestowed a complexity to the theory, which threatens to undermine the goal of identifying dangerous conditions in the international system.

B. DEFINING THE THEORY

1. Conflict, War, Offense, and Defense

Before moving into a finer definition of the offense-defense theory, the more basic issue arises of distinguishing between “conflict” and “war” and between “offense” and

⁶⁶ Jervis, “Cooperation,” 186–211.

⁶⁷ Wohlforth, “Realism,” 142.

“defense.” Understanding these basic roles of conflict helps build the foundation for the theory.

“War” tends to suffer from an ever-expanding range of definitions, raising the need for such phrases as “conflict.” In terms of the offense-defense theory, the meaning in words such as “invasion” and “attack” is clear: violence. Even Clausewitz, who famously links war to politics, brings his readers back repeatedly to the destructive components of war, including “force” and “violence.”⁶⁸ However, newer forms of war, including cyberwar, have found other means besides violence to inflict suffering or coerce an adversary into accepting a political goal, lending credence Clausewitz’s emphasis on politics. Because war tends to refer to a prolonged set of battles and competition between states often comprises a limited or non-sequential set of events, it is often appropriate to use the term “conflict” for such engagements. A conflict often involves suffering though not at the scale seen in war. For instance, one may argue that a full “cyberwar” has yet to transpire, though fierce competition has arisen that threatens mass suffering to reach a political end. To cope with the vague undertones of war and conflict, the quantitative analysts at the Correlates of War project have introduced a minimum number of battle deaths that a given combat situation must exhibit before qualifying as a war.⁶⁹ Thus, this thesis considers war the result of two or more organized entities that enact violent suffering on each other in an effort to force a political goal on the opposition and requires at least 1,000 battle deaths, in accordance with the Correlates of War.⁷⁰ Conflict also involves suffering and international competition, though at a scale below this definition of war. Hence, relatively low violence

⁶⁸ Clausewitz, *On War*, 75–89.

⁶⁹ For the Correlates of War project, if a conflict does not cross the threshold of 1,000 battle deaths, it is considered a “Militarized Interstate Dispute” instead of a war: Daniel M. Jones, Stuart A. Bremer, and J. David Singer, “Militarized Interstate Disputes, 1816–1992: Rationale, Coding Rules, and Empirical Patterns,” *Conflict Management and Peace Science* 15, no. 2 (1996): 171, <https://doi.org/10.1177/073889429601500203>.

⁷⁰ For a definition of war that ties together many references, see the “Object and Nature of War” in: General Counsel of the U.S. Department of Defense, *Department of Defense Law of War Manual (Updated 2016)* (Washington, DC: U.S. Government Printing Office, 2015), 15–17, https://permanent.access.gpo.gov/gpo71097/DOD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf; George Quester raises an important point when he emphasizes the organized nature of war: Quester, *Offense and Defense*, 16.

inflicted thus far through cyberspace, “cyber conflict” is the appropriate terminology for this thesis

Traditionally, war requires one side of the conflict to assume an offensive role and the other a defensive role.⁷¹ One attacks, while the other thwarts. One invades, while the other resists. Clausewitz offers a straightforward definition of defense that still applies today: “What is the concept of defense? The parrying of a blow. What is its characteristic feature? Awaiting the blow. It is this feature that turns any action into a defensive one; it is the only test by which defense can be distinguished from attack in war.”⁷² Clausewitz also warns that delving into the nuance of selected actions only serves to confuse the matter, and any attempt to distinguish between offense and defense should consider the broad context, not the individual actions. The overall disposition at the operational level of war defines the roles between two adversaries—not the individual units. For instance, an invading army may not fire the first shot of the war; yet, an invasion clearly denotes the offensive side of the war. Recalling the brief definition of the offense-defense theory from Chapter I, the fundamental purpose of the theory is to identify a condition that can incite war. Consequently, an attempt to determine if an action is offensive must consider the prebattle status quo.⁷³ Clausewitz’s definition does not account for an essential tenet of a sound defense: the counterattack.⁷⁴ When does a counterattack become offensive? In answer, it is best to consider the differing purposes of offense and defense: the defense is passive in the grand context and seeks to maintain the current disposition, while the offense is proactive and projects one’s capabilities.⁷⁵ Thus, a counterattack becomes offensive if it

⁷¹ Clausewitz, *On War*, 357–58.

⁷² Clausewitz, 357.

⁷³ The concept of a “prebattle status quo” arises in Carter’s discussion of offense and defense at the operational level of war: John R. Carter, *Airpower and the Cult of the Offensive*, Air University CADRE Papers (Maxwell AFB, AL: Air University Press, 1998), 7, <https://www.airuniversity.af.edu/AUPress/CADRE-Papers/>.

⁷⁴ Though it did not appear in his basic definition, Clausewitz does discuss counteroffensive, by stating, “a war in which victories were used only defensively without the intention of counterattacking would be ...absurd”: Clausewitz, *On War*, 358.

⁷⁵ Clausewitz, *On War*, 358. The use of passive here does not preclude active defensive measures taken behind one’s own battle lines.

projects power in some way, or by seizing control or attempting to encroach on an adversary's assets. The U.S. military doctrine aligns with this notion, including when it deals with modern forms of conflict. Looking specifically at cyber conflict, doctrine delineates between offensive cyber operations (OCO) and defensive cyber operations (DCO) as those that project power and those that protect against threats.⁷⁶ In applying these doctrinal definitions, the “defend forward” strategy of the U.S. Department of Defense (DOD) appears offensive, as the strategy entails disrupting malicious cyber activity at the source.⁷⁷ Defending forward implies a level of pro-action: projecting forward to degrade the capability of an adversary without first suffering an adversary's attack. Hence, the defend forward strategy is an admission that while offensive maneuvers may be preferred, the DOD must adopt this branding to signal its intentions to maintain stability.

Thus, the doctrinal definitions of OCO and DCO demonstrate how the concepts of offense and defense have truly survived the test of time, and statesmen and practitioners can still use these notions to categorize actions in conflict.⁷⁸ Because war offers such distinctions between offense and defense, the international community has attempted to leverage this distinction for arms control purposes. For instance, the Disarmament Conference of 1932 aimed to limit “aggressive” armament, though the parties ultimately disagreed over what constituted an offensive or defensive weapon.⁷⁹ IR theorists soon followed suit, building on the distinction between offense and defense to identify conditions may increase or decrease the chances of conflict.⁸⁰ Since war requires an

⁷⁶ U.S. Department of Defense, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2018), xi, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

⁷⁷ James N. Mattis, *Summary of the 2018 Department of Defense Cyber Strategy* (Washington, DC: Office of the Secretary of Defense, 2018), 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

⁷⁸ A message often extracted from Ben Buchanan's book is that cyberspace has blurred the lines between offense and defense because cyber defense often requires cyber offense. Analysis in this thesis leads to a different interpretation. This thesis argue that both are still distinct; however, perceptions of cyber defense are at times so weak that it requires supplemental offense. See: Buchanan, *Cybersecurity Dilemma*, Chapter 3.

⁷⁹ Boggs, *Attempts to Define and Limit*, 93.

⁸⁰ Quester, *The Continuing Problem of International Politics*, 51–55.

offense and a defense, does the chances of war decrease if conditions discourage offensive actions? How are international relations impacted if all states prefer defensive strategies?

2. Causes of War: Origin or Outbreak

Understanding the distinction between the *origins* of war and the *outbreak* of war proves valuable in analyzing the causes of war and is pertinent to offense-defense theory. The origins are a set of conditions present in a given system that foster war, while an outbreak refers to the event(s) immediately prior to the war that spark its initiation.⁸¹ An exploration into the origins of war involves looking at the deep cultural or systemic issues that promote war or, in the timeless words of Thucydides, “made war inevitable.”⁸² These underlying issues can combine to a point where the conditions are sufficient for the outbreak of war. By contrast, exploring the outbreak of a war involves analyzing the events immediately prior that offered the last chance to avoid war. Focusing on the outbreak often leads to placing blame on poorly managed signals or miscalculations that sparked war. Both views—origins and outbreaks—offer valuable ways to analyze the cause of war. The offense-defense theory identifies a cause of war, based on the balance of offense and defense. Understanding the distinction in origin and outbreak helps to clarify both the definition of the theory and the implications of the balance.

3. Preventive Wars and Pre-Emptive Strikes

Though commonly tied to ethical discussions, the difference between preventive and pre-emptive wars also becomes important in offense-defense theory as both types of war stem from a need to seize the initiative. A preventive war is proactive in nature while a pre-emptive war is reactionary in nature. In their article on justifications for preventive

⁸¹ Thucydides’ timeless work on the Peloponnesian War aptly reveals the distinction. He believes the war to be an origin story—that Sparta’s growing alarm stoked by the rising power of Athens made war inevitable is an origin. The skirmishes before the war that sparked its outbreak were mere pretexts: Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, ed. Robert B. Strassler, trans. Richard Crawley (New York: Free Press, 1996); The historian Donald Kagan even credits Thucydides for “invent [ing] the distinction between the underlying, remote causes of war and the immediate causes”: Donald Kagan, *The Outbreak of the Peloponnesian War* (Ithaca, NY: Cornell University Press, 1969), 345.

⁸² Thucydides, *The Landmark Thucydides*, 1.23.

use of force, Buchanan and Keohane write that, “Preventive use of force may be defined as the initiation of military action in anticipation of harmful actions that are neither presently occurring nor imminent.”⁸³ In realist literature, the typical reason for a preventive war is to steady the balance of power amongst states, especially as one nation threatens to rise above the others. The typical example of a balancing preventive war is the War of Spanish Succession in 1701, in which several European powers allied against France when it threatened to create a unified Franco-Spanish state.⁸⁴ A pre-emptive strike, on the other hand, is one in which the state is in imminent danger and waiting to act can only intensify the risk.⁸⁵ In his seminal book on just war theory, Michael Walzer offers up examples of acts that can spark a pre-emptive strike, including mobilizations, border incursions, and naval blockades, and cites the 1967 Israel attack of Egypt in response to Egypt’s Sinai troop mobilization as a pre-emptive strike.⁸⁶

When following the logic of offense-defense theory, both preventive wars and pre-emptive strikes become more likely when states desire to fight an offensive conflict instead of a defensive conflict.⁸⁷ In a preventive war, the belligerent nation senses that a war is inevitable, though no direct hostilities or threatening maneuvers have occurred. In the case of a pre-emptive strike, a threatened nation senses a shortened timeline and must hasten to seize the initiative if it prefers an offensive strategy. In a world in which militaries prefer offensive strategies, the actors have an incentive to undertake preventive wars or pre-emptive strikes. This incentive exists because any failure to seize the initiative and pre-empt a threatening adversary may cause the threatened state to be forced into fighting a defensive war when it prefers an offensive war.

⁸³ Allen Buchanan and Robert O. Keohane, “The Preventive Use of Force: A Cosmopolitan Institutional Proposal,” *Ethics & International Affairs* 18, no. 1 (2004): 1, <https://doi.org/10.1111/j.1747-7093.2004.tb00447.x>.

⁸⁴ Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, Fourth ed. (New York: Basic Books, 2006), 76–80.

⁸⁵ Walzer, 80–82.

⁸⁶ Walzer, 81–85.

⁸⁷ Snyder and Lieber, “Defensive Realism,” 174–79.

4. Offense-Defense Theory: Definition and Balance

These concepts build a definition of the offense-defense theory. As defined in this thesis, the theory predicts that states are *prone to aggression* when their leaders perceive that conditions favor an offensive military strategy.⁸⁸ Conditions that favor an offensive strategy are those that make offensive actions appear more effective or dominant than defensive actions, or vice versa.⁸⁹ These two possible conditions represent the two ends of the offense-defense balance: actors prefer either offensive or defensive strategies. When the balance favors offense, escalation is likely; when balance favors defense, actors favor the status quo.⁹⁰ Because the balance links directly to military strategy, the offense-defense theory deals with the *perceptions* of decision-makers concerning *military capability*—both theirs and their rivals—as perceptions drive strategy.⁹¹ In particular, two factors sway these perceptions: *technology and geography*.⁹² When conditions cause the balance to favor the offense, the theory indicates that a *hazardous condition* exists in the international system—an origin of war—implying that circumstances are ripe for the outbreak of war. As a result, military capability and, thus, the offense-defense balance plays a role in the stability of the international system. The implications of a more aggressive stance stemming from preferences for the offense are numerous; however, the bottom line is that *escalations are*

⁸⁸ For a definition of offense-defense theory from others, see: Quester, *Offense and Defense*, 1–2; Keir A. Lieber, “Grasping the Technological Peace: The Offense-Defense Balance and International Security,” *International Security* 25, no. 1 (2000): 71–77, <https://doi.org/10.1162/016228800560390>; Buchanan, *Cybersecurity Dilemma*, 103–06.

⁸⁹ Another phrase that is common in the offense-defense theory literature is “relative ease” of offense or defense. This phrase is more useful if the underlying assumption is that states have an overall preference for conquest or war. See, for instance: Lieber, “Grasping the Technological Peace.”; Van Evera, “Offense, Defense, and the Causes of War,” 5.

⁹⁰ Jervis, “Cooperation,” 187–211.

⁹¹ The IR scholar Shiping Tang refers to the perceptions as the “subjective offense-defense theory”: Shiping Tang, “Offence-Defence Theory: Towards a Definitive Understanding,” *Chinese Journal of International Politics* 3, no. 2 (2010): 240, <https://doi.org/10.1093/cjip/poq004>; Quester relates how offense-defense issues revolve around military capabilities: Quester, *Offense and Defense*, 2.

⁹² Jervis, “Cooperation,” 194; Quester, *Offense and Defense*, 2; Van Evera, “Offense, Defense, and the Causes of War,” 16–19; Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914*, ed. Robert J. Art, Robert Jervis, and Stephen M. Walt, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 1989), 19–22.

more pronounced.⁹³ When coupled with a balance that favors the offense, these heightened escalations couple can devolve into conflict through preventive wars or pre-emptive strikes.⁹⁴

The underlying logic of offense-defense theory stems from the notion that states avoid attacking if they believe that their attacks will fail against their opponent's defenses. This notion implies that theory rests on a set of assumptions about states and their decision-makers; namely, we expect the decision-makers to react rationally to the incentives that they encounter.⁹⁵ If they perceive their offense to be inferior to another's defense, their likelihood of attack decreases. The takeaway is that when states perceive the relative utility of either offense or defense as favoring offense, the rational expectation is that states will attack if provoked. Conversely, in a world in which defense is perceived as the dominant strategy, there is a decreased chance of aggression, thereby bringing an increased likelihood of peace.⁹⁶

Because the implications of the offense-defense balance tipping toward offense can raise concerns about international stability, it can serve as a threat indicator. When new

⁹³ Van Evera, "Offense, Defense, and the Causes of War," 7–16.

⁹⁴ Though more commonly tied to ethical discussions, preventive war and pre-emptive strike also aids analysis of the offense-defense balance, as both stem from a need to seize the initiative. Preventive war is proactive in nature while a pre-emptive strike is reactionary in nature. For a definition on preventive use of force: "Preventive use of force may be defined as the initiation of military action in anticipation of harmful actions that are neither presently occurring nor imminent." Buchanan and Keohane, "The Preventive Use of Force: A Cosmopolitan Institutional Proposal," 1; In his seminal book on just war theory, Michael Walzer defines pre-emptive strike as action taken because the state is imminent danger and waiting to act can only intensify its risk: Walzer, *Just and Unjust Wars*, 80–82.

⁹⁵ The problem of rationality is, itself, a rich and difficult problem. For instance, deterrence scholars have long debated its merits. For some of the recent works on rationality and war avoidance, see: James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995), <https://doi.org/10.1017/S0020818300033324>; Bruce Bueno De Mesquita, *The War Trap* (New Haven, CT: Yale University Press, 1981); For a sharp criticism of assuming rationality in this context, see: Janice Gross Stein, "Rational Deterrence against 'Irrational' Adversaries? No Common Knowledge," in *Complex Deterrence: Strategy in the Global Age*, ed. Thazha V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago, IL: University of Chicago Press, 2009).

⁹⁶ In his book on this theory, George Quester purveys, "a tone of approval for the defense." See: Quester, *Offense and Defense*, 208; In his seminal article, Robert Jervis applauds the "safe" nature of a defensive world: "There is no reason for a status-quo power to be tempted to procure offensive forces." See: Jervis, "Cooperation," 214.

technologies emerge and permeate the world's militaries, those technologies offer a new approach to warfare. If those new technologies offer the maximum benefit through offensive use, then we should all expect offensive use. Ergo, a warfighting marketplace saturated with offensive technology indicates a heightened threat of war; or, to it put another way, a balance that favors the offense serves as an origin of a war. Consequently, the academic and research communities often cite the offense-defense balance in the persisting debates about cyber conflict and its emerging technology. Cyber tools have shifted military strategy, and many believe that a military can best employ its tools offensively.⁹⁷ It is this concern that renews the debate about offense-defense theory.

C. THE CRITIQUES OF OFFENSE-DEFENSE THEORY

Since Jervis and Quester first brought offense-defense theory into the realist lexicon, several important critiques of the theory have emerged that call its tenets into question.⁹⁸ The first quarrel with offense-defense theory is the argument that strategy and policy cause conflict, not technology. Some prominent sources of this argument are Mearsheimer's *Conventional Deterrence* and Colin Gray's *Weapons Don't Make War*.⁹⁹ In his work, Mearsheimer assesses methods of deterrence and ultimately concludes that deterrence is probable when an aggressor decides that they must employ an attrition strategy to win, as the high cost of attrition will deter their attack.¹⁰⁰ Conversely, when an aggressor perceives that they possess the ability to achieve a rapid victory, deterrence is likely to fail.¹⁰¹ The findings of Mearsheimer's deterrence study suggest that strategy is the key to determining aggression, not perceptions of offensive dominance as dictated by technology or geography. The crux of Gray's work is similar—that weapons are

⁹⁷ See Chapter 5.

⁹⁸ For a broad brush of the ongoing critiques, see: James Davis et al., "Taking Offense at Offense-Defense Theory," *International Security* 23, no. 3 (1998), <https://doi.org/10.2307/2539342>.

⁹⁹ John J. Mearsheimer, *Conventional Deterrence*, ed. Robert J. Art and Robert Jervis, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 1983); Colin S. Gray, *Weapons Don't Make War: Policy, Strategy, and Military Technology* (Lawrence, KS: University Press of Kansas, 1993).

¹⁰⁰ Mearsheimer, *Conventional Deterrence*, 206–08.

¹⁰¹ Mearsheimer, 203.

subordinate to strategy and policy in causing war—though he does not make this argument from a deterrence standpoint.

However, the arguments of both Mearsheimer and Gray both offer a subtle admission that weapons do play at least some role in policy and strategy. A logical counterpoint to Mearsheimer and Gray is that a rapid victory is often achieved, in part, through the tools employed by the military. For example, a nation with poor weaponry is unlikely to act aggressively in the face of a well-armed nation, meaning that political goals only flow from such considerations as technology. Moreover, in a not-so-subtle admission, Gray explicitly advocates for greater urgency in developing the Strategic Defense Initiative, an anti-missile technology that he believes could increase the likelihood of peace.¹⁰² Proponents of offense-defense theory do not purport to offer the sole key to predicting war; rather, they argue that it describes a condition that makes the opportunity ripe for aggressive strategies and policy and the outbreak of war.

Another point that Gray offers as a challenge to offense-defense theory is that policy guidance and strategy guides weapon acquisition in a healthy defense architecture, not the other way around. Gray's argument contradicts one of the basic tenets of offense-defense theory by proposing that people, and not weapons, cause war.¹⁰³ To understand Gray's point, one need only observe the evolution of military technology in the United States: the U.S. government has always placed a huge emphasis on the construction of its navy, a policy that greatly impacted its technology over time.¹⁰⁴ However, a government cannot wholly guide what technologies its defense industry produces. Many of the most important military innovations have not emerged as a result of a military acquisition process; rather, disruptive technologies often emerge from the civilian world and impose great shifts in military strategy. Business scholars have long understood this concept; the demand for specific new technology does not typically produce important innovations.¹⁰⁵

¹⁰² Gray, *Weapons Don't Make War*, 83.

¹⁰³ Gray, 65–66.

¹⁰⁴ Weigley, *The American Way of War*, 42, 59, 167, 82, 370.

¹⁰⁵ Paul Geroski, *The Evolution of New Markets* (New York: Oxford University Press, 2003), 21–57.

Rather, it is the “supply-push” of innovations that typically yields the most important breakthrough and disruptive technologies.

In other words, the military’s articulated demand for certain weapons rarely results in momentous swings of strategy—including preferences for offense or defense.¹⁰⁶ Martin van Creveld highlights this phenomenon, underscoring how all major military innovations of the nineteenth century and most of those in the twentieth century emerged from the minds of civilians and not from a military requirements document.¹⁰⁷ For instance, international governments did not foresee the advent of nuclear fission before two German civilians—Otto Hahn and Fritz Strassman—discovered the process in 1939. They discovered nuclear fission while working in an academic setting apart from the direction of the German government.¹⁰⁸ Likewise, consider the demands of the Reagan and Bush Administrations for the Strategic Defense Initiative, which was a demand for a specific technology: it failed to yield meaningful counter-missile technology—a point bemoaned by Gray himself.¹⁰⁹ In the end, technologies can come from a variety of sources, and while policy and strategy can play a hand in the development of technology, the opposite effect can occur, as well.

Another important critique of offense-defense theory is that the properties ascribed to weapons by offense-defense theorists (referred to as variables in this thesis) do not necessarily assist the offense or the defense. This critique of offense-defense theory is compelling because it undermines the notion that decision-makers perceive military capability to be a result of technological and geographic factors—a core argument in this thesis. To understand this critique, we turn again to Mearsheimer, who attacks this

¹⁰⁶ Geroski, Chapter 2.

¹⁰⁷ Martin van Creveld, *Technology and War: From 2000 B.C. to the Present*, Revised and Expanded ed. (New York: The Free Press, 1991), 220.

¹⁰⁸ Hahn and his collaborators, Lise Meitner and Fritz Strassmann, worked at the Kaiser Wilhelm Society and resisted Nazi inducements to join any Socialist groups. His group also collaborated with many universities in Allied nations. See: Otto Hahn, *Otto Hahn: A Scientific Autobiography*, trans. Willy Ley (New York: Charles Scribner’s Sons, 1966), 137–80.

¹⁰⁹ Gray, *Weapons Don’t Make War*, 83.

underlying assumption of offense-defense theory by raising the dubious effects of mobility on the balance: “[I]t is not clear that mobility favors the offense; in fact, we might argue that mobility favors the defense ... It is not essential that the offense have highly mobile weapons to effect surprise—provided its movements can be concealed from the defense. Because the defense places a premium on rapid reaction to move its forces to meet the attacker in those initial battles, it requires highly mobile forces.”¹¹⁰ Mearsheimer’s general attack on the offense-defense theory is problematic for a few reasons. First, the offense-defense balance is a matter of perceptions, and the perceptions that some technologies grant the ability to seize the initiative are what tip the balance, not a practical assessment from any analyst. Mearsheimer attacks mobility (which this thesis ultimately discards as a variable – see Chapter III), though at the time of mobility’s inclusion in offense-defense theory, many strategies were emerging that reflected a perception that mobility impacted strategy a certain way. For instance, the U.S. procurement of mobile capabilities has allowed it to export war off the North American continent, allowing it to participate in more inter-state wars than any other country since the end of WWII.¹¹¹ Further, the offense-defense balance is a net sum of the factors impacting military strategy, not any one factor. Confusion about a particular factor may simply boost another factor’s ability to impact the perceptions that define the balance.

Perhaps the most significant critique of offense-defense theory is that the balance cannot be measured in any appreciable way. If, in fact, the offense-defense balance cannot be measured, then it cannot offer insights into the current threat levels of the international system, implying that the theory lacks practical value. The overriding argument of this thesis is that measuring the offense-defense balance may be difficult; however, it can be assessed through an analytical framework. By knowing those key factors and their pertinent variables, an analysis of the offense-defense balance can offer keen commentary on the

¹¹⁰ Mearsheimer, *Conventional Deterrence*, 25–26.

¹¹¹ To garner a sense of the investment in mobility made by the United States, see: “Chapter Two: Comparative Defence Statistics,” *The Military Balance* 120, no. 1 (2020): 21–27, <https://doi.org/10.1080/04597222.2020.1707962>; Meredith Reid Sarkees and Frank Wayman, “Resort to War: 1816–2007,” in *Correlates of War* (Washington, DC: CQ Press, 2010), <http://www.correlatesofwar.org/data-sets/COW-war>.

present state of conflict in the international system and the resulting likelihood of increased escalations. Nevertheless, it is important to address the criticism directly: can one measure the offense-defense balance? This question has been addressed by past offense-defense theory advocates. Sean Lynn-Jones concedes that it is difficult; however, that is because it is a perception-based theory¹¹² He posits that analysis at the unit-level must be included when analyzing these perceptions. Measuring or assessing may pose a challenge; however, that does not negate the underlying theory.¹¹³ It simply means that either we must conduct the difficult measurements or engage in the abstract thought necessary to determine the threats in our international system.

D. CUTTING THROUGH THE NUANCE OF OFFENSE-DEFENSE THEORY

Despite the criticism, the offense-defense theory remains a valuable tool in identifying conditions that incite conflict. However, the definition of the offense-defense theory in this thesis does not align perfectly with the literature. Instead, this thesis pairs away much of the excessive complexity that plagues the theory and leaves it unable to analyze modern conflict. Though a nuanced understanding of problems is often beneficial for practical problems, a nuanced approach to theoretical development can, at times, produce excessive complexity, as it has in the case of the offense-defense theory. Theory is meant to identify generalities and organize difficult problems in a way that aids analytical thinking.¹¹⁴ Excess complexity in a theory leaves the theory in state that can only contend with very specific problems, and aligning new problems with the theory becomes a difficult exercise. Despite the complexity within offense-defense theory, its sound logic rings through in discussions surrounding cyber conflict, thereby demanding that the theory not fold under harsh criticism or theoretical complexity. Hence, for this thesis to analyze the

¹¹² Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4, no. 4 (1995): 670–82, <https://doi.org/10.1080/09636419509347600>.

¹¹³ Lynn-Jones, 679–80.

¹¹⁴ In relation to IR theory, Waltz sums up this idea nicely: "A theory is a depiction of the organization of a domain and of the connections among its parts ... theory isolates one realm from all others in order to deal with it intellectually": Waltz, "The Origins of War," 615.

cyber offense-defense balance, it is essential to cut through this nuance and discard the axioms of the theory that hinder analysis.

1. The Divide Between Perception and Reality

One of the first issues that befuddles the offense-defense theory is the divide between perception and reality, which creates a parallel version of the offense-defense balance that distracts from the issue of avoiding war.¹¹⁵ In the simplest terms, the distinction is this: perceptions lead to war, while the reality dictates how the war proceeds. Numerous scholars point to World War I (WWI) as one of the prominent examples of this dissonance.¹¹⁶ A widely held conclusion among historians is that military doctrine throughout Europe at the onset of WWI upheld offensive strategies as the “silver bullet” of war, including in Germany.¹¹⁷ By attacking first, the Germans believed that they would gain the upper hand; their perception that offense was dominant caused them to initiate the war. However, those beliefs proved tragically incorrect as numerous troops subsequently found themselves embroiled in dismal trench warfare conditions. This tragic outcome often earns the WWI-era strategists and diplomats the moniker “cult of the offensive,” as many of them perceived an advantage in taking the offensive only to find themselves in a reality dominated by the defense.¹¹⁸

This example raises the issue at hand: should offense-defense theory focus on the cause of war (perception) or the likely outcome of war (reality)? In his work on offense-defense theory, Van Evera attempts to bridge this divide by positing that the theory can be

¹¹⁵ In his article, Tang refers to this divide as the “subjective” and “objective” versions of the offense-defense balance, respectively; Tang recommends against the objective version: Tang, “Offence-Defence Theory,” 216.

¹¹⁶ Arquilla, “From Blitzkrieg to Bitskrieg,” 61–62; Singer and Friedman, *Cybersecurity and Cyberwar*, 153–54.

¹¹⁷ Snyder, *The Ideology of the Offensive*.

¹¹⁸ Stephen Van Evera, “The Cult of the Offensive and the Origins of the First World War,” *International Security* 9, no. 1 (1984), <https://doi.org/10.2307/2538636>; Arquilla, “From Blitzkrieg to Bitskrieg,” 61–62.

thought of with “two parallel variants: real and perceptual.”¹¹⁹ By proposing this version of the theory, Van Evera suggests that there are two versions of the offense-defense balance, and both serve a keen purpose. The perceptual balance is how actors subjectively view offensive and defense strategies, while the real balance denotes which of the two is objectively stronger, or actually prevails in conflict. Van Evera makes the case that both version of the balance offer value by pointing out that states overestimate the danger that faces them (perception) and undertake corresponding offensive actions that sparks balancing behavior amongst the state’s opponents, resulting in disaster for the offensive state (reality).¹²⁰ Hence, Van Evera argues, by knowing that a state’s perceptions can lead to unnecessary wars, the parallel versions of the offense-defense balance can help calm aggressive states. In general, he arrives at this assessment through a historical analysis.¹²¹

However, such attempts to create two versions of the offense-defense balance are counterproductive, and this thesis rejects the reality-based version for three reasons. First, the reality-based version serves no practical purpose because it does not clarify how states may interact in the international system. To build a theory that presages war, and because war stems from perceptions, the offense-defense theory must focus on the perceptions, not the reality.¹²² An analysis of present realities is, at best, an estimate, and it is only in

¹¹⁹ Van Evera, “Offense, Defense, and the Causes of War,” 6.

¹²⁰ “History suggest that offense dominance is at the same time dangerous, quite rare, and widely overstated ... States are seldom as insecure as they think they are.” Van Evera, “Offense, Defense, and the Causes of War,” 42; Jack Levy presents a historical overview of the offense-defense balance and where it resided, in reality: Jack S. Levy, “The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis,” *International Studies Quarterly* 28, no. 2 (1984): 230–34, <https://doi.org/10.2307/2600696>.

¹²¹ “History suggest that offense dominance is at the same time dangerous, quite rare, and widely overstated ... States are seldom as insecure as they think they are.” Van Evera, “Offense, Defense, and the Causes of War,” 42; Jack Levy presents a historical overview of the offense-defense balance and where it resided, in reality: Levy, “The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis,” 230–34.

¹²² “The theory ultimately aims to explain decision to initiate war; what matters is leaders’ expectations of final war outcomes based on their perceptions of the strategic balance.” From: Lieber, “Grasping the Technological Peace,” 74; Rather than overemphasizing time pressures for preemption, the cult of the offensive literature claimed that the perceived feasibility of the offensive increased Germany’s incentive for preventive war,” from: Snyder and Lieber, “Defensive Realism,” 177; “With offense-defense balance it is perception, not reality, that is important.” From: Buchanan, *Cybersecurity Dilemma*, 104.

hindsight that the reality becomes clear. Second, as Shiping Tang emphasizes, constructing a useful reality-based balance *ex ante* requires an analyst to make calculations based on pre-conditions that typically prove unreliable.¹²³ Specifically, these pre-conditions are that opponents must possess the same technology as each other and universally deploy that technology in an optimal fashion during a possible war to make objective analysis accurate.¹²⁴ Because war proceeds with imperfect humans, these pre-conditions are mere assumptions that make the reality-based balance inaccurate.¹²⁵ Third, a whole range of factors determines the final outcome of war—not solely the relative balance of offense and defense. An incomplete list of such factors may contain strategy, alliances, or leadership.¹²⁶ Even happenstance can impact the direction of war, including disease or weather. While determining the reality offers an alluring exercise, it is at once encumbered with endless complexities and does not provide the desired outcome of determining how opposing states are likely to react in a crisis.

While Van Evera provides valuable insights into the implications of the offense-defense balance, his attempts to create a reality-based version of the balance are impractical and suffer logical flaws. To be effective, theorists can best employ the offense-defense theory by focusing on perceptions, as it is these perceptions that can fuel further war. As conditions arise sparking offense-prone strategies, the offense-defense theory can coherently identify a dangerous situation that can heighten international escalation. Viewing the offense-defense balance as a problem rooted in perception also serves a practical purpose, as it facilitates bargaining and cooperation. When diplomats understand how perceptions may incite aggressive behavior, they can work toward conditions that enable cooperation between states. In sum, offense-defense theory must provide a coherent description of the conditions in international politics, and though historical realities may feed the perceptions, the perceptions themselves are the condition.

¹²³ Tang, “Offence-Defence Theory,” 231–32.

¹²⁴ Tang, 231–32.

¹²⁵ Tang, 231–32.

¹²⁶ Tang, 237.

2. Excess Factors Attributed to the Offense-Defense Balance

Another obstacle hindering the offense-defense theory is that theorists have sought to apply an assortment of factors that may impact the offense-defense balance, sparking a debate about which factors are pertinent to military capability and strategy.¹²⁷ However, two factors consistently emerge in the literature: technology and geography; these are the two factors on which this thesis proceeds.¹²⁸ Though the next chapter further explores technology and geography, it is worth briefly defining both at this stage. Technology is the sum of devices, components, practices, and skills meant to fulfill a human purpose, while geography is the spatial considerations of the operational environment (OE).¹²⁹ In terms of war, the human purpose for developing technology is typically some advantage for its user, such as eliminating an adversary's capabilities or maneuvering into an advantageous position. As new technologies enter the fray—particularly, “breakthrough” or “disruptive” technologies—the world's militaries find themselves competing or fighting in ways previously unimagined, such as through cyberspace.¹³⁰ Cyber conflict involves competition beyond the traditional battle geometries, drawing opposing sides into a battle for control of the information fed to their respective populations. Thus, technology can change the basic form of warfare, sometimes rendering a whole mode of warfighting obsolete. These events can cause a new warfighting paradigm to emerge, sparking a shift

¹²⁷ Lieber, “Grasping the Technological Peace,” 75–77.

¹²⁸ Jervis, “Cooperation,” 194; Quester, *Offense and Defense*, 2; Van Evera, “Offense, Defense, and the Causes of War,” 16–19; Snyder, *The Ideology of the Offensive*, 19–22; Keir Lieber argues that adding geography as a factor confuses the theory: Lieber, “Grasping the Technological Peace,” 75–78.

¹²⁹ See chapter three for the trove of citations that it took to arrive at those definitions.

¹³⁰ For definitions and a view into disruptive technologies, see: Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Revised ed. (Boston, MA: Harvard Business School Press, 1997), xviii; For an overview of breakthrough technologies, see: Mark Stefik and Barbara Stefik, *Breakthrough: Stories and Strategies of Radical Innovation* (Cambridge, MA: MIT Press, 2004), 3; To understand the interaction of disruptive, breakthrough technologies, and the military, see: Tai Ming Cheung, Thomas G. Mahnken, and Andrew L. Ross, *Assessing the State of Understanding of Defense Innovation*, (San Diego, CA: The Study of Innovation and Technology in China, 2018), 3–5, <https://escholarship.org/uc/item/3wt3613v>.

in military doctrine as a result.¹³¹ An important component of the new strategies is the preference for offense or defense. It is at this point that geography and its overlap with new technologies impact how these changes give rise to preferred warfighting strategies. For instance, the geography of Europe greatly impacted the offensive use of the tank at its advent. Had the geography of Europe evolved differently or involved less forgiving terrain features, its leaders may have perceived new technologies, like the tank, differently.

The need to focus offense-defense theory exclusively on technological and geographical factors emanates from a core tenet of offense-defense theory—that it hinges on military capability, as capability feeds strategy. A specific factor that fails to inform strategy is “social and political order,” which Van Evera suggests is an important factor in determining perceptions of the balance.¹³² He makes this argument primarily by proposing that popular regimes can raise loyal forces capable of fighting an offensive war. However, social and political order do not directly feed military strategy, and a quickly-raised army can still be raised for either offensive or defensive purposes. Hence, this factor does not inform the balance. On the other hand, technology and geography represent factors that drive military strategy and, therefore, guide how a country with high social and political order would utilize its army, once raised. For instance, if an army’s technology centers on waiting and counter-attacking, the balance drives the state to a defensive strategy. Moreover, Van Evera admits that unpopular regimes are just as prone to assume offensive strategies as popular regimes, making it unclear how the regime sways the balance.¹³³ Unpopular regimes, much like popular regimes, can incite offensive behavior as foreign opponents may choose to foment subversion within the borders of the unpopular regime, sparking aggression between both countries. In sum, the additional factors can confuse the analysis of the offense-defense balance.

¹³¹ To garner a sense of a warfighting paradigm, see: John Arquilla and David Ronfeldt, “A New Epoch—and Spectrum—of Conflict,” in *In Athena’s Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997).

¹³² Van Evera, “Offense, Defense, and the Causes of War,” 19–20.

¹³³ Van Evera, 20.

Furthermore, avoiding extraneous factors helps achieve a level of parsimony that allows for a robust theory. The political scientist Keir Lieber makes a keen point that sticking to what he calls the “core version” of offense-defense theory achieves a level of parsimony: “[T]he core version makes for a much more parsimonious theory than the broad version ... Adopting the broad balance renders offense-defense theory atheoretical; it becomes a grab bag of variables employed in a purely post hoc descriptive enterprise.”¹³⁴ A factor that appears extraneous is that of “diplomatic factors,” which Van Evera raises to bring in the concept that alliances can impact the offense-defense balance.¹³⁵ In terms of the logic, Van Evera is correct, as alliances impact the balance through presenting aggregate forces that may discourage offensive strategies.¹³⁶ However, in the interest of building a parsimonious theory that does not exclude other entities, including non-state, diplomatic factors and alliances is best subsumed by geography. Geography aptly covers the spatial and social-political factors that play into alliances and encourages analysts to gain insights into the offense-defense balance.

Where this thesis departs from Lieber’s quest for parsimony is that he proceeds with a “core version” of offense-defense theory that only includes technological impacts. Though his narrowed version does simplify analysis, it ignores the vital factor of geography in formulating offensive or defensive strategies. For instance, geography played a monumental role for Britain during World War II (WWII) and impacts the world today in theaters such as the Arctic Ocean. To get a sense of the impact that geography had on Britain in WWII, one need only need to consider how its defensive air war helped stave off the Luftwaffe at the height of the 1940 Battle of Britain.¹³⁷ The Luftwaffe had attained a reach of about one hundred miles inland of Great Britain and devastated London in the process. However, Britain ultimately leveraged its strategic position across the English Channel along with its early warning RADAR system to scramble the British Fighter

¹³⁴ Lieber, “Grasping the Technological Peace,” 77.

¹³⁵ Van Evera, “Offense, Defense, and the Causes of War,” 21–22.

¹³⁶ Van Evera, 21–22.

¹³⁷ Posen, *The Sources of Military Doctrine*, 96.

Command each time that the Luftwaffe was inbound. Absent the English Channel, Germany may have launched a blitzkrieg-style invasion of Great Britain in 1940, or the British military may have pursued strategy other than building the defensive capability in its Fighter Command. In present times, the strategic importance of geographically-blessed locations, such as Greenland, continue to influence states to adopt offensive or defensive strategies.¹³⁸ Among other locations, the United States positioned key early warning devices on Greenland in the height of the Cold War to strengthen its defensive missile posture against Soviet Russia.¹³⁹ To not include geography in offense-defense theory would bypass a vital factor in the perceptions of either offensive or defensive dominance.

3. Distinguishing Between Offense and Defense—Not Pertinent to the Balance

Perhaps, one of the greatest stumbling blocks of the offense-defense theory is the attempts to distinguish between an offensive posture and a defensive posture, an issue raised by Jervis in his canonical work on the theory. While distinguishing between offense and defense does have its uses, including crisis diplomacy, it does not aid in examining the offense-defense balance. In other words, it is a separate—though parallel—in determining whether escalatory behavior is likely. Because the fundamental purpose of offense-defense theory is to signpost when the offense-defense balance favors the offense—thereby identifying a hazardous condition in the international system—attempts to distinguish between postures only complicates the theory. Because it does not extend to perceptions of dominance and, therefore, does not impact the balance, this thesis does not consider it in any analysis of the offense-defense balance.

Distinguishing between offensive and defensive postures does help explain the interaction of cooperation, the security dilemma, and military conditions—the principal purpose of Jervis’ work. Jervis divides offense-defense theory into two main variables: the

¹³⁸ J. B. Pranow, *Greenland and its Strategic Importance*, AD-A137 433 (Washington, DC: Naval Intelligence Support Center Translation Division, 1983), 508, <https://apps.dtic.mil/docs/citations/ADA137433>.

¹³⁹ Pranow, *Greenland and its Strategic Importance*, 507–10.

advantage of either offense or defense (determining which is stronger) and the ability to distinguish between the two.¹⁴⁰ He sums these variables into the “four worlds” that can result from the different permutations of these variables, as shown in Figure 2. As states procure new weapons that are versatile—meaning that they can serve either an offensive or defensive purpose—their rivals invariably assume that the weapon is offensive, regardless of the true intentions. The logic behind this is clear, as rivals are prone to assuming the worst-case scenario, and offensive intentions represent the worst case. As a result, new weapons that ostensibly serve a defensive role, yet offer offensive capabilities, leave rivals feeling threatened as they assume that the underlying purpose is nefarious. Consider, for example, a fighter aircraft: a nation may choose to purchase a fleet of fighter aircraft under the auspices of securing their sovereign airspace, which is a defensive posture, by using the fighters in an interceptor role. Unfortunately, fighter aircraft also fill a vital role in offensive operations. In Offensive Counterair Operations (OCA), for instance, fighters conduct a “fighter sweep,” meaning that they project forward to gain air superiority through destroying airborne targets of opportunity and denying an adversary use of the air.¹⁴¹ Posturing a nation with fighter aircraft, no matter the intent, signals the possibility of offensive actions to a rival, which can appear threatening to that same rival. What are the implications of an indistinguishable posture? Already, it is clear that an indistinguishable posture may complicate cooperation between rivals due to misunderstood signals. Jervis also stresses that the ability to distinguish between offense and defense is an essential factor in containing the security dilemma. Without a clear distinction in postures, the chances of a spiraling arms race and escalations are high.¹⁴² As weapons or policy are produced that can serve either an offensive or defensive role, their activation may arouse the suspicion of an impending attack.

¹⁴⁰ Jervis, “Cooperation,” 199–201.

¹⁴¹ U.S. Air Force, *Air Force Doctrine Annex 3–01: Counterair Operations* (Maxwell AFB, AL: Lemay Center for Doctrine, 2019), 8–10, <https://www.doctrine.af.mil/>.

¹⁴² Jervis, “Cooperation,” 199–201.

	Offense has the advantage	Defense has the advantage
Offensive posture <i>not</i> distinguishable from defensive one	1 Doubly Dangerous	2 Security dilemma, but security requirements may be compatible
Offensive posture distinguishable from defensive one	3 No security dilemma, but aggression possible. Status-quo states can follow different policy than aggressors. Warning given.	4 Doubly stable

Figure 2. The “Four Worlds” as Re-created from Jervis’ 1978 Article¹⁴³

While distinguishing postures may help provide insights into the security dilemma and crisis diplomacy, it does not directly impact the balance of offense and defense. For instance, consider world number two from Jervis’ “four worlds.” If Jervis’ model is correct, the security dilemma predicts that arms races would occur, implying that escalation can occur even if world leaders consider defense to be the dominant strategy.¹⁴⁴ While true, world number two includes the perception of defense being the dominant strategy. As long as world leaders believe their offense inferior to their opponent’s defense, the balance favors defense, meaning that the balance predicts diminished chances of war, even if posturing or signaling fails. Adding distinguishability merely confuses the balance. World number three is the other condition that warrants discussion; in world three, posturing is evident but the balance favors offense and, therefore, aggression. In this world, Jervis highlights the dangers associated with an offensively-dominated balance: “[E]ven a status-quo state may take the initiative rather than risk being attacked and defeated.”¹⁴⁵ Thus, signaling may prove effective. However, signaling represents a separate issue from the balance, which predicts a state’s preference for aggression when its leaders perceive a dominance of offensive strategies.

¹⁴³ Source: Jervis, “Cooperation,” 211.

¹⁴⁴ Jervis, 212.

¹⁴⁵ Jervis, 213.

Further, attempting to categorize weapons as offensive and defensive has historically proven a fruitless endeavor. The history of warfare is pockmarked with defensive weapons being used offensively, and vice versa.¹⁴⁶ Further, diplomatic efforts to limit purely offensive weapons have mainly been in vain, as with the 1932 Disarmament Conference.¹⁴⁷ Weapon differentiation amounts to an insurmountable task that is subjective and suffers from logical flaws, as covered in the introductory literature review. In sum, this thesis does employ weapon and posture differentiation as impactful to the offense-defense balance, instead, pursuing a perception-based approach outlined in Chapter III.

E. CONCLUSIONS

The final section of this chapter discards the complexity that riddles the offense-defense theory, leaving behind a version of the theory that analysts can apply to modern forms of conflict. The complexity that plagues the offense-defense theory stems from an overly-nuanced approach that theorists adopted during theory development. This chapter pairs down three particular axioms that befuddle the theory: the reality-based balance, excess factors impacting the balance, and issues of distinguishability.

The result of paring down the offense-defense theory is a theory that focuses on the core items that presage conflict in terms of offense and defense: perceptions, the balance, and military strategy that arises from technology and geography. Fundamentally, offense-defense theory is a descriptive theory, much like the other theories that persist in realism.¹⁴⁸ That is, it helps to describe conditions that, when met, generate predictions in international politics. Generally, when the conditions suggest that offense is dominant, opponents are incentivized by this imbalance and are prone to aggressive behavior. The ideas of preventive war and pre-emptive strikes also aid analysis, as these events can emerge when opponents prefer offensive strategies. Conversely, when conditions cause

¹⁴⁶ van Creveld, *Technology and War*, 177.

¹⁴⁷ Boggs, *Attempts to Define and Limit*, 93.

¹⁴⁸ For a sample list of realist theories, see: Wohlforth, "Realism," 141–43.

actors to favor the defense, these same opponents to suppress the urge to adopt aggressive behavior and instead favor the status quo. In short, when striking first appears to yield an advantage, the allure to do so will increase the probability of conflict.¹⁴⁹ The balance of offense and defense is impacted by technology and geography, and those factors sway perceptions of international statesmen. Factors outside of technology and geography may arise that may impact these perceptions; however, such factors are typically subsumed by technology and geography. Finally, offense-defense theory does not directly address the objective reality of either offensive or defensive strategies; it simply deals in the perceptive balance of offense and defense, as perceptions incite aggressive behavior amongst statesmen and military leaders.

Offense-defense theory continues to find appeal amongst scholars, as it aptly describes an origin of war. However, before applying the theory to cyber conflict, the array of views surrounding offense-defense theory necessitated an inquiry into the theoretical underpinnings of the theory. To conduct this inquiry, this chapter has delved into the roots and concepts of offense-defense theory and, importantly, cuts through the nuance that has grown to befuddle it. In the end, a few important conclusions emerge: offense-defense theory must link to the offense-defense balance, which represents an aggregate of individual perceptions about military capability and whether offensive or defensive strategies are dominant. The version of the offense-defense theory in this chapter leads to an explanatory theory that predicts when conflict may be likely.

As mentioned, this thesis does not further address how offense-defense theory fits with other theories of international relations. Rather, this thesis seeks to analyze our tools of war and the modern modes of conflict—chiefly in cyberspace. Offense-defense theory may have emerged from the realist movement and IR discipline; however, its applications vastly overlap with those of war practitioners. Those in the military must understand how their technology sways their perceptions, which, in turn, sways their actions. In pursuit of

¹⁴⁹ In his work on strategy through the lens of an economist, Thomas Schelling discusses this scenario as it relates to the problem of “surprise attack.” Thomas C. Schelling, *The Strategy of Conflict*, 1980 Paperback ed. (Cambridge, MA: Harvard University Press, 1960), 207–29.

this understanding, the next few chapters aim to distill the pertinent technological and geographical factors that can tip the offense-defense balance.

III. THE CONDITIONS THAT TIP THE BALANCE: THE CURRENT THEORY REVISITED

Hence the overall numerical relationship between the total force of the offense employed in the breakthrough attempt, and the total defending force holding the full frontage, is irrelevant to the outcome.

—Edward *Luttwak*, “The Operational Level of War”¹⁵⁰

The previous chapter hones the definition of offense-defense theory and sorts through the nuance that leaves the theory difficult to apply. If a theory purports to identify conditions provoking war, much as the offense-defense theory does, it also ought to identify those conditions. Otherwise, the theory loses credibility as any scenario can fit its criteria. This chapter moves to study the variables impacting the offense-defense balance. In other words, what technological and geographic properties can tip the balance in favor of offense or defense? By identifying and defining these variables, future research can leverage the variables to understand whether emerging conditions incentivize offensive strategies.

To formulate a new approach that other theorists have yet to undertake, this chapter conducts a sweeping assessment of the offense-defense literature that explores what variables sway the offense-defense balance. The purpose is to distill the pertinent technological and geographic variables across different modes of warfare that best predict whether states view either offensive or defensive strategies as dominant. Collectively, offense-defense theorists have identified a trove of technological and geographical properties that exert a role in tipping the balance. By accumulating that effort into a coherent set of variables, an analytical framework of the offense-defense balance can emerge. This chapter presents that accumulative effort. Ultimately, the offense-defense balance tips as the result of six variables: the information advantage, decisive effects, exposure, insulation, criticality, and resilience. The overwhelming key to understanding

¹⁵⁰ Edward N. Luttwak, “The Operational Level of War,” *International Security* 5, no. 3 (1980): 70–71, <https://doi.org/10.2307/2538420>.

these variables relies a core tenet defined in Chapter II: perceptions rule the balance. Each variable only impacts the balance to the extent that military and political leaders perceive that it does.

To facilitate clear organization, this chapter proceeds in three parts. First, it explores the two factors of offense-defense theory: technology and geography, introducing a salient definition for each and briefly exploring how they evolve in the context of warfare and offense-defense theory. Next, this chapter introduces the six variables and proposes how each impacts the balance. The development of each variable is aided by four different but intertwining tests: logical judgment, doctrine, short examples, or significant arguments from the offense-defense literature. In most cases, this chapter assigns fresh terminology to each variable to overcome some of the logical barriers, especially in light of modern warfare terminology. Finally, three variables that are significant in the literature ultimately fail to offer insights into the offense-defense balance: mobility, temporary weapon potency, and counterforce versus countervalue weapons. However, these three variables appear salient at first glance, demanding an explanation for their exclusion from the variables captured in this thesis. The final output of this chapter is an analytical framework comprised of the two factors and six variables. This thesis leverages the analytical framework to provide insights in to the offense-defense balance of modern conflict.

A. THE FACTORS OF OFFENSE-DEFENSE THEORY: TECHNOLOGY AND GEOGRAPHY

Before proceeding, it is important to note the *distinction* between a variable and a factor within this thesis. The pertinent factors of offense-defense theory are technology and geography; both influence the balance of offense and defense. In terms of warfare, as technological and geographic factors evolve, the offense-defense balance tips and impacts actor preferences for either offensive or defensive strategies. The variables, meanwhile, are those pertinent aspects of technology and geography that, when altered, impact the offense-defense balance. In other words, the variables are a subset of the factors. Importantly, each variable does not fall seamlessly into the “technology” or “geography” category. On the contrary, as analysts considers each variable, they must weigh the technological and

geographical considerations that come hand-in-hand with that variable in order to assess the offense-defense balance.

Unfortunately, technology and geography are both terms that can include a breadth of material, causing many scholars to abuse both terms. Multiple definitions have surfaced in various literature, resulting in a lack of clarity. Thus, to avoid confusion, this chapter provides definitions of technology and geography. While both terms surface time and again in the gamut of academic disciplines, offense-defense theory demands that the definitions resonate from the literature on war. Thankfully, military scholars have sensed the immense importance of technology and geography, thereby developing definitions applicable to the offense-defense balance.

Furthermore, as the tipping balance of the offense-defense theory implies, technology and geography are not stagnant entities. Their ebb and flow are relatively constant, emerging in a host of fashions, causing the offense-defense balance to shift, accordingly. Understanding the course of these changes can put technology and geography into focus for offense-defense theory.

1. Technology

Though technology often signifies tools and equipment—or weapons in the case of warfare—its expanded use across academic disciplines reveals a richer definition. Technology permeates almost all aspects of human existence and, consequently, requires a broad definition. The economist W. Brian Arthur captures a wide-ranging definition of technology, noting that “technology is a means to fulfill a human purpose.”¹⁵¹ War is a human purpose, along with the host of intermediary actions that come along with it, including organizing, training, and planning. Martin van Creveld argues that the use of technology in war comes in many forms, incorporating an expansive range of processes, skills, equipment, and knowledge.¹⁵² Moreover, van Creveld stresses that an analysis of

¹⁵¹ W. Brian Arthur, *The Nature of Technology: What It Is and How It Evolves* (New York: Penguin Books, 2009), 11.

¹⁵² van Creveld refers this as a “certain kind of knowhow”: van Creveld, *Technology and War*, 1.

war-making technology must expand beyond weapons and other instruments that play a direct role in combat, as a society's broader technology—including its war-making support structure—play an important role in how that society conducts war.¹⁵³ As a society's technology evolves, so does war's relationship with technology, altering the nature of war.¹⁵⁴ To capture an array of concepts associated with technology, this thesis encapsulates succinctly defines technology as *the sum of devices, components, practices, and skills meant to fulfill a human purpose*.

Disruptive or revolutionary technologies can introduce two basic changes to war-fighting: either a Revolution in Military Affairs (RMA) or an emergence of new warfighting domains. First, many credit the DOD's Office of Net Assessment with introducing the concept of an RMA into the American dialogue in the aftermath of the First Gulf War.¹⁵⁵ The central idea of an RMA is that the use of new technologies or innovations reaches a point at which profound changes emerge in the overall conduct and character of war.¹⁵⁶ The business literature typically refers to distinct technologies that produce such revolutionary breaks as “disruptive technologies,” as such technologies cause consumers to depart from their established values and norms, thereby adopting new preferences or orientations.¹⁵⁷ Military literature has adopted this terminology, broadening the concept to include architectural breakthroughs (those that impact doctrine or organizations) and technological breakthroughs (those that alter a military's preferences for various technical

¹⁵³ van Creveld, 1–5.

¹⁵⁴ A similar idea is captured by the concept of military technical revolutions, a term that largely began with this article: Andrew F. Krepinevich, Jr., “Cavalry to Computer: The Pattern of Military Revolutions,” *The National Interest*, 1 September 1994, <https://nationalinterest.org/article/cavalry-to-computer-the-pattern-of-military-revolutions-848>.

¹⁵⁵ The leading personality at the ONA was Andrew Marshall, and many credit one of his Defense Memorandums for bringing RMA to American defense literature: Andrew W. Marshall, *Some Thoughts on Military Revolutions (Second Version)* (Washington, DC: Office of the Secretary of Defense, 1993), <https://stacks.stanford.edu/file/druid:yx275qm3713/yx275qm3713.pdf>; One of the leading academic articles on RMA: Krepinevich, “Cavalry to Computer: The Pattern of Military Revolutions.”; Adamsky, *The Culture of Military Innovation*, 2, 65.

¹⁵⁶ Depending on the source, an RMA may also be referred to as a Military-Technical Revolution (MTR). Gray compiles a typology of these changes: Gray, *Another Bloody Century*, 58–60.

¹⁵⁷ Christensen, *The Innovator's Dilemma*, xviii.

systems).¹⁵⁸ The literature has coined the current RMA as the Information-Technology (IT) RMA, owing to the increased emphasis on the mastery of information through C4I (command, control, communications, computers, and information) and RSTA (reconnaissance, surveillance, and target acquisition) systems.¹⁵⁹ Much like past RMAs, the IT-RMA prompts a shift in the offense-defense balance as IT has drastically reoriented the values and norms of the modern warfighter. Unfortunately, the direction of the shift poses a difficult question for military and political leaders. One of the centerpieces of the IT-RMA is the rising strife in cyberspace, a place in which the conduct of war remains an evolving puzzle.¹⁶⁰

The second fundamental change that technology can spur in warfighting is to introduce new warfighting domains, introducing further opportunities for shifts in the offense-defense balance. Domains describe where conflict can transpire and are often physical. Much of the DOD remains organized around the concept of warfighting domains, and doctrine lists the five warfighting domains: land, maritime, air, space, and cyberspace.¹⁶¹ Thankfully, listing the domains reveals the central concept; a domain is a physical space in which human activity—including war—occurs.¹⁶² More importantly, a domain offers a frame of reference for needed behaviors and capabilities, giving rise to organizations that can specialize in those needs.¹⁶³ Technology provides the ability to operate in new domains, and the nature of those tools then shapes the efficacy of offense

¹⁵⁸ Thomas G. Mahnken, “Uncovering Foreign Military Innovation,” *Journal of Strategic Studies* 22, no. 4 (1999): 4, <https://doi.org/10.1080/01402399908437768>.

¹⁵⁹ Adamsky, *The Culture of Military Innovation*, 2.

¹⁶⁰ John Arquilla and David Ronfeldt, “Cyberwar Is Coming!,” *Comparative Strategy* 12, no. 2 (1993), <https://doi.org/10.1080/01495939308402915>.

¹⁶¹ U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2019), 127, 36, 11, 98, 55, <https://www.jcs.mil/Doctrine/DOD-Terminology-Program/>.

¹⁶² To the extent that one can conceptualize cyberspace as physical.

¹⁶³ Michael C. Davies and Frank G. Hoffman, “Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?,” *Small Wars Journal*, 10 June 2013, <https://smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework>.

and defense. Though technology offers a certain mastery of the physical domains, it does not completely conquer the spatial aspects of geography.

2. Geography

Much like technology, geography can elicit a broad range of concepts depending on its contextual use. Unlike technology, however, geography tends to refer to a specific academic and professional discipline. Within the geography discipline, four distinct “traditions” have proceeded in a linear yet separate fashion over the years, causing geography’s central purpose to remain elusive.¹⁶⁴ Over the past few decades, however, the geography discipline has seen a resurgence, owed in large part to the growing interest in the intersection of the natural and social sciences, particularly, the study of human geography.¹⁶⁵ Human geography approaches social problems from a *spatial* aspect. The geographic scholar Andrew Jones writes, “Human geographers think about how things exist in space, how features of the social world change across spaces and the difference that places make to the nature of human existence. They are also concerned with the *unevenness* of human existence in space and between different places. This rests on a basic philosophical viewpoint that everything that happens in human life occurs in a certain space and time.”¹⁶⁶ Hence, geography represents the spatial features of Earth—its inhabitants and features, and its complex inter-relations.

In the context of conflict and war, military doctrine refers to such spatial features as a part of the OE, leading to a definition of geography that befits offense-defense theory. Throughout the past century, the U.S. government has seen great value in understanding geography and geospatial intelligence, including the production of an entire joint military

¹⁶⁴ For instance, the geographer William Pattison offers four areas of geographic studies: Spatial, Area Studies, Man-Land, and Earth Science: William D. Pattison, “The Four Traditions of Geography,” *Journal of Geography* 89, no. 5 (1990), <https://doi.org/10.1080/00221349008979196>.

¹⁶⁵ Andrew Jones, *Human Geography: The Basics*, The Basic Series (New York: Routledge, 2012), 2.

¹⁶⁶ Jones, 3.

publication that stresses the importance of understanding the geographic OE.¹⁶⁷ Moreover, the U.S. military leverages continental and cultural geography to simplify the expansive nature of modern military operations, dividing up operational responsibility of the globe to six Geographic Combatant Commands (GCC).¹⁶⁸ In turn, GCCs maintain the regional expertise needed to plan and conduct operations in its area of responsibility. While military doctrine refers to the OE as the combination of all conditions that impact the employment of capabilities, the spatial features of an OE specifically account for the time, space, and geo-strategic considerations.¹⁶⁹ For this thesis, *geography refers to the spatial conditions that affect the employment of military capabilities.*

Military scholars have not dwelled on geography like they did for technology, leaving those who tackle the geography room define theory. Initially, geography presents challenges that appear relatively fixed: the Pacific Ocean is likely to remain a reality throughout our lives. However, international society, political boundaries, and the shifts in valued resources all present an ever-evolving problem pertinent to the offense-defense balance. First, social geography refers to the spread and structure of human communities.¹⁷⁰ The most striking change in recent social geography is the overwhelming rise in urbanization; over four billion people—more than half the world’s population—reside in urban areas, and projections estimate that the proportion will rise to two-thirds by

¹⁶⁷ Cyril Falls, “Geography and War Strategy,” *The Geographical Journal* 112, no. 1/3 (1948), <https://doi.org/10.2307/1789151>; *National Defense Authorization Act for Fiscal Year 2017*, Pub. L. No. 114–328, Title 10 U.S.C. § 167b, 114th Congress, 2nd Session (23 Dec 2016). <https://www.govinfo.gov/app/details/PLAW-114publ328/>; U.S. Department of Defense, *Joint Publication 2-03: Geospatial Intelligence in Joint Operations* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017), vii, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

¹⁶⁸ There are a further five functional combatant commands: U.S. Department of Defense, *Joint Publication 1: Doctrine for the Armed Forces of the United States, Incorporating Change 1*, 12 July 2017 (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2013), III-7 - III-9, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

¹⁶⁹ U.S. Department of Defense, *Joint Publication 3-0: Joint Operations, Incorporating Change 1*, 22 October 2018 (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017), xv, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

¹⁷⁰ This definition is an off-shoot from the definition of human geography offered by Andrew Jones in his text: Jones, *Human Geography*, 3.

2050.¹⁷¹ Second, political geography refers to political institutions and their span of control or influence; though “political institutions” chiefly refers to states, non-state actors can also exert control over a given area.¹⁷² Political boundaries and alliances pose vastly important considerations for offense and defense; moreover, both are clearly malleable as the past decade has borne witness to a host of alliance shifts, disputed borders, and even annexation.¹⁷³ Finally, the physical location of key resources can play a vital role in decisions to undertake or forego defensive strategies.¹⁷⁴ In the traditional sense, natural resources often represent key resources; however, because natural resources do not necessarily remain critical to all actors, the geography of key natural resources are also not constants.¹⁷⁵ Furthermore, key resources in the fast-paced realm of cyberspace also represent a geographic factor that can impact the offense-defense balance. For instance, cyberspace heavily relies on Internet Service Providers (ISPs) to “carry” most all Internet traffic. Even ISPs must exist in a physical geographic space, and their location can facilitate strife in the cyber realm. Ultimately, the shifting nature of geography, albeit subtle, can come to play an important role in the offense-defense balance.

¹⁷¹ Hannah Ritchie and Max Roser, “Urbanization,” *OurWorldInData.org* (web page), ed. Oxford Martin Programme on Global Development, University of Oxford, updated November 2019, accessed 4 March 2020, <https://ourworldindata.org/urbanization>.

¹⁷² Definition drawn from Jones’ exploration into the inter-related ideas of states, nations, and culture and their overlap with geography: Jones, *Human Geography*, 62–69.

¹⁷³ On impacts to offense and defense: Van Evera, “Offense, Defense, and the Causes of War,” 21–22; As recently as 2014, Russia annexed Crimea, moving political boundaries: Michael Kofman et al., *Lessons from Russia’s Operations in Crimea and Eastern Ukraine*, RR-1498 (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1498.html; Eve Conant, “6 of the World’s Most Worrisome Disputed Territories,” *National Geographic*, 28 March 2014, <https://www.nationalgeographic.com/news/2014/3/140328-disputed-territories-geography-russia-crimea>; One of the seminal forays into alliance theory and how it shifts power can be found in the work of Stephen Walt: Stephen M. Walt, “Alliance Formation and the Balance of World Power,” *International Security* 9, no. 4 (1985), <https://doi.org/10.2307/2538540>.

¹⁷⁴ Similar definitions emerge in U.S. doctrine on “critical capability” and “decisive point”: U.S. Department of Defense, *Joint Publication 5-0: Joint Planning* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017), GL-7 - GL-8, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

¹⁷⁵ While many view oil and natural gas as vital to national security that promote “hot spots” around the world, modern innovations suggest that is only an indefinite, not a permanent, condition. To view how resources can lead to geographic “hot spots,” see: Janice Gross Stein, “The Wrong Strategy in the Right Place: The United States in the Gulf,” *International Security* 13, no. 3 (1989), <https://doi.org/10.2307/2538739>.

B. THE CURRENT VARIABLES EXTOLLED BY OFFENSE-DEFENSE THEORY

The methods of assessing the offense-defense balance within offense-defense literature reveal a lack of cohesion amongst the theorists. Furthermore, the methods of assessing the balance fail to achieve a level of generalizability. To build a sense of the current theory, Table 1 briefly summarizes the predominant variables that the literature suggests may influence the balance. Variables such as “mobility” and “firepower” may provoke powerful insights on bygone wars; however, both fail to present any useful insights in the information age. As a result, the offense-defense literature offers only negligible insights into modern warfare, particularly cyber conflict.

Table 1. Consolidated List of the Variables that Impact the Offense-Defense Balance

Variable	Aids/ Encourages	Theorist
Mobility	Offense	Quester ¹⁷⁶ Van Evera (“motorized armor”) ¹⁷⁷ Glaser and Kaufmann ¹⁷⁸
Mobility	Defense	Snyder ¹⁷⁹
Firepower	Defense	Van Evera ¹⁸⁰ Glaser and Kaufmann ¹⁸¹
Temporary weapon potency	Offense	Quester ¹⁸²
Counterforce weapons	Offense	Quester ¹⁸³
Countervalue weapons	Defense	Quester ¹⁸⁴
Second-strike capability	Defense	Jervis ¹⁸⁵ Van Evera ¹⁸⁶ Lynn-Jones (“invulnerable retaliatory forces”) ¹⁸⁷
Strategic Defense	Offense	Jervis ¹⁸⁸ Quester ¹⁸⁹
Weapons that deal with peculiarities of terrain	Defense	Quester ¹⁹⁰
Weapon vulnerability in garrison	Offense	Jervis ¹⁹¹
Fortifications	Defense	Jervis ¹⁹² Van Evera ¹⁹³
Fortification-reducing weapons	Offense	Jervis ¹⁹⁴ Van Evera (siege techniques) ¹⁹⁵
Weapons that rely on surprise	Offense	Jervis ¹⁹⁶ Snyder ¹⁹⁷
Mobilizing technology	Offense	Van Evera (mass infantry warfare) ¹⁹⁸ Glaser and Kaufmann (force size) ¹⁹⁹
Precision/ Weapon-accuracy	Defense	Mearsheimer ²⁰⁰
Precision/ Weapon-accuracy	Offense	Lynn-Jones ²⁰¹
Geographic buffer zones (rough terrain, mountains, oceans)	Defense	Jervis ²⁰² Van Evera (also urban sprawl) ²⁰³ Snyder (also narrow frontages) ²⁰⁴ Glaser and Kaufmann (emphasize narrow spaces) ²⁰⁵
Geography – flat terrain	Offense	Snyder ²⁰⁶

-
- 176 Quester, *Offense and Defense*, 3.
- 177 Van Evera, "Offense, Defense, and the Causes of War," 17.
- 178 Glaser and Kaufmann, "What Is the Offense-Defense Balance," 62–63.
- 179 Snyder, *The Ideology of the Offensive*, 20–21.
- 180 Van Evera, "Offense, Defense, and the Causes of War," 17.
- 181 Glaser and Kaufmann, "What Is the Offense-Defense Balance," 64.
- 182 Quester, *Offense and Defense*, 4.
- 183 Quester, 4–6.
- 184 Quester, 4–6.
- 185 Jervis, "Cooperation," 206–08.
- 186 Van Evera, *Causes of War*, 177.
- 187 Lynn-Jones, "Offense-Defense Theory," 675–76.
- 188 Jervis, "Cooperation," 206–08.
- 189 Quester, *Offense and Defense*, 159–62.
- 190 Quester, 4.
- 191 Jervis, "Cooperation," 196–97.
- 192 Jervis, 197.
- 193 Van Evera, "Offense, Defense, and the Causes of War," 16.
- 194 Jervis, "Cooperation," 205.
- 195 Van Evera, "Offense, Defense, and the Causes of War," 16.
- 196 Jervis, "Cooperation," 205.
- 197 Snyder, *Myths of Empire*, 4; Snyder, *The Ideology of the Offensive*, 20–21.
- 198 Van Evera, "Offense, Defense, and the Causes of War," 16.
- 199 Glaser and Kaufmann, "What Is the Offense-Defense Balance," 66.
- 200 Mearsheimer, *Conventional Deterrence*, 675–76.
- 201 Lynn-Jones, "Offense-Defense Theory," 676.
- 202 Jervis, "Cooperation," 194–95.
- 203 Van Evera, "Offense, Defense, and the Causes of War," 19.
- 204 Snyder, *Myths of Empire*, 23.
- 205 Glaser and Kaufmann, "What Is the Offense-Defense Balance," 65–66.

A possible explanation for the lack of cohesion throughout Table 1 is that offense-defense theorists never endeavored to find enduring variables that impact the offense-defense balance, instead focusing on its implications. This means that measuring the balance may not represent the important step. In other words, offense-defense theory may fulfill its purpose by simply prompting an analysis of the offense-defense balance without specifying any explicit means. However, the disagreements provoked during analysis of the cyber offense-defense balance demonstrate a clear problem with leaving the tools of analysis an open-ended question. Without a shared understanding or common terminology, the arguments made about cyber offense and defense have largely gone unheard by the outside world. This chapter aims to build generalizable offense-defense variables that can better predict the offense-defense balance.

Almost universally, offense-defense theory critics urge for a review of the theory.²⁰⁷ A prudent approach involves using the current variables of the offense-defense theory as a starting point. The past offense-defense theorists derived these variables from historical observation and analysis; therefore, the current variables offer some discerning value for offense and defense in war, and new approaches cannot discount the past literature. Therefore, the prudent approach is to re-visit the current variables of offense-defense theory and identify the enduring themes. Where do these variables hold sway? What modern parlance can clarify the taxonomy of the past? In this endeavor, the current American military doctrine serves as a useful point of reference, as it specifies key terms in modern warfare and is widely available. The following section derives new variables from the collective wisdom of doctrine and the current offense-defense literature and weighs them against logical assessment and short examples, aiming to propose variables that can better predict the offense-defense balance.

²⁰⁶ Snyder, *Myths of Empire*, 23.

²⁰⁷ Lieber, "Grasping the Technological Peace," 77–78; Gray, *Weapons Don't Make War*, 29–46; Gartzke and Lindsay, "Weaving Tangled Webs," 325.

C. THE PROPOSED VARIABLES: REFORMATTING OFFENSE-DEFENSE THEORY FOR MODERN CONFLICT

1. Variable 1. The Information Advantage: Enabling Surprise

In the context of the offense-defense balance, the information advantage *is the degree to which modern technological and geographic factors build the perception that its users either enjoy an operational advantage conferred by the flow of information or believe that they can rapidly seize such an advantage*. As technology increasingly provides the perception that it delivers an edge in the informational realm—including intelligence and manipulation of the adversary’s perceptions—it encourages a corresponding boost in a bias for the offense. In this variable, perceptions matter greatly. The reality of who enjoys the information advantage is often unknown; however, modern technology offers many enticing avenues into believing that one holds the informational edge. A true information advantage allows an organization to seize the initiative or exploit important changes in the environment—both capabilities that favor offensive actions. U.S. joint doctrine refers to the information advantage as “information superiority,” and defines it as, “[t]he operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.”²⁰⁸ By gaining and maintain an information advantage, an organization better understands the competitive environment than its adversaries allowing it to detect meaningful changes or enact change that manipulates the behavior of others.²⁰⁹

In terms of the existing offense-defense literature, the information advantage receives support, in part, from the repeated notion that surprise encourages offensive behavior. Specifically, Robert Jervis and Jack Snyder both identify surprise as a keen offensive feature, with Jervis arguing, “Weapons and strategies that depend for their

²⁰⁸ U.S. Department of Defense, *Joint Publication 3-13: Joint Operations, Incorporating Change 1*, 20 November 2014 (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2012), GL-3, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

²⁰⁹ The JCOIE focuses on the ‘security’ environment instead of the ‘competitive’ environment: U.S. Department of Defense, *Joint Concept for Operating in the Information Environment (JCOIE)* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2018), 22–30, <https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>.

effectiveness on surprise are almost always offensive.”²¹⁰ Surprise implies a known variable, such as a concealed strike or hidden capability, of which only one side has knowledge—an information advantage. At first glance, this concept struggles to pass a logical test because effective defenses also rely on the element of surprise—employing an ambush or presenting an ambiguous level of defense represents a defensive strategy of surprise, thereby aiding the defense. However, surprise defensive strategies can only shift international perceptions toward a defensive bias once they have reached what the business literature refers to as a “demonstration point.” A demonstration point denotes the time or event that reveals sufficient information about new innovations—such as defensive strategies—to the relevant community.²¹¹ Without a demonstration, a defensive strategy inherently remains an unknown, and, ipso facto, it neither encourages nor discourages perceptions about the offense-defense balance. Moreover, a defender lying in wait in an ambush is not necessarily operating with an information advantage; they do not have any idea if an attack may ever happen. This rationale implies that an information advantage logically assists seizing the initiative and going on the offensive, thereby tipping the offense-defense balance. In order to bring forth Jervis’ and Snyder’s notion that surprise impacts the offense-defense balance, this thesis considers the information advantage conferred by technology to play a role in decisions about offensive and defensive strategies—a theme that has emerged time and again in history.

Throughout history, the belief in an information advantage has played a role in persuading militaries to pursue an offensive strategy; any effort to advance the offense-defense theory must consider these events. As recent as the First Gulf War, technologies that operate on low observable principles in military aviation—more commonly referred to as stealth technology—confers an almost overwhelming offensive advantage capable of

²¹⁰ For Jervis’ quote on the impact of surprise, see: Jervis, “Cooperation,” 205; For a sampling of Snyder’s work on offense-defense theory, see: Snyder, *The Ideology of the Offensive*, 20–21; and: Snyder, *Myths of Empire*, 4.

²¹¹ In his book on military innovations, Horowitz uses the example of the First Gulf War in providing the demonstration point for precision airstrikes to the international community: Michael C. Horowitz, *The Diffusion of Military Power - Causes and Consequences for International Politics* (Princeton University Press, 2010), 15.

tipping the balances toward the offense.²¹² The ability to move or mass forces without an adversary's awareness offers enormous incentives to seize the initiative and move first against an adversary, much as U.S. stealth aircraft did in the First Gulf War.²¹³ Stealth is one of the prime examples of a technology that convinces its users that they enjoy the information advantage. Other clear examples of a perceived information advantage tipping the offense-defense balance emerge from history, including:²¹⁴

- Hannibal's renowned intelligence practices convinced him to go on the offensive and attempt to manipulate Rome's allies in the Second Punic War;
- Napoleon had what he believed to be a firm grasp on the numerical troop balance between his *Grande Armée* and the Russian army in 1812; and
- The Allies' maintained firm security over the time and place of the D-Day invasion, making an offensive response to Germany feasible.

With the dawn of cyber conflict, the information advantage becomes a virtual requirement for nearly all offensive actions. Aaron Brantly argues that all offensive cyber operations (OCO) are a form of covert action, while Gartzke and Lindsay argue that

²¹² Avionics Department, *Electronic Warfare and Radar Systems Engineering Handbook*, NAWCWD TP 8347, Fourth ed. (Point Mugu, CA: Naval Air Warfare Center Weapons Division, 2013), 1–1.19, <https://apps.dtic.mil/docs/citations/ADA617071>; G. A. Rao and S. P. Mahulikar, "Integrated Review of Stealth Technology and Its Role in Airpower," *The Aeronautical Journal* 106, no. 1066 (2002): 632–35, <https://doi.org/10.1017/S0001924000011702>.

²¹³ For instance, see the impact that stealth had on the First Gulf War: Rao and Mahulikar, "Integrated Review of Stealth Technology and Its Role in Airpower," 631; David A. Fulghum, "F-117 Pilots, Generals Tell Congress About Stealth's Value in Gulf War," *Aviation Week & Space Technology* 134, no. 18 (1991).

²¹⁴ Richard Miles, "Hannibal and Propaganda," in *A Companion to the Punic Wars*, ed. Dexter Hoyos, Blackwell Companions to the Ancient World (Malden, MA: Wiley-Blackwell, 2011); Klaus Zimmermann, "Roman Strategy and Aims in the Second Punic War," in *A Companion to the Punic Wars*, ed. Dexter Hoyos, Blackwell Companions to the Ancient World (Malden, MA: Wiley-Blackwell, 2011), 284–97; Armand de Caulaincourt, *With Napoleon in Russia*, ed. Jean Hanoteau and Goerge Libaire (Mineola, NY: Dover Publications, 2005), 2–9; Stephen E. Ambrose, *D-Day, June 6, 1944: The Climactic Battle of World War II* (New York: Simon & Schuster, 1994).

deception is a necessary part of all OCO.²¹⁵ Both covert action and deception are information-enabled operations; without skillful manipulation of the information, the operations are prone to fail. Further, the offensive cyber kill chain proffered by a Lockheed Martin white paper also underscores that once infiltrated, offensive cyber actions require continued information-exchange to avoid detection by defenders and obtain meaningful objectives.²¹⁶ Hence, cyber conflict is likely to continue with the historical trend: the information advantage bends perceptions toward the offense. Because of the historical and logical implications of the information advantage, this thesis deems the information advantage salient in determining the offense-defense balance.

2. Variable 2. Decisive Effects: The Modern Firepower

For the offense-defense balance, decisive effects *represent the degree to which technological and geographic factors generate perceptions that offensive actions are likely to nullify, undermine, or wholly overcome adversaries or their defenses*. In U.S. military doctrine, causing destruction on the enemy is more broadly referred to as “fires,” which is a term that has come to take on new meaning as a result of the changing face of warfare. Doctrine defines employing fires as, “us [ing] available weapons and other systems to create a specific effect on a target ... Fires typically produce destructive effects, but various other tools and methods can be employed with little or no associated physical destruction.”²¹⁷ This doctrinal change to focus broadly on “effects on a target” illustrates how impacting an adversary often requires a coordinated assault across a range of platforms to produce results. “Effects” stands in broad contrast to the narrow topic of destruction, which is all that is implied by “firepower.” “Decisive effects” refers to the critical nature of the effects; without the effects, the attack may fail. Further, the word “decisive” suggests

²¹⁵ Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*, ed. William W. Keller and Scott A. Jones, Studies in Security and International Affairs (Athens, GA: The University of Georgia Press, 2016), 43; Gartzke and Lindsay, “Weaving Tangled Webs.”

²¹⁶ Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, (Bethesda, MD: Lockheed Martin Corporation, 2010), 3–5.

²¹⁷ U.S. Department of Defense, *JP 3-0, Change 1*, III-30.

that any actor introducing these effects hopes to seize the initiative, creating conditions that permit mission success on the initiator's terms. In other words, the introduction of effects typically implies initiation of conflict—counter to Clausewitz's definition of defense from the previous chapter. Therefore, introducing the effects completely alters the conditions from a defense-favoring situation to one that favors the offensive action.

In general, offense-defense theorists have determined that that firepower tends to favor the defense. As used in offense-defense literature, the term firepower typically focuses narrowly on destructive effects, characterized by such attributes as explosive power, range, accuracy, and rate of fire.²¹⁸ The rationale in categorizing firepower as favoring the defense is that attacking forces tend to find themselves exposed and more susceptible to the effects of firepower, much as displayed during WWI.²¹⁹ Unfortunately, this argument runs into significant logical short-comings due to its significant utility for attacking forces. Keir Lieber, again, offers convincing arguments against the inclusion of firepower as a variable in the offense-defense balance.²²⁰ He focuses on the importance of suppressive fire, the utility of bombardments (especially pre-assault bombardments), and firepower's use in dispersing concentrations of defenders. First, suppressive fire is often necessary in advancing troops on an attack; insufficient firepower may not produce the intended effect of ceasing defensive fires during this advancement. Second, bombardments serve a number of roles, all valuable to an attacking force. It can destroy defensive positions, disrupt a defender's counter-attack plan, and pre-assault firepower eliminates threats necessary to allow an attacking force forward, similar to suppressive fire. Finally, a threatening concentration of defensive forces can find themselves scattered by effective firepower.

Furthermore, the IT-RMA and modern capabilities place firepower on an equal-footing with other effects while also reinvigorated its use in offensive actions. The emergence of cyber warfare over the past few decades poses a key coercive tool between

²¹⁸ Lieber, "Grasping the Technological Peace," 80.

²¹⁹ Glaser and Kaufmann, "What Is the Offense-Defense Balance," 64.

²²⁰ Lieber, "Grasping the Technological Peace," 80–81.

adversaries. Much as overwhelming firepower previously served as a means to quickly overcome an enemy, cyber weapons now purport to serve as a pre-emptive weapon that can undermine an enemy's defenses or simply overwhelm their forces.²²¹ Moreover, modern technology does not necessitate that the attacker be the one to run into the open during the attack. Militaries can conduct attacks from a stand-off distance while ensuring the effects through precision. Thus, this thesis flips the stance of the offense-defense literature on firepower, noting how "effects" now subsumes "fires" and serve as a tool to seize the initiative, creating perceptions of gaining offensive dominance.

3. Variable 3. Exposure: Protection, Duration, and Costs for the Attack

When determining the offense-defense balance, exposure *signifies the degree to which technological and geographic factors enable perceptions that offensive actions require the assumption of risk for the attacking units*. As the exposure required for an attack decreases, the balance tips toward the offense. Logically speaking, as the risk undertaken by the attacking units decreases, the bias for offensive action increases. To frame exposure in business terminology, if the cost of attack appears low, military and political leaders have a keen incentive to launch attacks.

While definitions of risk abound, referencing U.S. doctrine on risk provides a war-centric view. In a recent memo, the Joint Chiefs of Staff impart a pertinent definition of risk: "the probability and consequence of an event causing harm to something valued."²²² In this view, risk subsumes some of the key considerations of risk analysis—specifically complexity, uncertainty, and ambiguity—that the academic views on risk tend to hold

²²¹ John Arquilla, "The Computer Mouse that Roared: Cyberwar in the Twenty-First Century," *The Brown Journal of World Affairs* 18, no. 1 (2011): 43.

²²² The Joint Chiefs of Staff, *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3105.01: Joint Risk Analysis* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2019), B-1, <https://www.jcs.mil/Library/CJCS-Manuals/>.

separate.²²³ Ultimately, in war, societies expect their commanders to assess the risk before sending any asset on the attack; in other words, militaries conduct an analysis—however brief—of the harm that can befall those on the offensive. A key part of the analysis includes a consideration of what or who the attacking unit is, as an attacking unit purposely covers the gamut of military assets:

- A solitary person concealed by anonymity
- An aircraft laden with the latest electronic warfare countermeasures
- A valuable line of code embedded in software posing as an innocuous program

The exposure of such attacking units presents a risk as a function of the method of protection, the duration until success, and the potential loss should harm befall such assets. As technology and geography appear to mitigate these risks, the perceived strength of offensive strategies is likely to grow.

Though indirectly, several offense-defense theorists spend time writing about offensive-enabling characteristics that hints at the concept of exposure.²²⁴ For instance, the prominent offense-defense-proponent Stephen Van Evera conveys the idea that if weapons can move forward while protected through “motorized armor,” this aids the offense.²²⁵ Van Evera’s concept that protection for the attacker aids the offense neatly abides by the concept of limiting exposure during attack. His example of motorized armor illustrates the value of protection. In his book, he argues that the rise of motorized armor in the form of the tank gave rise to the offensive military doctrine of blitzkrieg during the

²²³ The Joint Chiefs of Staff, *CJCSM 3105.01*, B-6; Academic views on risk associate risk with numerical values and probabilities, while uncertainty invokes qualitative issues that can negatively impact situations: Bertrand R. Munier, “A Guide to Decision-Making Under Uncertainty,” in *Risk, Decision and Rationality*, ed. Bertrand R. Munier, Theory and Decision Library: Mathematical and Statistical Methods (Dordrecht, Holland: D. Reidel Publishing Company, 1988), 3.

²²⁴ Van Evera, “Offense, Defense, and the Causes of War,” 17; Quester, *Offense and Defense*, 4; Snyder, *Myths of Empire*, 4.

²²⁵ Van Evera, “Offense, Defense, and the Causes of War,” 17.

interwar period.²²⁶ Van Evera is not alone in citing this example: the case study of how tanks played a technological role in the origin of WWII receives frequent use in offense-defense literature.²²⁷ Unfortunately, the concept of armor has not translated well for modern forms of warfare. For instance, air warfare may rely on well-protected bases to protect its technology in garrison; however, offensive airpower tends to rely on the electromagnetic spectrum (EMS) for protection.²²⁸ Likewise, OCO do not rely on armor for protection during its offensive actions.²²⁹ It relies on intellectual tools including covert or clandestine infiltration, deception, and remaining elusive for protection.²³⁰ However, the concept is the same; the attacker seeks to limit exposure before and after offensive actions.

4. Variable 4. Insulation from Attack: Fortifications and Buffer Zones

A variable that tips the offense-defense balance toward the defense is an increase in a property that the literature refers to as insulation. Insulation *denotes the degree to which technological and geographic factors appear to either disallow or shield any defensive units or nonbelligerent objects from an adversary's attacks*. While the offense-defense literature mostly focuses on insulation as hard, or physical, barriers, this section

²²⁶ Van Evera, *Causes of War*, 162.

²²⁷ Quester, *Offense and Defense*, 139–46; Arquilla, “From Blitzkrieg to Bitskrieg,” 62; Levy, “The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis,” 233; Lieber, “Grasping the Technological Peace,” 90–94.

²²⁸ U.S. Air Force, *Air Force Doctrine Annex 3–51: Electromagnetic Warfare and Electromagnetic Spectrum Operations* (Maxwell AFB, AL: Lemay Center for Doctrine, 2019), 2–11, <https://www.doctrine.af.mil/>.

²²⁹ U.S. Department of Defense, *JP 3-12*, x-xi.

²³⁰ Gartzke and Lindsay, “Weaving Tangled Webs,” 326–27; Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, *The Diamond Model of Intrusion Analysis*, ADA586960 (Hanover, MD: Center for Cyber Threat Intelligence and Threat Research, 2013), 11, <http://www.activeresponse.org/fundamental-intrusion-analysis-reading-list>; Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict* (Kopidion Press, 2017), 96.

expands the concept to include soft barriers, as well.²³¹ Hard barriers include the physical protection afforded by fortifications, supporting populations, or geographic buffer zone, while soft barriers can include technology or strategies, such as electronic warfare, deceptive software, or “white” propaganda.²³² An important distinction exists between *insulation* and *exposure*; specifically, exposure protects units on the attack, while insulation protects everything else. Insulation ultimately limits what U.S. doctrine refers to as “drivers of risk”:²³³

- Vulnerability to the threat or hazard: the amount of harm that can be caused time frame of the harmful effects;
- Accessibility: the ease with which a hostile force or capability reach critical objects; and
- Recognition: the ease with which a hostile force or capability can identify critical objects.

While reducing these items truly does offer tangible protection from attack, the offense-defense balance is a reflection of perceptions. As each driver of risk decreases as a result of hard and soft barriers, the inducements for attack decrease, as well. Without inducements for offensive action because of heightened insulation, the offense-defense balance tips toward the defense.

The term “insulation” emerges in Van Evera’s offense-defense article in relation to physical defenses, though other theorists emphasize the physical aspects of insulation in

²³¹ Offense-defense literature on insulation: Van Evera, “Offense, Defense, and the Causes of War,” 16–19; Quester, *Offense and Defense*, 4; Jervis, “Cooperation,” 194–206; Snyder, *The Ideology of the Offensive*, 21; Snyder, *Myths of Empire*, 23; Glaser and Kaufmann, “What Is the Offense-Defense Balance,” 64–66.

²³² Unlike “black” propaganda, white propaganda openly acknowledges its source and uses gentle persuasion to sway public opinion: Central Intelligence Agency, “The Office of Strategic Services: Morale Operations Branch,” *CIA News and Information* (Featured Story), updated 30 April 2013 2010, accessed 5 March 2020, <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-morale-operations.html>.

²³³ The Joint Chiefs of Staff, *CJCSM 3105.01*, B-3.

other ways. In terms of describing the physical forms that insulation can take, Jervis, Van Evera, and Snyder all hail the importance of fortifications and geographic buffer zones.²³⁴ Fortifications imply an unmoving barrier meant to protect and house war-time assets, while a geographic buffer zone may include natural barriers (mountains or oceans) or structures produced without military intentions, such as urban sprawl.²³⁵ The offense-defense literature tends to frame these barriers as defense-enabling, focusing on how such barriers reduce the relative ease of conquest. While the literature tends to frame insulation strictly as physical protection, as opposed to a tool that alters perceptions. By expanding the variable to include soft barriers, insulation takes on a richer meaning and better encapsulates the perceptions of the offense-defense balance.

Thankfully, the literature is not wholly devoid of soft barrier concepts, as Quester provides a soft barrier example: weapons that deal with the “peculiarities of terrain.”²³⁶ For Quester, an example of a weapon that deals with the peculiarities of terrain is light firepower as wielded by a militia of local fighters.²³⁷ A force comprised of local fighters aids the defense because of their intricate knowledge of the terrain, rendering them difficult to attack and, simultaneously, potent when attacking.²³⁸ As demonstrated by Quester, less tangible barriers may support defensive aims, in addition to physical insulation. Because certain weapons or technology can play a defensive role despite not being a physical barrier underscores the point that soft technology can serve as defensive insulation, as well.²³⁹ To take Quester’s concept a step further, a supporting population may also serve as a form of insulation and tip the offense-defense balance. When armed with modern digital

²³⁴ Jervis, “Cooperation,” 194–206; Van Evera, “Offense, Defense, and the Causes of War,” 16–19; Snyder, *The Ideology of the Offensive*, 21; Snyder, *Myths of Empire*, 23.

²³⁵ Van Evera, “Offense, Defense, and the Causes of War,” 19.

²³⁶ Quester, *Offense and Defense*, 4.

²³⁷ Jervis also suggests that, “Any force that for various reasons fight well only when on their own soil in effect lack mobility and therefore are defensive:” Jervis, “Cooperation,” 204.

²³⁸ Quester, *Offense and Defense*, 4.

²³⁹ Quester’s main point is that terrain-agnostic technology tends to be offensive while technology that relies on certain terrain is defensive because it must remain in that terrain to remain effective. This chapter covers the issue of weapon differentiation later in this chapter.

technology, for instance, a supporting population can convey its strategic message with little effort, as online mobilizing platforms have given life to such social movement as the 2009 “Green Revolution” and the 2011 “Arab Spring.”²⁴⁰ As a result, the concept of insulation offers a broad stroke of how the offense-defense balance may tip toward the defense.

An important counterpoint to address is how strategic defense may aid the offense—a conspicuous anomaly within Table 1 that runs counter to the argument that increased insulation tips the offense-defense balance toward the defense.²⁴¹ Anti-Ballistic Missile (ABM) systems and the Strategic Defense Initiative (SDI) both represent prime examples of strategic defense that, as some strategists envisioned, were supposed to provide nuclear missile defense. As a result, both systems are textbook examples of insulation, as both could theoretically protect a state from foreign nuclear strikes. The argument that strategic defense tips the balance toward the offense emanates from Cold War deterrence literature, when the pervasive logic—and fear—was that any state enjoying an absolute defensive advantage could be free to conduct attacks without the concern of retaliation. This argument held considerable sway in the Cold War. Soviet Russia and the U.S. both signed the ABM Treaty in 1972, and the SDI remained a point of contention throughout the Reagan administration.²⁴² The offense-defense literature that directly addresses nuclear deterrence concurs with the concerns encapsulated by the ABM Treaty. Jervis and Quester both assert that the offense-defense theory flips in the context of nuclear deterrence: “offensive weapons are those that provide defense” in deterrence.²⁴³ Going a

²⁴⁰ Singer and Friedman, *Cybersecurity and Cyberwar*, 109.

²⁴¹ Lacking a definition of strategic defense in the offense-defense literature, the most fitting definition derives from the U.S. doctrinal definition of strategic attack, and defining strategic defense as anything that repels a strategic attack. Strategic attack is, “offensive action specifically selected to achieve national strategic objectives ... Strategic attack involves the systematic application of force against enemy systems and centers of gravity, thereby producing the greatest effect for the least cost in lives, resources, and time.” U.S. Air Force, *Air Force Doctrine Annex 3-70: Strategic Attack* (Maxwell AFB, AL: Lemay Center for Doctrine, 2017), 2, <https://www.doctrine.af.mil/>.

²⁴² William E. Burrows, “Ballistic Missile Defense: The Illusion of Security,” *Foreign Affairs* 62, no. 4 (1984).

²⁴³ The quote can be found in: Jervis, “Cooperation,” 206; Quester, *Offense and Defense*.

step further, Colin Gray actually argues that this same logic applies to conventional war, as well. He argues that inherently-defensive items, such as fortifications, can provoke offensive actions by freeing the fortified force to conduct offense without fear of attack from the fortified direction.²⁴⁴ Gray raises the WWII example of the Siegfried Line, which was a German-built defensive fortification in 1939–40 on the western front that allowed Germany to conduct offensive actions in the east.²⁴⁵ How then to conceptually deal with insulation? By some arguments, it seems to aid the offense as much as the defense. Does it not incite offensive behavior through playing the role of enabler?

The answer unfolds in two parts. First, the argument that strategic defense strictly aids the offense grew from a Cold War tunnel vision, in which bipolarity ruled the day. The offense-defense balance assesses the balance between offense and defense, *not* the balance of military capability between two actors, such as the Soviets and Americans. If one actor enjoys a vastly superior defense while its adversaries lack the same defense, clearly it may feel emboldened to strike without fear. In such a case, the world is no longer bipolar, it becomes unipolar. In a unipolar world in which the dominant actor perceives that it can project decisive effects with little risk of retaliation, offense becomes a tempting route to foreign policy goals for that dominant actor. Hence, the focus needs to remain on the balance of offense and defense, not the balance of power or a mismatch in great power capability. If both the U.S. and Russia suddenly came into possession of a strategic defense capability simultaneously in the early 1970s, the balance would have shifted to defense. Moreover, Jervis and Quester may never have published arguments that the balance becomes inverted in nuclear deterrence.

Second, the offense-defense balance is a sum of all the variables that proposed in this chapter, not any single variable. The threat of a nuclear missile strike represents such an overwhelming decisive effect, that it amplifies as the other variables shift—information advantage, exposure, and insulation. Perhaps a better way to pose strategic defense is not as a capability that boosts insulation; rather, it is a capability that impacts exposure. An

²⁴⁴ Gray, *Weapons Don't Make War*, 29–46.

²⁴⁵ Gray, 31–32.

attacking unit in a strategic attack—the state itself—assumes very little risk during an attack when protected by Strategic Defense. However, exposure can tip the balance, as well, which gives rise to a mutually assured destruction scenario, much like that of the Cold War.²⁴⁶

In terms of Colin Gray's point that conventional means of defense have found offensive uses, he chooses an odd example in the Siegfried Wall. Predominantly, historians credit the German's mastery of technology to produce decisive effects in Poland at the start of WWII—blitzkrieg with tanks—not the Siegfried Wall.²⁴⁷ Moreover, the Munich Conference in 1938 also provided Hitler with a context of France and Great Britain as Germany invaded Poland in 1939.²⁴⁸ Both had a strong preference for peace which provided the needed time for an invasion of Poland, not the Siegfried Wall.

5. Variable 5. Criticality

In the context of the offense-defense balance, criticality *signifies the degree to which targetable objects appear necessary to a population's security or welfare*. As objects grow in perceived criticality, the offense-defense balance tips toward the offense—a result of the temptation elicited by critical objects. Simply put, if an actor perceives his or her adversary is completely dependent on a certain object, that object presents a tempting target. Thus, as technology and geography create either relied-upon objects *or* avenues to target a relied-upon object, offense becomes a tempting strategy, tipping the balance toward the offense.

²⁴⁶ Many credit Donald Brennan from the Hudson Institute with coining the phrase “Mutually Assured Destruction” in this article: Donald G. Brennan, “Strategic Alternatives: I,” *New York Times*, 24 May 1971, <https://www.nytimes.com/1971/05/24/archives/strategic-alternatives-i.html>; Another way to conceptualize how arms races increases the attacker's exposure, see the “Cone of Mutual Deterrence” in: Michael D. Intriligator and Dagobert L. Brito, “Can Arms Races Lead to the Outbreak of War?,” *Journal of Conflict Resolution* 28, no. 1 (1984): 74, <https://doi.org/10.1177/0022002784028001004>.

²⁴⁷ William L. Shirer, *The Rise and Fall of the Third Reich: A History of Nazi Germany* (New York: Simon & Schuster, 1960), 625–56.

²⁴⁸ Shirer, *The Rise and Fall of the Third Reich*, 414–37; A.J.P. Taylor, *The Origins of the Second World War* (New York: Antheneum, 1962), 190–91.

To weigh “criticality” in the context of the offense-defense balance, the keen analyst must understand what items appear critical.²⁴⁹ As suggested by the definition, critical items tend to emerge in two broad categories:²⁵⁰

- Essential to security: any source of power perceived necessary to mount a defense, which is akin to the theoretical and doctrinal concept of a “center of gravity” (COG); and
- Essential to welfare: the perceived foundational underpinnings of sovereignty or maintenance of a population’s way of life.

Security fears represent a cornerstone of realist IR theories, while welfare tends to emerge in economic theory. As demonstrated by the U.S. National Security Strategies (NSS), including the most recent NSS in 2017, states stand ready to declare war if these items become threatened.²⁵¹ At the height of the Cold War, Defense Secretary Caspar Weinberger famously argued that threats to U.S. vital national interests should serve as the test when deciding whether to commit troops abroad—an idea echoed by others who served as Secretary of Defense.²⁵² What did Secretary Weinberger mean by “vital national interests?” He meant security and welfare. The advent of cyber conflict has further

²⁴⁹ In describing how criticality relates to risk, the doctrinal guide to risk simply asks “How important is the object?”: The Joint Chiefs of Staff, *CJCSM 3105.01*, B-3.

²⁵⁰ Through a study of past National Security Strategies and academic works on vital national interests, security and welfare emerge as enduring themes, and this was neatly summarized by George Kennan in 1948, as quoted in: John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War*, Revised and Expanded ed. (New York: Oxford University Press, 2005), 26; For a study into “center of gravity”: Clausewitz, *On War*, 595–96; U.S. Department of Defense, *JP 5-0*, GL-6; For the importance placed on sovereignty, see: “Chapter I: Purposes and Principles,” in *Charter of the United Nations* (San Francisco, CA: The United Nations Conference, 1945), <https://www.un.org/en/charters-united-nations/index.html>; To garner an understanding of how foundational objects, such as a banking system, to a country’s way of life, see: Lawrence R. Samuel, *The American Way of Life: A Cultural History*, ed. Kalman Goldstein, Fairleigh Dickinson Series in American History and Culture (Teaneck, NJ: Fairleigh Dickinson University Press, 2017).

²⁵¹ Donald Trump, *National Security Strategy of the United States* (Washington, DC: The White House, 2017), <http://nssarchive.us/>.

²⁵² Caspar Weinberger, “The Uses of Military Power,” National Press Club Speech (Washington, DC: Office of Assistant Secretary of Defense, 1984), 5–6; William J. Perry, “Let Wisdom Guide Our Use of the Military,” *Navy Times*, 8 May 1995.

highlighted how systems critical to international welfare—such as power grids and financial infrastructure—can spur offensive actions and create a daunting task for the defenders.²⁵³ Ergo, technology can present a tempting target for one’s adversaries, while security and welfare represent scalable items that translate to criticality in the offense-defense balance.

The offense-defense literature nearly broaches the topic of criticality when Jervis describes how exposed weapons can trigger a destabilizing effect between adversaries. He argues that a destabilizing effect arises when weapons are exposed, creating a vulnerability.²⁵⁴ An exposed weapon is a critical object, and its lack of protection creates an inducement to strike between two adversaries. In other words, an actor may fear that if an exposed weapon goes unused, other actors may choose to strike the weapon first out of fear of its eventual use. Thus, Jervis’ argument hinges on the “first-striker” problem. In the first-striker problem, two opponents face each other, and both possess a capability to win if and only if they strike first; therefore, both opponents have an incentive to strike first. While Jervis’ argument also highlights the importance of insulation, it does underline the effect that criticality has on the offense-defense balance. A weapon is critical to a state’s security. Because the state’s opponents view the weapon as critical, they have a temptation to strike it, leading to preferences for offensive strategies.

Two historical examples—the Second Punic War and the Schlieffen Plan—both reveal how a state’s critical source of power can induce adversaries into offensive strategies. In the case of the Second Punic War, Hannibal identified the Roman allies as a keen source of Rome’s power.²⁵⁵ The Roman allies are a classic example of a center of gravity; Rome relied on its allies for security. Because Hannibal perceived this criticality,

²⁵³ Graham Allison, Dimitri Simes, and James Thomson, *America’s National Interests: A Report from the Commission on America’s National Interests*, (Cambridge, MA: Belfer Center for Science and International Affairs, 1996), 3, <https://www.belfercenter.org/publication/americas-national-interests-report-commission-americas-national-interests-1996>; Ted Koppel, *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, First ed. (New York: Crown Publishers, 2015), 3–16.

²⁵⁴ Jervis, “Cooperation,” 196–97.

²⁵⁵ Arthur Cotterell, Roger Lowe, and Ian Shaw, *Leadership: Lessons from the Ancient World* (Chichester, UK: John Wiley & Sons, 2006), 153–54.

he undertook an offensive campaign that allowed him to target Rome's allies and turn them to his campaign.²⁵⁶ In the case of the German's Schlieffen Plan prior to WWI, the Germans identified the French army's striking power as central to its security.²⁵⁷ As a result, the German general staff proceeded with the assumption that the only true way to win in a war against France was to completely destroy French striking power. Any delayed efforts to eliminate this critical source of power would permit enough time for the Russian army to mobilize and envelop Germany in a two-front war.²⁵⁸ Though numerous factors can draw an actor into an offensive strategy—such as the case for the Germans in WWI—the critical links in an adversary's chain also play a role. As these examples demonstrate, an adversary's targetable items that appear critical to either security or welfare sways the offense-defense balance toward the offense.

6. Variable 6. Resilience: The Modern Second-Strike

The final variable that can impact the offense-defense balance is resilience. Resilience *represents the degree to which technology and geography offer the ability to recover from an attack*. An increase in resilient capabilities leads to a corresponding movement of the offense-defense balance toward the defense. The underlying logic of this argument is straightforward. If one side perceives that their opponents will recover from an attack, then the incentive to attack decreases and defense becomes the preferred strategy. The 2013 *Presidential Policy Directive/PPD-21* catapulted the importance of resiliency into the security spotlight by mandating that U.S. critical infrastructure acquire an increased level of resiliency to withstand cyber-attacks. PPD-21 defines resilience as, “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly

²⁵⁶ Michael P. Fronda, “Hannibal: Tactics, Strategy, and Geostrategy,” in *A Companion to the Punic Wars*, ed. Dexter Hoyos, Blackwell Companions to the Ancient World (Malden, MA: Wiley-Blackwell, 2011).

²⁵⁷ Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth*, trans. Andrew Wilson and Eva Wilson (Auckland, NZ: Eschenburg Press, 2018), 77, <http://www.pp-publishing.com/>, e-Book.

²⁵⁸ Ritter, 74–75.

from disruptions.”²⁵⁹ This definition echoes the U.S. doctrinal view, though the military literature further offers recommendations to increase resiliency, including the development of redundant or robust capabilities.²⁶⁰

In the offense-defense literature, the notion that resiliency aids defensive strategies emerges in the discussions of a second-strike capability and its interplay with deterrence.²⁶¹ The second-strike capability became increasingly important during the Cold War, and the prominent work that gave life to the issue was Albert Wohlstetter’s “Delicate Balance of Terror.”²⁶² The meaning in the title is clear—only the fear of death prevents nuclear war but does so in a tenuous manner. By maintaining a second-strike capability, opponents can achieve deterrence by presenting a credible threat to return an attack, in kind, which is the hallmark of a deterrent strategy.²⁶³ The U.S. and Russia ensured the capability to deliver retaliatory strikes through Polaris-type systems, such as the submarine-launched ballistic missile (SLBM).²⁶⁴ Through this “delicate” political dance, both sides avoid a nuclear exchange as striking first buys the offender a credible response-in-kind, thereby presenting a strong incentive to avoid the first attack. Hence, a second-strike capability captures the very essence of a resilient capability; it implies that one recovers from an attack and retaliates. In this way, perceiving a resilient adversary leads to a preference for defensive strategies.

²⁵⁹ Barack Obama, *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience* (Washington, DC: The White House (Office of the Press Secretary), 2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

²⁶⁰ The Joint Chiefs of Staff, *CJCSM 3105.01*, b-3.

²⁶¹ Jervis, “Cooperation,” 206–08; Van Evera, *Causes of War*; Lynn-Jones, “Offense-Defense Theory,” 675–76.

²⁶² Albert Wohlstetter, “The Delicate Balance of Terror,” *Foreign Affairs* 37, no. 2 (1958), <https://doi.org/10.1080/00396335908440116>.

²⁶³ A simple definition of deterrence: “One deters another party from doing something by the implicit or explicit threat of applying some sanction if the forbidden act is performed”: Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961), 9.

²⁶⁴ Jervis, “Cooperation,” 207; In his article, Wohlstetter lists the conditions needed to ensure a second-strike capability: ability to survive enemy attacks, communicate decision to retaliate, and possess range and penetration capability: Wohlstetter, “The Delicate Balance of Terror,” 216.

In the conventional sense of deterrence, the concept of resilience plays a further role through deterrence by denial strategies. In his seminal work on denial strategies, Glenn Snyder defines denial as deterring through convincing a potential aggressor that aggression is likely to fail and any objectives will remain uncaptured.²⁶⁵ By creating this perception, a denial strategy convinces any opponent that there is an unacceptable up-front cost to pay for aggression. How might one create the perception that any adversary may find an immense up-front cost? It is done by creating a level of resiliency. As discussed in chapter two, Mearsheimer's work on conventional deterrence concludes that a denial strategy is often a successful deterrence strategy, in which an example of a denial strategy involves signaling a commitment to—or at least a preference for—a prolonged attrition-based war.²⁶⁶ Much as a second-strike capability embodies resilience, so, to, does attrition.²⁶⁷ One of the central tenets of attrition warfare involves regenerating troops for continued battle. As a result, attrition requires resilience, as it necessitates trading blow-for-blow, recovering from each blow, and continuing the fight. Clearly, the literature hails resilience as a key to deterrence, and deterrence implies that offensive strategies are a poor choice.

The concept of resilience has gained considerable footing in the cybersecurity community. The chief reason is that defense networks cannot stop the pure volume of cyber-attacks that plague cyberspace.²⁶⁸ As a result, cybersecurity experts warn that cybersecurity is not a panacea for cyber-attacks.²⁶⁹ Rather, businesses and organizations should prepare for cyber-attacks as an inevitability—it is not a question of if, but when. Following PPD-21, organizations such as the National Institute of Standards and

²⁶⁵ Snyder, *Deterrence and Defense*, 14–16.

²⁶⁶ Mearsheimer does not specifically refer to attrition as a “denial strategy.” His main proposition is that if an aggressor perceives a blitzkrieg strategy viable and consequently perceives war to be of little cost, deterrence is likely to fail: Mearsheimer, *Conventional Deterrence*, 203–08.

²⁶⁷ Attrition is a resource-based method of warfare involving brute strength applied against brute strength, and the optimized or longer-lasting opponent emerges the victor: Luttwak, “The Operational Level of War,” 64–65.

²⁶⁸ Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, MD: Rowman & Littlefield, 2017), 130–32.

²⁶⁹ Christopher Mele, “Data Breaches Keep Happening. So Why Don’t You Do Something?,” *New York Times*, 1 August 2018, <https://www.nytimes.com/2018/08/01/technology/data-breaches.html>.

Technology (NIST) have begun issuing reports outlining how cyber resilience should unfold.²⁷⁰ The answer captures distinct characteristics of defense: absorb the threat, focus on its effects, and identify the vital functions that an organization must preserve if attacked.²⁷¹ Consequently, cyber conflict highlights the applicability of resilience to the offense-defense balance, as a resilient system tips the balance toward the defense.

D. THE EXCLUDED VARIABLES

As much as the proponents of offense-defense theory have endeavored to advance the theory, some of its critics also identify considerations that, if heeded, can help strengthen the theory. In particular, the critics of offense-defense theory question the efficacy of mobility and firepower. As shown on the previous pages, this thesis reformats firepower; it is now based on effects. Mobility, on the other hand, is a distinctly physical element, that struggles to achieve consistency in the offense-defense balance. Because mobility emerges prominently in the offense-defense literature, it is necessary to address the decision to exclude it from this thesis. Two other notable variables—temporary weapon potency and weapon differentiation—also warrant a brief justification, as well.

1. Mobility: Insufficient Evidence of Tipping the Balance

Any study of the history of offense-defense theory is incomplete without a discussion of how mobility impacts the balance. The logic for any effort to include mobility as salient to the balance is understandable: without the ability to move weapons or forces, there is no ability to undertake an offensive campaign. Even the critics of offense-defense theory concede this logical notion.²⁷² As a result, most offense-defense theorists find

²⁷⁰ Ron Ross et al., *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800–160 Volume 2 (Gaithersburg, MD: National Institute of Standards and Technology, 2019), <https://doi.org/10.6028/NIST.SP.800-160v2>.

²⁷¹ Ross et al., *SP 800–160 Vol 2*, 73.

²⁷² “Despite the high degree of confusion, there appears to be at least some consensus that mobility innovations favor offense.” Lieber, “Grasping the Technological Peace.”; Gray writes on the importance of “reach” in making a weapon offensive: Gray, *Weapons Don’t Make War*, 31; Mearsheimer concedes that an important offensive capability is choosing the time and place of attack: Mearsheimer, *Conventional Deterrence*, 26.

themselves compelled to address the issue of mobility. Does it enable the offense by allowing the forward movement of weapons, or does it aid the defense by allowing the defender to adjust to an attack? Ultimately, the offense-defense literature fails to classify mobility in a way that predicts the balance because a defensive force that is mobile often claims supremacy over an equally mobile offensive force. This view aligns with arguments first put forth by Jervis, then convincingly restated by Mearsheimer and Lieber in the decades following Jervis.²⁷³ The inconclusive nature of mobility in determining the offense-defense balance allows us to exclude mobility from testing in this thesis.

As one of the originators of offense-defense theory, Quester is the first to suggest that mobility is a key indicator of tipping perceptions toward the offense.²⁷⁴ He argues that without the ability to move, a weapon is “supremely defensive.”²⁷⁵ For instance, consider a minefield; once created, a minefield does not penetrate sovereign boundaries, it simply protects an area until deactivated in some way. This argument does not take into account initial placement or re-arrangement of immobile weapons. Placing a minefield surreptitiously in an adversary’s area, for example, constitutes a clear offensive use of a mine. Thought of another way, an intrinsically defensive weapon that lacks mobility can be placed in a way that eases the passage of invading troops or bolster an aggressor’s position on newly gained ground, therefore bolstering the offense. An example of a weapon considered by many to be intrinsically defensive is a strategic Surface-to-Air Missile (SAM), which is meant to protect key areas from intruding aircraft, and erecting them in along a forward-line-of-troops or key avenue of approach aids the offense. Next, consider the opposite argument: that creating a mobile asset automatically deems it offensive. Again, we can turn to the example of SAMs; this time, consider a mobile SAM. A mobile SAM becomes problematic for an invading aviation force, as its location can become difficult to pinpoint. This uncertainty of SAM locations bolsters the primacy of an air

²⁷³ Mearsheimer, *Conventional Deterrence*, 25–27; Lieber, “Grasping the Technological Peace,” 79–80; Jervis also concedes that classifying mobility in an effective way for the balance leads to contradictory and ambiguous terminology:” Jervis, “Cooperation,” 197–98, 203.

²⁷⁴ Quester, *Offense and Defense*, 3.

²⁷⁵ Quester, 3.

defense, and, thus, aids the defense. In this regard, *mobility actually represents a key part of defense, as well*, and mobility does not inherently aid either side of the offense-defense balance.

Next, Quester also argues that mobility creates the ability to mass numerical advantages and to attack the weak spots of an opposing force.²⁷⁶ Without the ability to reposition or move weapons, there would be a lack of incentives to pursue offensive operations without this ability. In his book, Mearsheimer addresses this argument by examining mobility's impact in the initial contact and exploitation phases of an attack.²⁷⁷ First, in the initial contact (which Mearsheimer refers to as "breakthrough"), a defender benefits greatly from a rapid reaction to bolster its weak points during a surprise attack, and a rapid reaction is only gained through mobility. Next, as an invading force attempts to exploit its early battlefield victories, the defender is left with the unpleasant task of mobilizing reinforcements elsewhere from its forces and moving to repel the invading force. Having this ability may dissuade an attacker of their advantage before even launching an invasion. Mearsheimer then offers a historical example from WWII by citing instances of German tanks that repeatedly repelled a numerically-superior Soviet force on the eastern front from 1943–1945.²⁷⁸ What allowed the German tanks to achieve defensive success was their mobility. These arguments also cast sufficient doubt on the inclusion of mobility in offense-defense theory.

Finally, Lieber advances persuasive counterarguments to mobility's importance to the offense by pointing out how mobility aids the defense at multiple levels of warfare, namely, the strategic, operational, and tactical levels.²⁷⁹ These three levels of mobility refer to inter-theater, intra-theater, and intra-battlefield mobility, respectively. First, strategic mobility is crucially important to a defender, at times, by allowing reinforcements to flow back to the terminal defensive area from overseas missions, or from supporting

²⁷⁶ Quester, 3.

²⁷⁷ Mearsheimer, *Conventional Deterrence*, 26.

²⁷⁸ Mearsheimer, 26.

²⁷⁹ Lieber, "Grasping the Technological Peace," 79–80.

allies. Next, operational mobility allows a defender to react to a “breakthrough” and supply reinforcements, much as Mearsheimer argued in his book. Finally, tactical mobility has the potential to overextend an attacker, while also allowing a defender to counter-attack in the heat of a battle. Collectively, the three levels of mobility and their importance to a well-structured defense blur the lines of mobility’s impact on the offense-defense balance. A review of the offense-defense literature helps focus future theory in a beneficial direction.

2. Temporary Weapon Potency: Insufficient Evidence of Tipping the Balance

In his work, Quester broaches the idea that temporary durations of weapon potency tips the offense-defense balance toward the offense.²⁸⁰ Though this concept is mentally appealing, it ultimately does not adhere to sound logic. The argument that weapon duration furthers offensive incentives is that when a weapon offers only a fleeting opportunity to produce effects, the incentive is strong to capitalize on those effects before losing the opportunity. However, the duration of weapon potency does not necessarily tie it to an offensive use; a weapon may also offer only a fleeting defensive advantage. For instance, a well-concealed defender may quietly obtain a fleeting opportunity to devastate an attacking force through an ambush. As a result, one may argue that duration also clearly bolsters defense. Moreover, to induce offensive preferences, a short-duration weapon must offer effects that are (1) overwhelming, (2) well-forecasted to the attacker, and (3) not leave the attacker exposed in any way following the attack. Because of the narrow category that these required effects offer, the duration of weapon potency does not indicate a strong indicator of aggressive behavior, nor does it aid the offensive.

In light of the temporary duration that exemplifies many cyber weapons, Quester’s argument about duration has taken on new life. Many cyber weapons are built around zero-day exploits or “applets” that are meant to exploit software vulnerabilities that are currently

²⁸⁰ Quester, *Offense and Defense*, 4.

unpatched.²⁸¹ Because these vulnerabilities may become discovered and patched at any moment, the potency of zero-day exploits or applets assumes a temporary aspect. However, it is not the temporary nature of many cyber weapons that incentivizes attack, it is typically one of the three effects listed above: an overwhelming or well-known outcome, or minimal exposure for the attacker. Furthermore, short-duration cyber weapons such as zero-days are massively expensive, leading to a use that is purposely well-timed. If a zero-day becomes “burned” with little to show for its use, the weapon cost the attacker a damaging cost. The great cost of short-duration weapons creates an incentive to exert control over their use, as demonstrated by zero-days. Ultimately, short-duration weapons fail to tip the offense-defense balance.

3. Counterforce and Countervalue Weapons: Inability to Distinguish

Quester does suggest one interesting distinguishing feature: counterforce versus countervalue weapons.²⁸² Making this distinction, Quester argues, could help determine whether technology is offensive or defensive. Counterforce, he argues, are offensive, while countervalue weapons are defensive. A counterforce weapon infers that its primary purpose is to degrade or destroy the capability of the opposing forces. By contrast, a countervalue weapon is intended to cause suffering beyond the opposing forces and into their civilian population base. As a result, countervalue weapons tend to be retaliatory in nature as they often serve no battlefield purpose. A prime example of this distinction is illustrated by the difference between a tactical nuclear weapon and a strategic nuclear weapon. The chief purpose of a tactical nuclear weapon is for use on the battlefield to massively attrite opposing forces, while a strategic nuclear weapon is meant to strike at a nation’s ability to wage war.²⁸³ Like Quester, Jervis and Van Evera also speculate on the importance of counterforce technology, though they use terms that imply a weapon’s ability to reduce

²⁸¹ Zero-day exploit vulnerabilities: Brantly, *The Decision to Attack*, 39; applets: Clarke and Knake, *Cyber War*, 89; Conti and Raymond describe a temporary software exploit as “nobody but us” (NOBUS): Conti and Raymond, *On Cyber*, 137–38.

²⁸² Quester, *Offense and Defense*, 4–6.

²⁸³ Amy F. Woolf, *Nonstrategic Nuclear Weapons*, RL32572 (Washington, DC: Congressional Research Service, 2019), Summary Page, <https://crsreports.congress.gov/product/pdf/rl/RL32572>.

fortifications.²⁸⁴ The essence is the same—both refer to the ability to pierce defenses, expose the adversary, and potentially devastate or attrite.

Unfortunately, this argument presents too many logical hurdles. Take strategic bombing and its inability to act as a strictly counterforce or countervalue attack option. Quester intended strategic attacks to form a deterrence by retaliation strategy, which may appear defensive by virtue of its association with deterrence. However, its classical advocates offered it as a means to strike at an adversary's COG, including the morale of the supporting population, which both the allies and axis did in an offensive manner during WWII.²⁸⁵ Moreover, in modern use, doctrine refers to strategic attack as strike intended to hinder a state's ability to conduct war, and it is often offered as a policy option to rapidly achieve national objectives, separating it from the strictly deterrent effects to which Quester points. Further, it is not clear that deterrence by retaliation is viable when done in the context of two unequal sides.²⁸⁶ As tempting as it is to categorize each weapon as either offensive or defensive—counterforce or countervalue—this analysis method has not fit in offense-defense theory.

E. CONCLUSION

Though conflict continues to evolve, the basic notions of offense and defense have not—the offense still attacks while the defense still waits.²⁸⁷ Because this aspect of conflict has remained constant, offense-defense theory can provide useful insights into emerging forms of conflict, such as cyber conflict. By accumulating the collective work of offense-

²⁸⁴ Jervis, "Cooperation," 205; Van Evera, "Offense, Defense, and the Causes of War," 16.

²⁸⁵ The U.S. Air Force now broadly refers to strategic bombing as "strategic attack:" U.S. Air Force, *AFD 3-70*; Giulio Douhet, *The Command of the Air*, ed. Donna Budjenska, trans. Dino Ferrari (Maxwell AFB, AL: Air University Press, 2019), 371–94, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0160_DOUHET_THE_COMMAND_OF_THE_AIR.pdf.

²⁸⁶ Intriligator and Brito, "Can Arms Races Lead to the Outbreak of War?," 74.

²⁸⁷ In 431 BC during the Peloponnesian War, the Spartans repeatedly invaded Attica and laid siege to Athens, while the Athenians leveraged their city fortifications and naval superiority in an effort to outlast the Spartans--offense and defense: Thucydides, *The Landmark Thucydides*, 1.139-2.03; The essence of offense and defense in cyber operations remains intact; doctrine defines offensive cyber operations as projecting power (attack) and defensive cyber operations as protecting from threats (waiting): U.S. Department of Defense, *JP 3-12*, xi.

defense theorists, the opportunity stands to create an analytical framework to those wishing to assess where the balance stands. Past efforts to do so lacked the insights of modern conflict and, consequently, often suffered from the influences of the Cold War or strict land warfare. The efforts in this chapter to produce testable variables produced a set of variables to test the offense-defense balance: information advantage, decisive effects, exposure, insulation, criticality, and resilience. The duty of the analyst is to consider how each of these variables impacts the balance when assessing new forms of conflict or significant geographic changes. While analyzing each of these variables, it is vital to consider the technological and geographic factors that can impact the balance. Furthermore, an analysis of the offense-defense balance requires one to ask questions centered around the proposed variables:

- Does the tools and practices of modern warfare confer an Information advantage and, therefore, tip the balance toward the offense?
- Do the geographic concerns of the European Union help insulate its residents from attack, bolstering the defense?

Table 2. The Factors and Variables of Offense-Defense Theory (Developed by This Thesis)

	Item	Definitions/Considerations	
Factors	Technology	Means to fulfill a human purpose	
	Geography	Spatial conditions that impact operations	
Variables	Item	Perception	An increase aids...
	Information advantage	Can manipulate the information	Offense
	Decisive effects	Nullifies or overwhelms defenses	Offense
	Exposure	Offense requires risk	Defense
	Insulation	Disallows or shields from attacks	Defense
	Criticality	Targetable items appear necessary	Offense
	Resilience	Ability to recover from attacks	Defense

The coming chapters test these proposed variables by considering their explanatory power in modern forms of conflict. By refining these variables, it strengthens an assessment of emerging forms of warfare. The ultimate goal is to offer an assessment of a modern and immensely relevant form of conflict: cyber conflict

IV. TESTING THE UPDATED OFFENSE-DEFENSE THEORY: AIR WARFARE AND IRREGULAR WARFARE

Democracy has stimulated the will of the people to eliminate war, although it has not yet enlightened their intelligence as to the means

—Quincy Wright, *A Study of War*²⁸⁸

While the previous chapters focus intently on the development of the offense-defense theory, cyber conflict still guides this thesis, and the ultimate goal remains to analyze the balance of cyber offense and cyber defense. The next logical step is to apply the theoretical findings of the previous chapters to the cyber offense-defense balance. However, the pursuit of empiricism demands a link—an intermediary step between the proposal of the new theoretical variables and their application to cyber conflict.²⁸⁹ The previous chapter synthesizes the variables in Table 2 from the available offense-defense literature. Before applying these variables, this thesis must first ensure a level of robustness. In other words, can the variables developed in Chapter III provide insights into modern conflict, or only describe conflict at an earlier point in time? This chapter presents a test of the proposed offense-defense variables through two case studies: air warfare and Irregular Warfare (IW). Testing the theory against air warfare and IW accomplishes the crucial step of determining whether the theory is both robust and can provide insights into the offense-defense balance of emerging modes of conflict.

A. DEFINING AIR WARFARE AND IRREGULAR WARFARE

Before conducting an offense-defense analysis of air warfare and IW, the first hurdle is to define terms. For both forms of conflict, this section provides two contextually-

²⁸⁸ Quincy Wright, *A Study of War*, vol. 1 (Chicago, IL: University of Chicago Press, 1942), 5.

²⁸⁹ For a view into how objective inquiry coincides with theory development, see: King, Keohane, and Verba, *Designing Social Inquiry: Scientific Inference in Qualitative Research*, 12–33; James D. Fearon, “Counterfactuals and Hypothesis Testing in Political Science,” *World Politics* 43, no. 2 (1991): 175–77, <https://doi.org/10.2307/2010470>; Peter Godfrey-Smith, *Theory and Reality: An Introduction to the Philosophy of Science* (Chicago, IL: University of Chicago Press, 2003).

different views: the military's doctrinal view, and a view external to the DOD to provide a check on doctrinal concepts.

This chapter bounds air warfare to conflict in the air domain to seize air superiority, including those ground efforts to control the air, for analysis of the offense-defense balance.²⁹⁰ While the air domain is the medium, or physical space, where air warfare unfolds, airpower is the vehicle by which a military interacts in the air domain, enabling the needed campaign effects.²⁹¹ U.S. Air Force (USAF) doctrine defines airpower as “the ability to project military power or influence through the control and exploitation of air, space, and cyberspace to achieve strategic, operational, or tactical objectives.”²⁹² The inclusion of space and cyberspace in this definition is a result of USAF authority over the majority of DOD's space and cyberspace assets; however, that structure is rapidly changing, and space and cyberspace are not the focus of this chapter.²⁹³ The view that air warfare's focal contest is over control of the air extends beyond doctrine, as well. In his study of the expanding importance of airpower, the security analyst Richard Hallion argues, “[t]he single most important enduring requirement of air power forces is ensuring air dominance ... And generally speaking, loss of control of the air usually equates to the inability to control or to hold the surface, and, more importantly, to exert national

²⁹⁰ “Air superiority is that degree of control of the air by one force that permits the conduct of its operations at a given time and place without prohibitive interference from air and missile threats”: U.S. Department of Defense, *Joint Publication 3-01: Countering Air and Missile Threats* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017), I-4, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

²⁹¹ Joint doctrine defines the air domain as, “the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible”: U.S. Department of Defense, *Joint Publication 3-30: Joint Air Operations* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2019), I-1, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

²⁹² U.S. Air Force, *Air Force Doctrine Volume I: Basic Doctrine* (Maxwell AFB, AL: Lemay Center for Doctrine, 2014), 25, <https://www.doctrine.af.mil/>.

²⁹³ USCYBERCOM was made into a unified Combatant Command in 2017: *Title 10 U.S.C. § 167b*; The U.S. Air Force Space Command was re-designated as the U.S. Space Force, establishing the sixth branch of the U.S. armed forces, in 2019: *National Defense Authorization Act for Fiscal Year 2020*, Pub. L. No. 116–92, Title 9 U.S.C. § 9081, 116th Congress, 1st Session (20 Dec 2019). <https://www.congress.gov/bill/116th-congress/senate-bill/1790>.

sovereignty.”²⁹⁴ Generally, airpower serves as part of a broader military campaign, providing effects—from missions to seize air superiority to mobility support—to move the campaign toward a set of objectives by and through the air domain.²⁹⁵ However, bounding air warfare to the struggle for air superiority concentrates the analysis and permits testing of the six offense-defense variables.

To assess the offense-defense variables proposed in this thesis, this chapter defines IW as a struggle for control of a population between a state and non-state actor—referred to as insurgencies throughout the analysis. This definition follows the concepts in Joint doctrine, which defines IW as “a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s).”²⁹⁶ This definition highlights three key points: the DOD role through the inclusion of *violence*, the lack of a clear-cut Westphalian context through *irregularity*, and the contest for control of a population through *influence*. IW is a term that emerged only recently to help the DOD distinguish between conventional campaigns and the limited operations that typify modern conflict. The threats that epitomize IW operations are often terrorists, insurgents, and criminal networks who exploit new technologies, weakened states, and political divides to bolster their influence.²⁹⁷ Because it includes such problems as insurgencies and revolutionaries, IW has been a reality for nearly as long as traditional war—just fought under different names.²⁹⁸ In the colonial era, the problem of guerilla warfare in the British colonies gave rise to the term “Small Wars,” defined in their seminal literature on the topic as any

²⁹⁴ Richard P. Hallion, “Air and Space Power: Climbing and Accelerating,” in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010), 379. There are various degrees of air dominance, ranging from superiority to supremacy, a point covered later in this chapter.

²⁹⁵ U.S. Department of Defense, *JP 3-30*, II-3 - III-12.

²⁹⁶ U.S. Department of Defense, *JP 1, Change 1*, I-6.

²⁹⁷ U.S. Department of Defense, *Joint Operating Concept: Irregular Warfare: Countering Irregular Threats, Version 2.0* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2010), 14–15, <https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>.

²⁹⁸ Revolutions and “insurgencies” were a problem as far back as the Roman empire, when three Servile Wars sprouted between 135 BC and 71 BC: William Smith and Eugene Lawrence, *The History of Rome: From Early Times to the Establishment of the Empire* (Luton, UK: Andrews UK Limited, 2010), 129–217.

campaign other than those in which both sides consist of regular troops.²⁹⁹ This definition coincides with an article penned by a Central Intelligence Agency (CIA) analyst named Jeffrey White in 1996. The chief purpose of White's article, at the time, was to stress how the U.S. intelligence community was not well-oriented to the complex problems posed by IW.³⁰⁰ Much like the other definitions, White also defines IW as those conflicts that do not strictly include regular troops. He further aligns his definition with joint doctrine by citing guerilla wars and rebellions as examples of IW, emphasizing the insurgent's struggle to gain control.³⁰¹ Thus, the doctrinal view, as corroborated by White's definition, aptly fits the purposes of this chapter.

B. CASE SELECTION

Embedded within this chapter's introduction and subsequent definitions is an important question that requires an answer. Why air warfare and IW? How do they serve as a link between the traditional forms of warfare and cyber conflict, and what bearing do they have on offense-defense theory? Re-examining the offense-defense theory necessitates the study of previously-ignored concepts. The lack of attention in the offense-defense literature for air warfare and IW first signifies that both fit the bill. However, what truly makes them essential to the discussion is how both have redefined the concepts of offense and defense in warfare—a trend that continues with cyber conflict. Because traditional measures of success like the forward line of troops (FLOT) and security of vital sea-lines of communication have become only part of the equation, how should military leaders gain and maintain the advantage over their adversaries? Exploring aspects of air warfare and IW provides the bridge from conventional war to cyber conflict for the offense-

²⁹⁹ C. E. Callwell, *Small Wars: Their Principles and Practice*, Third ed. (Lincoln, NE: University of Nebraska Press, 1996), 21; Interestingly enough, the term irregular seems to come from an English translation of a German book on "Small Wars:" Friedrich August Freiherr von der Heydte, *Modern Irregular Warfare in Defense Policy and as a Military Phenomenon*, trans. George Gregory, First English ed. (New York: New Benjamin Franklin House, 1986).

³⁰⁰ Jeffrey B. White, "Some Thoughts on Irregular Warfare: A Different Kind of Threat," *Studies in Intelligence* 39, no. 5 (1996), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/>.

³⁰¹ White.

defense theory. Succinctly put, air warfare and IW both *receive only sparing attention* in the offense-defense literature, both *maintain relevance* from historical through modern conflict, and both *possess analytical features similar to cyber conflict*.

First, the offense-defense literature does not dwell on air warfare or IW, and examining both fosters growth for the theory. Further, the variables gleaned in the previous chapter emerge from conventional warfare analysis, and applying the variables to previously-unexamined forms of conflict help determine whether the variables are robust. In terms of air warfare, previous offense-defense research focuses primarily on nuclear missile engagement, as the result of the Cold War.³⁰² An Air University occasional paper by John Carter presents an insightful assessment of airpower's offense-defense balance, finding that the defense does not enjoy an inherent advantage in the air domain.³⁰³ However, the primary focus of his research is on the effects of organizational biases within air forces, as such biases impair objectivity and can promote a "cult of the offensive."³⁰⁴ Further, Carter's paper does not aim to test for any enduring variables that may impact the balance across multiple forms of conflict. For offense and defense in IW, Quester and Posen both dwell on the subject; however, neither offers a definitive assessment.³⁰⁵ Quester presents the issues that could tip the IW balance in for each case, while Posen dwells on the tools needed for the U.S. to assume an offensive stance during its "struggle against terrorism."³⁰⁶ While these studies are informative, both leave open the inquiry of this thesis and oblige an examination of the IW offense-defense balance.

³⁰² Jervis, "Cooperation," 206–10; Lynn-Jones, "Offense-Defense Theory," 675–76.

³⁰³ "[T]he traditional view of the relationship between offense and defense is altered for airpower. Because airpower defense has no advantage of position and time accrues to the detriment of [both], airpower defense enjoys no inherent advantage": Carter, *Airpower and the Cult of the Offensive*.

³⁰⁴ Specifically, it does this by examining three case studies: the RAF in the interwar period, the Israeli Air Force from 1967–73, and the USAF from 1953–65: Carter, *Airpower and the Cult of the Offensive*, 4.

³⁰⁵ "Is guerrilla war in the end a promising tool for the offensive, or for the defense? The answer depends on gimmicks of technology and weaponry": Quester, *Offense and Defense*, 181; "[T]he United States is accustomed to being on the offensive, but in this campaign the defensive must assume equal or greater importance": Barry R. Posen, "The Struggle against Terrorism: Grand Strategy, Strategy, and Tactics," *International Security* 26, no. 3 (2002): 45, <https://doi.org/10.1162/016228801753399709>.

³⁰⁶ Quester, *Offense and Defense*, 171–82; Posen, "The Struggle against Terrorism," 45–51.

Second, *air warfare and IW* both played a significant role in warfare over the past century and are still highly relevant today. Moreover, air warfare and IW link cyber conflict to the World Wars, which are arguably the formative historical events for offense-defense theory. For air warfare, WWI first witnessed the significant emergence of air warfare.³⁰⁷ WWII, meanwhile, revealed the profound effects that airpower could render through devastating strategic bombing campaigns and pivotal use of tactical airpower.³⁰⁸ Throughout the Cold War, strategic bombing remained a cornerstone of American military strategy, while the tactical use of airpower expanded in both the Korean and Vietnam wars.³⁰⁹ Airpower also underpinned doctrine development during the Cold War in both the U.S.—with its AirLand Battle (ALB) doctrine—and the U.S.S.R., through its “deep operations battle” and reconnaissance-strike and fire.³¹⁰ Finally, airborne precision weapons and Intelligence, Surveillance, and Reconnaissance (ISR) platforms had a pronounced effect on American wars in the Balkans and the Middle East over the past

³⁰⁷ John H. Morrow, Jr., “The First World War, 1914–1919,” in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010).

³⁰⁸ Douhet, *Command*, 31–83; Henry H. Arnold, *Global Mission*, First ed. (New York: Harper & Brothers, 1949), 149; Weigley, *The American Way of War*, 363–64; For a strategic use of airpower during WWII that proved unique for the time, see: Daniel L. Haulman, “The Yamamoto Mission,” *Air Power History* 50, no. 2 (2003); For a review of how some of Douhet’s predictions about WWII unfolded while others proved wrong, see: Bernard Brodie, *Strategy in the Missile Age*, R-335 (Santa Monica, CA: RAND Corporation, 1959), 73–96, https://www.rand.org/pubs/commercial_books/CB137-1.html; Posen, *The Sources of Military Doctrine*, 81–104; Richard Overly, “The Air War in Europe, 1939–1945,” in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010); Richard R. Muller, “The Air War in the Pacific, 1941–1945,” in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010).

³⁰⁹ Weigley, *The American Way of War*, 363–440; Alan Stephens, “The Air War in Korea, 1950–1953,” in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010); The 1987 NSS emphasizes the importance of maintaining a diversified array of strategic nuclear forces through a “Nuclear Triad” to maintain peace through deterrence, and the NSS identifies nuclear bombers as a key piece of this equation: Ronald Reagan, *National Security Strategy of the United States* (Washington, DC: The White House, 1987), 21, <https://history.defense.gov/Historical-Sources/National-Security-Strategy/>; For a history of air power’s strategic arm, see: Lindsay T. Peacock, *Strategic Air Command* (London, UK: Arms & Armour Press, 1988); Wayne Thompson, “Operations over North Vietnam, 1965–1973,” in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010).

³¹⁰ Adamsky, *The Culture of Military Innovation*, 25–35.

thirty years.³¹¹ In particular, this includes the war that the North American Treaty Organization (NATO) waged exclusively with airpower over Kosovo in 1999.³¹² Thus, history portrays the ever-growing and evolving demand for airpower.³¹³ Today, joint doctrine strongly recommends air superiority as the preferred objective at the onset of major combat operations, suggesting that air warfare remains a fixture in campaign planning.³¹⁴ Further, air assets constitute a generous portion of international defense spending, as the demand for airpower remains strong today.³¹⁵ IW, meanwhile, plays an important role in conflict today, much as it did in ancient and colonial times long before the term came into use. By at least one summation, the world has borne over 80 conflicts since the end of WWII that fit the definition of IW from the previous section.³¹⁶ While WWI and WWII shifted much of the world's focus off of IW for the first half of the twentieth century, the Cold War and 9/11 attacks collectively put IW back into the limelight. Though many violent clashes mar the Cold War, some of the formative events of the period were the Vietnam War and the Soviet-Afghan War—both IW conflicts that

³¹¹ Thomas A. Keaney, "Surveying Gulf War Airpower," *Joint Force Quarterly* 2 (1993), <https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-2.pdf>; Fulghum, "F-117 Pilots, Generals Tell Congress About Stealth's Value in Gulf War."; John Andreas Olsen, "Operation Desert Storm, 1991," in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010); Robert C. Owen, "Operation Deliberate Force, 1995," in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010); Benjamin S. Lambeth, "Operation Enduring Freedom, 2001," in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010); Williamson Murray, "Operation Iraqi Freedom, 2003," in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010).

³¹² Tony Mason, "Operation Allied Force, 1999," in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010).

³¹³ Hallion, "Air and Space Power," 381–82.

³¹⁴ U.S. Department of Defense, *JP 3-30*, I-1, III-12.

³¹⁵ "Chapter Two: Comparative Defence Statistics."

³¹⁶ White, "Some Thoughts on Irregular Warfare."

greatly impacted the U.S. and U.S.S.R.³¹⁷ Following 2001, the “Global War on Terror” claimed the lion’s share of international security issues, and one of the key organizations in that fight was U.S. Special Operations Command (USSOCOM).³¹⁸ Between 2001 and 2019, the USSOCOM budget and workforce swelled over 400% and 70%, respectively, to meet the growing demand from IW threats.³¹⁹ Even now, USSOCOM faces a demand to tackle a range of IW engagements, including unconventional warfare (UW) and Security Force Assistance, mostly as a result of rising Great Power Competition concerns.³²⁰ Regardless of this potential change, the demand for the rare capabilities at USSOCOM remains high, and the relevance of IW is only growing.

Finally, air warfare and IW *share three salient attributes with cyber conflict*: all are inherently disparate, all possess asymmetric qualities, and all fail to conform to traditional battleground geometries. First, the disparate nature of conflict in air and cyberspace arises

³¹⁷ For a discussion on the guerilla aspects of the Vietnam War, see: Andrew F. Krepinevich, Jr., *The Army and Vietnam* (Baltimore, MD: John Hopkins University Press, 1986); For a telling of the CIA’s covert support to the insurgent fighters in Afghanistan throughout the 1980s, see the following two titles: Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and bin Laden, From the Soviet Invasion to September 10, 2001* (New York: Penguin Press, 2004); George Crile, *Charlie Wilson’s War: The Extraordinary Story of the Largest Covert Operation in History* (New York: Atlantic Monthly Press, 2003).

³¹⁸ The Goldwater-Nichols Act and 1987 Defense Authorization Act first directed USSOCOM to organize, train, and equip to conduct activities associated with IW: *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, Pub. L. No. 99–433, Title 10 U.S.C. § 161, 99th Congress, 2nd Session (1 Oct 1986), 26. <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg992>; *Department of Defense Authorization Act for Fiscal Year 1987*, Pub. L. No. 99–661, Title 10 U.S.C. § 167, 99th Congress, 2nd Session (14 Nov 1986), 169–73. <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg3816>.

³¹⁹ 2001 to 2019, respectively: 3.1B to 12.8B (CY2014\$), and 42,800 to 73,000 U.S. Government Accountability Office, *Special Operations Forces: Opportunities Exist to Improve Transparency of Funding and Assess Potential to Lessen Some Deployments*, GAO-15-571 (Washington, DC: U.S. Government Accountability Office, 2015), 9–14, <https://www.gao.gov/assets/680/671920.pdf>; Andrew Feickert, *U.S. Special Operations Forces (SOF): Background and Issues for Congress*, RS21048 (Washington, DC: Congressional Research Service, 2019), 7–8, <https://fas.org/sgp/crs/natsec/RS21048.pdf>; Inflation adjusted to CY2014 O&M (Composite) Dollars; O&M used as it represents the bulk of USSOCOM budget; inflation adjustment calculated using the Joint Inflation Calculator (JIC): Naval Center for Cost Analysis, “NCCA Inflation Indices and Joint Inflation Calculator,” (web page), updated April 2019, accessed 22 Jan 2020, <https://www.ncca.navy.mil/tools/inflation.cfm>.

³²⁰ Feickert, *U.S. Special Operations Forces (SOF): Background and Issues for Congress*, 10–11; Today, joint doctrine still directs USSOCOM to conduct “core activities” central to IW: U.S. Department of Defense, *Joint Publication 3-05: Special Operations* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2014), x-xiii, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

from the inherent need of centralized command and decentralized execution of assets across a vast expanse.³²¹ Though this expanse is more physical for airspace than cyberspace, the analogy remains that a command entity must trust assets to project forward and autonomously conduct missions.³²² IW also relies on the basic tenet of decentralized execution, regardless of the mission and actors at play. While IW may often entail networks as opposed to a centralized command structure, an effective IW campaign still trusts its assets to produce effects across a disparate space.³²³ Next, air warfare, cyber conflict, and IW all permit asymmetric warfare, meaning that relatively under-resourced actors can compete with well-resourced actors by refusing to engage their strengths.³²⁴ In the case of air warfare, relatively cheap Man-Portable Air-Defense Systems (MANPADS) enable poorly-resourced actors to threaten a formidable air force, a point that has haunted the U.S. and Russia in the middle east.³²⁵ IW also presents asymmetric opportunities for insurgencies. Chief among these opportunities are guerilla strategies, which involves employing small unit raids to harass large conventional armies. These guerilla strategies undercut the strengths of a conventional army, as demonstrated by the Viet Cong in Vietnam.³²⁶ Much like IW and air warfare, cyber conflict allows relatively under-resourced actors to potentially cripple powerful state actors that have grown over-reliant on computing capabilities.³²⁷ Finally, air warfare, IW, and cyber conflict all allow for the

³²¹ U.S. Air Force, *AFD Vol I*, 67; U.S. Department of Defense, *JP 3-01*, IV-7; U.S. Department of Defense, *JP 3-12*, IV-11.

³²² Hutchins, Cloppert, and Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, 5–9; U.S. Department of Defense, *JP 3-12*, IV-13.

³²³ U.S. Department of Defense, *IW JOC*, v2.0, 28.

³²⁴ Andrew Mack, “Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict,” *World Politics* 27, no. 2 (1975): 181–82, <https://doi.org/10.2307/2009880>.

³²⁵ See for instance: Crile, *Charlie Wilson’s War: The Extraordinary Story of the Largest Covert Operation in History*.

³²⁶ The U.S. Army’s struggles to cope with the asymmetric threat posed by the Viet Cong: Krepinevich, *The Army and Vietnam*, 1–17.

³²⁷ Conti and Raymond, *On Cyber*, 28; Singer and Friedman, *Cybersecurity and Cyberwar*, 150–53; Clarke and Knake, *Cyber War*, 147–49.

breach of international boundaries, granting opportunities for offensive strikes to bypass the opponents' defenses and achieve strategic effects.³²⁸ This final similarity between the modes of conflict sets them apart from conventional warfare. Forward defensive lines represent the traditional measure of progress in conventional warfare, while it is merely a consideration in the modern forms of conflict examined in this thesis.

C. AIR WARFARE

"Control of the air is a prerequisite to success for modern operations," warns U.S. joint doctrine.³²⁹ This statement has become the foundation of all airpower theory.³³⁰ It shapes the tenets of airpower, underpins every campaign plan, and steers the interaction of modern air forces with their joint counterparts. The doctrinal phrase that denotes control of the air is "air superiority," meaning a level of control sufficient to execute air missions without "prohibitive interference."³³¹ While the precise origins of air superiority's importance could stir a debate, it is difficult to understate the impact of the 1973 Yom Kippur War between Israel and the opposing Arab Coalition. The short 20-day war pitted U.S. and Soviet technology, and the massive losses suffered by both sides captured the attention of military analysts worldwide.³³² Though debates continue about the Yom Kippur war, many experts agree that the Israeli military faltered at the war's onset by failing

³²⁸ Arquilla, "The Computer Mouse that Roared," 41–46; U.S. Air Force, *AFD 3–70*; Charles F. Parker and Eric K. Stern, "Blindsided? September 11 and the Origins of Strategic Surprise," *Political Psychology* 23, no. 3 (2002), <https://doi.org/10.1111/0162-895X.00300>.

³²⁹ U.S. Department of Defense, *JP 3-0, Change 1*, III-33.

³³⁰ "Air superiority is a necessity ... no state has lost a war while it maintained air superiority": John A. Warden, III, *The Air Campaign: Planning for Combat* (Washington, DC: National Defense University Press, 1988), 13; "The single most important enduring requirement of air power forces is ensuring air dominance": Hallion, "Air and Space Power," 379.

³³¹ U.S. Air Force, *AFD 3–01*, 4–5.

³³² In terms of aircraft losses, estimates place Israeli Air Force losses at 109, and Arab Coalition losses at 516: John F. Kreis, *Air Warfare and Air Base Air Defense, 1914–1973* (Washington, DC: Office of Air Force History, 1988), 336; All given respectively, estimates place Israel tank/APC losses at 700–1,000/1,500–2,000 and Arab Coalition tank/APC losses at 1,500–2,000/1,000: William E. DePuy, "Implications of the Middle East War on U.S. Army Tactics, Doctrine and Systems," in *Selected Papers of General William E. DePuy*, ed. Richard M. Swain, Donald L. Gilmore, and Carolyn D. Conway (Fort Leavenworth, KS: Combat Studies Institute, 1995), 79, <https://www.armyupress.army.mil/Books/CSI-Press-Publications/Doctrine/#books-doctrine>.

to seize air superiority, focusing, instead, on close air support missions.³³³ In the aftermath of the war, analysts at the U.S. Army's Training and Doctrine Command (TRADOC) grasped this concept and spurred a doctrinal shift within the military.³³⁴ In particular, TRADOC's first commander, General DuPuy, recognized the value in fostering a symbiotic relationship between air and land forces and led the charge for the U.S. military's adoption of the "Active Defense" doctrine in 1976.³³⁵ Active Defense encouraged the employment of a combined-arms team to gain air superiority and create an environment that allows forces to fight from the vantage point of a defender.³³⁶ Though other doctrinal innovations have since supplanted Active Defense, control of the air has persisted as a mainstay in airpower, including weapons procurement, organization, and training.

The struggle for air superiority also defines the conduct of offense and defense in air warfare.³³⁷ Many noted air theorists argue that an air force must assume an offensive mindset to win control of the air, and their arguments primarily focus on the nature of the air domain. Philip Meilinger and John Carter, for instance, argue that the unlimited avenues of approach and inherent neutrality of the air battlespace necessitate an offensive approach

³³³ Kreis, *Air Warfare and Air Base Air Defense, 1914–1973*, 339–42; William E. DePuy, "Letter to Creighton Abrams (January 1974)," in *Selected Papers of General William E. DePuy*, ed. Richard M. Swain, Donald L. Gilmore, and Carolyn D. Conway (Fort Leavenworth, KS: Combat Studies Institute, 1995), 70–71, <https://www.armyupress.army.mil/Books/CSI-Press-Publications/Doctrine/#books-doctrine>.

³³⁴ Benjamin M. Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, CA: Stanford University Press, 2006), 25–48.

³³⁵ Jensen, 25–48.

³³⁶ DePuy, "Letter to Creighton Abrams," 70; William E. DePuy, "Active Defense (n.d.)," in *Selected Papers of General William E. DePuy*, ed. Richard M. Swain, Donald L. Gilmore, and Carolyn D. Conway (Fort Leavenworth, KS: Combat Studies Institute, 1995), 141, <https://www.armyupress.army.mil/Books/CSI-Press-Publications/Doctrine/#books-doctrine>.

³³⁷ For a succinct overview of how offense and defense ties in with air superiority, see: Phillip S. Meilinger, "Supremacy in the Skies," *Air Force Magazine* 99, no. 2 (2016), <https://www.airforcemag.com/issue/2016-02/>; Increasing concerns of being outpaced by Warsaw Pact fighter aviation throughout the 1980s drove USAF requirements to modernize and expand Tactical Air Command: Congressional Budget Office, *Tactical Combat Forces of the United States Air Force: Issues and Alternatives*, (Washington, DC: Congressional Budget Office, 1985), 18–24, <https://www.cbo.gov/sites/default/files/99th-congress-1985-1986/reports/85-cbo-008.pdf>.

to campaigns.³³⁸ In order to safeguard air superiority, an air force cannot “dig in” and protect the high ground, as is done in land defense. Hence, according to airpower theorists, these characteristics of air warfare signify that it is chiefly an offensive undertaking. The resulting literature and historical examples of air warfare facilitate a test of the offense-defense variables developed in this thesis. Do the variables exhibit explanatory power when considering the claims of airpower theorists? This section applies the offense-defense variables to air warfare to answer this question, exploring the modern technological and geographic factors that impact air warfare.

1. The Key Attributes of Air Warfare

The same features of air warfare that align it with cyber conflict—disparate, nonlinear, and asymmetric—also provide insight into the aspects of air warfare that incite offensive and defensive strategies. First, the disparate nature of air warfare requires rapid and precise information sharing amongst its practitioners, which makes the proper application of airpower a challenge. In order to cope with the vast expanses of air warfare, the USAF abides by a tenet of airpower that theorists refer to as “centralized control and decentralized execution.”³³⁹ By allowing mission execution to unfold at the tactical level of war, a decentralized approach to air warfare enables simultaneous operations to unfold throughout a theater, bypassing the linear fronts of traditional warfare. Completing operations in this nonlinear fashion bestows a profound benefit when wielding airpower in this decentralized way, as it capitalizes on the opportunity to strike multiple targets at once. USAF doctrine further stresses that these benefits include a high level of flexibility, as airpower can also achieve simultaneous effects across the spectrum of war—from the tactical level to the strategic.³⁴⁰ This feature of air warfare has led to an outpouring of theory on how best to employ airpower against an enemy, including a prominent approach

³³⁸ Phillip S. Meilinger, *10 Propositions Regarding Air Power* (Washington, DC: Air Force History and Museums Program, 1995), 15; Carter, *Airpower and the Cult of the Offensive*, 13.

³³⁹ U.S. Air Force, *AFD Vol I*, 67.

³⁴⁰ U.S. Air Force, *AFD Vol I*, 28; Theorists also stress how air power is nonlinear, meaning that threats need not be addressed in a sequential geographic basis: Meilinger, *10 Propositions*, 34–40; Carter, *Airpower and the Cult of the Offensive*, 8.

known as the effects-based approach to operations (EBAO). EBAO treats the adversary as a system to help identify the critical nodes during the targeting process.³⁴¹ Finally, the asymmetry in air warfare sprouts from the proposition that airpower inherently relies on a force-in-being at the outbreak of hostilities to mount a meaningful air war.³⁴² This is at least true in producing effects from the air, as the technology and skills required to produce, maintain, and operate aircraft do not emerge overnight. However, an air force-in-being at the outbreak of war is not a necessary condition to produce any effects in the air domain, a point repeatedly made to great powers like the U.S.

A review of airpower theory reveals three other features of air warfare pertinent to offense-defense theory: it is inherently dynamic, technology-driven, and reliant on the EMS. Air warfare is three-dimensional; however, this aspect does not make it unique.³⁴³ What makes the three-dimensional overlay of air warfare unique is that it is inherently dynamic, as adversaries cannot simply “park” their assets in the sky to hold an advantageous position, given today’s technology. Instead of emphasizing this feature as a dynamism, past airpower theorists have referred to air as a neutral medium, meaning that one must expend resources simply to enter the third-dimension, continue to expend resources to remain, then, eventually, exit the third-dimension.³⁴⁴ Next, airpower technology has become intertwined with the EMS.³⁴⁵ EMS is an expansion of the more traditional military view on electronic warfare (EW). While EW focuses on attack, protection, and support via radio-frequency (RF) assets, EMS more broadly includes all electromagnetic radiation, including infrared (IR) radiation, visible light, and the emerging

³⁴¹ David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare*, (Arlington, VA: Aerospace Education Foundation, 2001), <http://www.ausairpower.net/PDF-A/AEF-AFA-Effect-Based-Operations-D.A.Deptula-2001.pdf>; U.S. Air Force, *Air Force Doctrine Annex 3-0: Operations and Planning* (Maxwell AFB, AL: Lemay Center for Doctrine, 2016), 13–21, <https://www.doctrine.af.mil/>.

³⁴² Meilinger, *10 Propositions*, 17–18.

³⁴³ For instance, naval power can also exploit a three-dimensional approach.

³⁴⁴ Carter, *Airpower and the Cult of the Offensive*, 13.

³⁴⁵ U.S. Air Force, *AFD Vol I*, 25–27; David Stuckenberg, R. James Woolsey, and Douglas DeMaio, *Electromagnetic Defense Task Force 2.0*, ed. Donna Budjenska, LeMay Papers (Maxwell AFB, AL: Air University Press, 2019), viii–ix, <https://www.airuniversity.af.edu/AUPress/LeMay-Papers/>.

directed energy weapons.³⁴⁶ Most assets in air warfare are susceptible to attack or tracking through the EMS, making it an important element. The EMS and dynamic aspects of air warfare raise its third feature; namely, that airpower is a function of technology. Douhet emphasizes the tie between technology and airpower by referring to it as the “technical means of warfare” that “created a new battlefield.”³⁴⁷ Over the past decades, that trend continues as scholars point out that air warfare technologies have seemingly unearthed a military-technological revolution.³⁴⁸

a. Technology

Broadly speaking, airpower technology serves three core purposes: projecting capabilities, increasing the pace of information, and reducing risk to the warfighter.³⁴⁹ USAF headquarters recently provided a strategy for its acquisition and management of future technologies, in which it echoes these trends.³⁵⁰ Projection and airpower practically go hand-in-hand, as militaries affix mission equipment to aircraft with the express intent of sending the aircraft forward to accomplish operational objectives, such as employing ordinance. However, air-to-air refueling represents the emblematic technology of airpower projection, though austere ground refueling has also found an important niche, as well. While projection is the obvious use of disparate refueling technologies, the USAF also frequently leverages these technologies to increase mission loiter time, allowing assets to produce effects for an extended period. In the information age, a key use of projection is

³⁴⁶ U.S. Air Force, *AFD 3-51*, 2-3; RF energy includes RADAR (Radio Detection and Ranging) technology: U.S. Air Force, *Electronic Warfare Fundamentals* (Nellis AFB, NV: Air Warfare Center, 2000), Preface, 1-1.

³⁴⁷ Douhet, *Command*, 3-4.

³⁴⁸ Benjamin S. Lambeth, “The Technology Revolution in Air Warfare,” *Survival* 39, no. 1 (1997): 65, <https://doi.org/10.1080/00396339708442897>.

³⁴⁹ Lambeth, 66.

³⁵⁰ USAF development will focus on: 1. Global Persistent Awareness, 2. Resilient Information Sharing, 3. Rapid, Effective Decision-Making, 4. Complexity, Unpredictability, and Mass, and 5. Speed and Reach of Disruption and Lethality: U.S. Air Force, *Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*, (Washington, DC: U.S. Air Force Headquarters, 2019), iv, <https://www.af.mil/Portals/1/documents/2019%20SAF%20story%20attachments/Air%20Force%20Science%20and%20Technology%20Strategy.pdf>.

affixing sensors to aircraft or creating airborne battle management that can share updated information within the battlespace. In particular, the progress by the U.S. in ISR and its near real-time sharing capability shape the conduct of air warfare.³⁵¹ Finally, emerging technologies endeavor to reduce risk to airmen by allowing them to strike while limiting the adversary's ability to counter-attack. The noted innovations that allow this include stand-off weapons, stealth, and remotely-piloted aircraft.

In this analysis, it is vital to avoid mirror-imaging from a U.S. perspective, as U.S. adversaries do not develop air technology in the same fashion as the United States. Thankfully, there are a few ways to understand how air technology develops throughout the world, including post-war reflections and translated doctrine. This analysis reveals that U.S. adversaries typically seek to develop technology that is either resilient or can achieve force protection through passive means. Translated doctrine from the Cold War unveils a Soviet preference for U.S. technology, including enhanced command and control (C2), precision targeting, and stand-off capability.³⁵² However, the U.S.S.R. lagged behind the U.S. in fielding technologies to enact its ground-breaking "revolutionary-strike" doctrine, and the over-arching belief in U.S.S.R. civilian leadership was that the country could outmatch American technology with brute firepower and the Soviet population's resilience.³⁵³ In a similar fashion, the U.S.-NATO adversaries in Operations Desert Storm (Iraq) and Allied Force (Yugoslavia) both employed defensive technology that relied heavily on passive defense and resilience. In leveraging such technology, Iraq and Yugoslavia aimed to achieve wartime objectives by absorbing military strikes for a period longer than the U.S. could politically deal them. In Desert Storm, Iraq relied heavily on the mobility, dispersion, and concealment of its air assets to outlast American air strikes, while

³⁵¹ Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge," *Foreign Affairs* 75, no. 2 (1996): 28, <https://doi.org/10.2307/20047486>.

³⁵² Adamsky, *The Culture of Military Innovation*, 33–37.

³⁵³ Miriam D. Becker, "Strategic Culture and Ballistic Missile Defense: Russia and the United States," *Airpower Journal* 8, no. 1 (Special Edition) (1994), <https://www.airuniversity.af.edu/ASPJ/Archived-Editions/>.

also working vigorously to ensure redundant communications.³⁵⁴ In a more successful attempt to mitigate NATO air strikes during Allied Force, Yugoslavia also enacted technologies that dispersed and concealed its military assets, including redundant communication nodes.³⁵⁵ Furthermore, in a lesson gleaned from Desert Storm, the Serbian military mostly engaged in small unit tactics within rugged terrain to keep the bulk of its strength concealed.³⁵⁶ In other words, Yugoslavia efficiently combined its light technology and advantageous geography to outlast the NATO air strikes.

b. Geography

The geographical impact on air warfare primarily centers on the disparate and dynamic nature of air warfare, and militaries typically endeavor to overcome both issues with technology. First, employing airpower involves thinking about the entire theater of war and the effects needed across that whole theater to sway the outcome of war. An air campaign should target assets throughout an adversary's span of control regardless of location while also observing force protection in the process.³⁵⁷ Most airpowers employ a mixture of both aircraft and weapons to overcome the problems posed by any vast distances. Fielding aircraft and weapons with greater range represents one technological fix for airpowers that attempt to strike across vast the distances while protecting its own territory. Also, the dynamic nature of air warfare signifies that adversaries can strike at any time across one's defended territory, and defensive air patrols—referred to as Defensive Counter Air (DCA) in doctrine—must adjust to these rapid developments. DCA missions typically adapts to a dynamic or long-term situation through finding ways to increase loiter time, such as through air-to-air refueling.

³⁵⁴ Deptula, *Effects-Based Operations*, 15; Olsen, "Operation Desert Storm."

³⁵⁵ Stephen T. Hosmer, *The Conflict Over Kosovo: Why Milosevic Decided to Settle When He Did*, MR-1351-AF (Santa Monica, CA: RAND Corporation, 2001), 80, https://www.rand.org/pubs/monograph_reports/MR1351.html.

³⁵⁶ Hosmer, 82.

³⁵⁷ See Warden's "Five Cases of War": Warden, *The Air Campaign*, 20–24.

An often-underappreciated aspect of the overlap between air warfare and geography is the issue of aircraft basing—an issue that GPC has forced the USAF to confront in recent years.³⁵⁸ Arguably, the core issue of geostrategy in air warfare is deciding whether to concentrate air force units at a few bases or spread the units across many bases. Massing combat aircraft may allow for greater efficiency or immense firepower; however, it also creates a force protection problem. The Serbian army demonstrated this trade-off during Operation Allied Force; their forces were distributed to limit the effects of NATO air strikes, resulting in notable limitations on their offensive campaign in Kosovo.³⁵⁹ A keen example of a dispersed air defense system was that of the British Fighter Command during WWII, in which the fighter aircraft and the supporting airfields were well-spread to ensure their survival from Luftwaffe bombardment.³⁶⁰ Both of these cases also underscore the importance of communications for a force that is dispersed. On the opposite side of this model is that of the USAF in the Middle East over the past few decades, where it largely avoided dispersing its forces.³⁶¹ Because of the relative sanctuary of each base from insurgent attacks coupled with its impressive projection capability, the USAF has been able to operate from a small number of bases, achieving a high rate of efficiency in the process.³⁶²

2. Offense in Air Warfare

Offensive operations in air warfare are those efforts to seize control of airspace that is either neutral, contested, or defended by an opponent.³⁶³ It is a move to alter the status quo and can range from an air or missile attack to the repositioning of EMS assets to deny

³⁵⁸ Miranda Priebe et al., *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*, RR-2959-AF (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2959.html.

³⁵⁹ Hosmer, *The Conflict Over Kosovo*, 85–86.

³⁶⁰ Posen, *The Sources of Military Doctrine*, 98.

³⁶¹ Priebe et al., *Distributed Operations in a Contested Environment*, x.

³⁶² Priebe et al., x.

³⁶³ This does not include the routine passage of air power assets through international airspace, e.g., a transiting Carrier Strike Group. The key phrase in this definition is seizing control.

the use of contested airspace. USAF doctrine states that “the offensive aim is to act rather than react and to dictate the time, place, purpose, scope, intensity, and pace of operations.”³⁶⁴ Offensive air operations seek to gain the initiative in some way, projecting into an adversary’s territory, and forcing that adversary into a reactionary state. In order to achieve offensive effects, airpower often relies on its ability to mass and maneuver, bringing decisive effects over a short or unexpected time on an adversary.³⁶⁵ However, the bottom line is that seizing control of airspace equates to gaining air superiority. If in contested airspace, it involves actions to strengthen one’s influence over the contested airspace and achieve air supremacy, which is a heightened state of control relative to air superiority.³⁶⁶ An airpower endeavors toward air superiority by neutralizing the adversarial forces that can interfere with air operations.³⁶⁷

USAF doctrine lists four categories of offensive counterair (OCA), offering a general framework for the many forms of offensive air operations.³⁶⁸ The first is suppression of enemy air defenses (SEAD), which, as its name implies, involves nullifying the defensive measures that an adversary has in place. Given today’s technology, SEAD often revolves around either finding, destroying, or discouraging the use of RADAR, or disrupting command and control. Another offensive air operation is the offensive fighter sweep, which can extend beyond air-to-air engagements and include efforts to destroy lucrative ground targets. A third offensive air mission is a fighter escort of other assets vital to the joint mission, including high-value airborne assets (HVAA) or, as was the overwhelming use for bombers in WWII, aircraft en route to a target.³⁶⁹ Finally, offensive

³⁶⁴ U.S. Air Force, *AFD Vol I*, 53.

³⁶⁵ U.S. Air Force, 53.

³⁶⁶ Air supremacy is that degree of control of the air wherein the opposing force is incapable of effective interference within the operational area using air and missile threats: U.S. Department of Defense, *DOD Dictionary*, 15.

³⁶⁷ Warden, *The Air Campaign*, 23.

³⁶⁸ U.S. Air Force, *AFD 3-01*, 8-9; Another place that these are succinctly described: Meilinger, “Supremacy in the Skies,” 49.

³⁶⁹ HVAA tends to include items such as AWACS, tankers, or other high-demand low-density assets.

air operations can also encompass kinetic and non-kinetic attacks meant to preclude an adversary's use of air or missile capabilities.³⁷⁰

In his paper on offense and defense in air warfare, Carter brings up a crucial point on how the concept of air superiority may confuse the concepts of offense and defense.³⁷¹ An air force that establishes air superiority over an adversary's territory may have earned a level of air control; however, the airspace remains contested, and the side that seized air superiority continues to assume the offensive role. Gaining air superiority does not change the greater context of offense and defense in air warfare, and operations undertaken to further solidify control of the contested airspace still constitutes offensive air operations. A prime example that Carter offers is that of Operation Desert Storm, in which coalition air forces seized air superiority over Kuwait within a matter of weeks, thereby allowing coalition air operations to continue without prohibitive interference.³⁷² However, even after attaining air superiority, the airspace remained contested coalition air forces continued offensive operations as Iraq attempted to defend against coalition aircraft with surface-to-air missiles (SAMs) and air defense artillery (ADA).

3. Defense in Air Warfare

Defensive operations in air warfare consist of those actions that deny another force's air operations in or through one's airspace.³⁷³ The use of the term "air operation" is purposely vague to encompass any effect projected through the air, including an EMS or missile attack. While air defense is passive in the broad context, it includes a barrage of activity to strengthen one's control over a given airspace without altering the status quo. These activities include the protection of not only air targets but also ground and sea targets from an air attack, seeking to limit an adversary's use of the air to produce effects.

³⁷⁰ U.S. Air Force, *AFD 3-01*, 8.

³⁷¹ Carter, *Airpower and the Cult of the Offensive*, 11.

³⁷² Carter, *Airpower and the Cult of the Offensive*, 11; The air campaign of Operation Desert Storm began on 17 January 1991, and by 26 January Iraq's control of the air had to degraded to the point that Saddam Hussein ordered all Iraqi combat aircraft to evacuate to Iran: Olsen, "Operation Desert Storm," 177–86.

³⁷³ A similar definition is found here: Carter, *Airpower and the Cult of the Offensive*, 9.

Airspace defense unfolds in two general categories—active and passive—and doctrine defines it as a systemic effort and labels that effort air and missile defense (AMD).³⁷⁴ Active AMD is the direct action that a defensive system uses to counter or destroy a threat or negate or diminish its effects and generally includes the use of aircraft, SAMs, or ADA to counter the threat or EMS to negate the effects.³⁷⁵ Passive AMD is all measures other than active AMD to nullify or reduce the effects of hostile air and missile threats.³⁷⁶ Examples of passive AMD include efforts or capabilities to camouflage, concealment, deception, hardening, dispersion, mobility, and detection and warning. Many modern air defenses consist of a whole system designed to repel air attacks, known as an integrated air defense system (IADS), which doctrine defines as an aggregated collection of sensors, communications, and AMD weapons coordinated by a central command system.³⁷⁷ Air defense requires this type of dispersed system, as maintaining control and protecting a vast airspace requires detailed monitoring and efficient tasking of one's defensive forces.

4. Do the Experts Perceive Air Warfare as Offensive or Defensive?

A survey of airpower theorists and doctrine reveals that the overall perspective is that airpower is chiefly an offensive form of warfare. Starting with Douhet and his famous dictum that “the airplane is the offensive weapon par excellence,” early airpower theorists argued that aircraft would reverse the defensive nature of firepower.³⁷⁸ Historically, many viewed firepower as emblematic of a keen defense, as it allows defenders to find entrenchments and repel numerous attackers. Douhet argues that because fortifications cannot repel the reach or speed of aircraft, firepower became the tool of the offense in air

³⁷⁴ U.S. Department of Defense, *JP 3-01*, ix.

³⁷⁵ Active AMD can take on more nuance than these categories; however, the general idea holds: U.S. Air Force, *AFD 3-01*, 9–10.

³⁷⁶ U.S. Air Force, 10.

³⁷⁷ U.S. Department of Defense, *JP 3-01*, xvii–xviii.

³⁷⁸ Douhet, *Command*, 14.

warfare.³⁷⁹ Many years after Douhet, John Warden, who went on to lead ground-breaking shifts in air doctrine while at Air University, writes, “[w]hichever side first wins air superiority will reap significant and perhaps overwhelming advantages.”³⁸⁰ With this notion came a stream of doctrine and literature that supports the idea of taking the initiative in air warfare to seize control of the air and, thereby, setting the pace of battle. Among this body of literature is Meilinger’s *10 Propositions Regarding Air Power* that proclaims that “[a]ir Power is primarily an offensive weapon,” as “careful routing and stealth technology make it extremely difficult to anticipate and prepare for an air assault.”³⁸¹ Also, Meilinger’s cohort included John Carter, the author of a paper on the air warfare offense-defense balance. Much like other air theorists, Carter concludes that Clausewitz’s famous dictum that defense is inherently stronger than offense does not apply to air warfare.³⁸² His conclusion arises from the inability of air defense assets to stake out and protect the high ground, which is the result of all aircraft needing to eventually land back on the ground for refueling and returning the air to a neutral state.³⁸³ Carter does admit that his conclusion rests on the nature of current technology, as defenses cannot currently defend a vast air expense in a manner that counteracts the inherent strengths of an air offense.³⁸⁴ Finally, the current USAF doctrine continues to emphasize the importance of using airpower as an offensive weapon.³⁸⁵ Simply put, its speed, range, and attacking power make it suited to gaining the initiative over an opponent to win military victories. The experts indicate that the offense-defense balance in air warfare tilts toward the offensive side of the scale.

³⁷⁹ Douhet, 13–14.

³⁸⁰ Warden, *The Air Campaign*, 14–16.

³⁸¹ Proposition Number Three: Meilinger, *10 Propositions*, 14.

³⁸² “Because airpower defense has no advantage of position and time accrues to the detriment of both offense and defense, airpower defense enjoys no inherent advantage”: Carter, *Airpower and the Cult of the Offensive*, 18.

³⁸³ “Because airpower defense has no advantage of position and time accrues to the detriment of both offense and defense, airpower defense enjoys no inherent advantage”: Carter, 18.

³⁸⁴ Carter, *Airpower and the Cult of the Offensive*, 15.

³⁸⁵ U.S. Air Force, *AFD Vol I*, 53.

5. Information Advantage—Air Warfare

The employment of airpower builds the perception for its users that they can seize a state of information superiority, thereby controlling the flow of information—a point illustrated by doctrine and historical examples. Recall that the information advantage is an operational edge conferred by the flow of information, and technology that purports to offer the information advantage is offensive in nature. In other words, airpower’s capacity to affect the information superiority tips the offense-defense balance toward the offense in air warfare. Airpower can shape the informational landscape by either providing a means of gathering and sharing intelligence or crippling an adversary’s flow of information.

Operating in the third dimension gives airpower the ability to generate a flow of information that militaries are keen to capture and rapidly disseminate. Hallion notes how air assets provide the “advantage of vantage,” granting its beneficiaries with a comprehensive and timely view of the battlespace.³⁸⁶ This advantage has translated into an emphasis across the joint force on the importance of airborne intelligence collection. The profound benefits of airborne intelligence systems comprise a significant part of the 2–0 joint doctrinal intelligence series, even going so far as to state: “airborne systems are primary sources for imagery collection used to produce [geospatial intelligence].”³⁸⁷ History also underscores this point, as the first use of aircraft in warfare was in a reconnaissance role to gain the informational edge.³⁸⁸ Some of the most celebrated war-time aircraft found their beginnings in reconnaissance, including the German Fokker *Eidecker*, Britain’s de Havilland *Mosquito*, and a host of premier aircraft from Lockheed’s fabled Skunk Works.³⁸⁹ Now, the predominant and ever-growing use of unmanned aerial vehicles (UAVs) centers around ISR.

³⁸⁶ Hallion, “Air and Space Power,” 378.

³⁸⁷ GEOINT expanded to “geospatial intelligence”: U.S. Department of Defense, *JP 2-03*, IV-6.

³⁸⁸ Hallion, “Air and Space Power,” 378.

³⁸⁹ Hallion, “Air and Space Power,” 378; Steve Pace, *The Projects of Skunk Works: 75 years of Lockheed Martin’s Advanced Development Programs* (Minneapolis, MN: Voyageur Press, 2016).

In modern warfare, airborne intelligence has become a vital part of offensive operations, including collection and dissemination. To coordinate its counterair battles, the USAF relies heavily on its airborne Theater Air Control System (TACS), comprised of three well-known C2 platforms: the Airborne Warning and Control System (AWACS), the Joint Surveillance Target Attack RADAR System (JSTARS), and the RIVET JOINT.³⁹⁰ These platforms combine a host of sensors, analysis suites, and battle management capabilities to provide a guiding hand during high-volume air battles.³⁹¹ Without this capability, the USAF would charge into enemy territory without a central nervous system, leaving each unit to fight uncoordinated and without the pertinent information. With an efficient battle-managing system that simultaneously collects and processes information, then decides and tasks, an air force becomes emboldened to strike out offensively to seize control of the air.

Some telling examples of how airpower facilitates the gathering and dissemination of information are the air campaigns of Operation Desert Storm, Operation Iraqi Freedom, and Iraq's 1990 invasion of Kuwait. In both Desert Storm and OIF, the U.S.-led coalitions faced Iraq's imposing IADS, composed of a redundant central control system, the "sixth largest air force in the world," and an array of Soviet-designed SAM batteries that fired over 1,660 missiles in OIF, alone.³⁹² Moreover, Iraq employed impressive passive solutions to absorb the coalition's airstrikes, including innovative means of repairing damage, and hiding or protecting its critical assets.³⁹³ Despite the difficulties posed by the Iraqi IADS, the coalition's air C2 and ISR structure achieved an unmatched display of information gathering and sharing in both Desert Storm and OIF, resulting in a coordinated air campaign that integrated fires, precisely struck vital targets, and minimized friendly losses.³⁹⁴ This structure successfully coordinated over 5,700 air strikes in Desert Storm

³⁹⁰ U.S. Air Force, *AFD 3-01*, 22-23.

³⁹¹ U.S. Air Force, 22-23.

³⁹² Murray, "Operation Iraqi Freedom," 288; Olsen, "Operation Desert Storm," 113.

³⁹³ Keaney, "Surveying Gulf War Airpower," 32; Murray, "Operation Iraqi Freedom," 284-85.

³⁹⁴ Murray, "Operation Iraqi Freedom," 283.

and controlled over 700 fighter/bomber aircraft in OIF.³⁹⁵ During the post-war reflections of OIF, one Iraqi General commented he was unable to execute many of his missions because his troops harbored a paralyzing-level of fear of precision air strikes.³⁹⁶ In the lead-up to Desert Storm in August 1990, the Iraqi military also captured a similar offensive edge by leveraging reconnaissance air during its two-day conquest of Kuwait.³⁹⁷ Iraq's offensive against Kuwait leaned heavily on an intelligence effort to enable its air assault, including reconnaissance flights in the months before the operation.³⁹⁸

While airpower enables the gathering of information, it also equips a military with the ability to disrupt an adversary's flow of information, again demonstrated within the borders of Iraq over the past few decades. First, during Iraq's 1990 invasion of Kuwait, the helicopter assaults undertaken by Iraqi special forces included the seizure of air traffic facilities and the broadcasting system in Kuwait City to relay coup messaging to Kuwait's population.³⁹⁹ The coalition campaign in Operation Desert Storm similarly halted the flow of information for the Iraqi military. The air campaign consisted of a three-track approach to neutralize the Iraqi IADS, and the first track centered on disabling the Iraqi's C2 system.⁴⁰⁰ The coalition accomplished through Tomahawk cruise missile and F-117 precision strikes and on the relays connecting Iraq's air defense sectors to central headquarters.⁴⁰¹ On one particular mission, a helicopter assault force crossed into Iraqi airspace and inserted a special operations team that destroyed a critical RADAR station guarding Baghdad.⁴⁰² By some estimations, the coalition strikes on Iraq's C2 infrastructure

³⁹⁵ Olsen, "Operation Desert Storm," 187; Murray, "Operation Iraqi Freedom," 285.

³⁹⁶ Murray, "Operation Iraqi Freedom," 291.

³⁹⁷ Pesach Malovany, *Wars of Modern Babylon: A History of the Iraqi Army from 1921 to 2003*, trans. Ronna Englesberg (Lexington, KY: University Press of Kentucky, 2017), 503–16.

³⁹⁸ Malovany, 509–10.

³⁹⁹ Malovany, 510–11.

⁴⁰⁰ Olsen, "Operation Desert Storm," 183–84.

⁴⁰¹ Olsen, 184.

⁴⁰² Olsen, 184.

forced the individual defense sectors into an autonomous mode, shattering the integrated nature of the IADS and spurring on the coalition's offensive campaign.⁴⁰³

While the information advantage can incite offensive air operations, the inverse is also true: a lack of information can deter offensive actions and move the balance toward the defense. Precision strikes and its reliance on accurate information illustrate this point.⁴⁰⁴ The world has grown accustomed to the lower rates of collateral damage associated with precision weapons, and international norms now place extreme pressure on militaries to consistently achieve these low rates. This pressure causes militaries to undertake the arduous task of building a precise intelligence picture and carefully verifying each target before any attack, and, in the end, many militaries are now “gun shy” without overwhelming intelligence about their targets. Hence, a lack of information guides preferences away from the offense and toward the defense. A telling example within air warfare unfolded during NATO's Operation Allied Force campaign against Serbia, in which pilots received instructions to cancel strikes if unable to obtain “positive” identification of their targets. Meeting the strict identification standards proved difficult, and aircraft regularly returned home without expending the intended ordnance.⁴⁰⁵ Moreover, to avoid collateral damage, political officials regularly instructed NATO aircrew to employ 500-lb laser-guided GBU-12 bombs, as opposed to the 2,000-lb GBU-27s that targeting experts recommended to achieve desired effects.⁴⁰⁶ Throughout numerous air campaigns, information superiority elicited a preference for offensive campaigns, and, conversely, limits on information impinged the inclination for offensive action.

⁴⁰³ Olsen, 184.

⁴⁰⁴ Murray, “Operation Iraqi Freedom,” 280.

⁴⁰⁵ Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment*, MR-1365-AF (Santa Monica, CA: RAND Corporation, 2001), 48, https://www.rand.org/pubs/monograph_reports/MR1365.html.

⁴⁰⁶ Lambeth, *NATO's Air War for Kosovo*, 48.

6. Decisive Effects—Air Warfare

One of airpower's defining offensive features is its ability to maneuver in a way that masses forces and produces devastating effects. Importantly, militaries can only capitalize on these layered effects by seizing the initiative or risk finding themselves on the receiving end of an adversary's layered effects. In the context of the offense-defense balance, the concept of decisive effects refers to the degree to which technological and geographic factors elicit the impression that offensive actions can overwhelm an adversary. Airpower's capacity to produce decisive effects tips the offense-defense balance toward the offense. In particular, airpower can produce decisive effects through three powerful abilities: mount a surprise mass attack, select targets throughout a theater, and layer effects. Within each of these abilities, historical examples illustrate how the decisive effects of airpower can overwhelm an adversary's defenses and often unable to mount a counter-offensive.

The speed, range, and versatility of airpower allow it to mass forces and mount surprise attacks, drastically reducing the chance of a meaningful response from the target. USAF doctrine repeatedly makes this point by pointing to airpower's flexibility and ability to concentrate—a point echoed by airpower theorists who also suggest that air's unlimited avenues of approach compound this feature.⁴⁰⁷ One of the premier examples of an air offensive that achieved surprise and devastating effects was Japan's mass air attack on Pearl Harbor.⁴⁰⁸ The characteristics of the attack that made it decisive were countless. However, two significant characteristics stand-out under close examination: the concentration of mass fires and the great distance from which the attack began. Another example of a surprise mass attack occurred during the Six Days War, in which the Israeli Air Force (IAF) was able to leverage this style of attack to overcome the quantitative

⁴⁰⁷ Meilinger, *10 Propositions*, 16; Air power can seize the initiative to set the terms of the battle, leverage flexibility and versatility to achieve surprise, and concentrate to dominate: U.S. Air Force, *AFD Vol I*, 28–29, 59, 73.

⁴⁰⁸ Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

advantage of the Arab Coalition Air Forces.⁴⁰⁹ To carry out this attack, the IAF simultaneously launched all of its serviceable combat aircraft—numbering a bit over 200—in a sunrise raid, concealing the mass launch through deceptive measures that created the illusion of being a typical training day.⁴¹⁰ The objective of this raid was to achieve air superiority in one day by destroying the Arab Air Force while still parked on the ramp, then moving to target the critical RADAR and SAM batteries. The IAF successfully caught their adversary's aircraft while still vulnerable on the ground, destroying over 400 out of the target 500 aircraft along with several ground targets, as well.⁴¹¹ Because of this surprise mass attack, the consensus among historians is that the IAF achieved air superiority in a mere twelve hours.⁴¹²

Another key to airpower's decisive effects is its ability to strike targets throughout the theater and at multiple levels of war, robbing the adversary of the initiative.⁴¹³ Airpower theorists highlight this through the concept of the effects-based approach to operations (EBAO).⁴¹⁴ Because airpower can impact targets throughout the theater, EBAO encourages military planners to concentrate on the effects needed to achieve the desired end-state and produce those effects by assigning capabilities to targets. If the desired end-state is incapacitating the Iraqi IADS, then one of the effects is cutting the communications between air defense sectors, much as the Desert Storm air campaign was able to do through targeted strikes deep in Iraqi territory.⁴¹⁵ Hence, airpower's ability to strike targets through a theater builds the perception that war planners can merely articulate effects that require strikes deep within enemy territory, and the air force will unleash those effects. As

⁴⁰⁹ Shmuel L. Gordon, "Air Superiority in the Israel-Arab Wars, 1967–1982," in *A History of Air Warfare*, ed. John Andreas Olsen (Washington, DC: Potomac Books, 2010), 130–35.

⁴¹⁰ Gordon, 130–35.

⁴¹¹ Gordon, 131–33.

⁴¹² Gordon, 131–33.

⁴¹³ U.S. Air Force, *AFD Vol I*, 53.

⁴¹⁴ Deptula, *Effects-Based Operations*; U.S. Air Force, *AFD 3–0*, 13.

⁴¹⁵ See the selected targets in the first twenty-four hours of the war: Deptula, *Effects-Based Operations*, 1.

foreshadowed in the preceding example, effects-based operations unfolded in an astonishingly effective manner in Operation Desert Storm.⁴¹⁶ Using this approach, the U.S.-led coalition air campaign was able to execute its three-track approach of first dismantling the IADS C2 system, then suppressing Iraq's RADAR-guided SAMs, and finally unleashing a wide array of deep attacks meant to discourage any Iraqi response.

Finally, airpower permits the ability to layer effects, which can decisively overwhelm an adversary's defenses. Though USAF doctrine does not discuss "layering" per se, it does emphasize massing effects to seize the initiative.⁴¹⁷ The concept of layering effects implies that airpower can apply pressure on an adversary in multiple ways, ensuring that all its possible responses to the attack become neutralized. A keen example of layering effects occurred during the USAF and U.S. Navy (USN) air strike on Libya in April 1986, named Operation El Dorado Canyon. The strike came as a response to Muammar Gaddafi's belligerent endorsement of terrorist acts against the U.S., and the mission achieved the political objectives as Gaddafi softened his rhetoric after the strike.⁴¹⁸ During the strike, the joint air offensive had to plan against Libya's relatively sophisticated air-defense system. However, it was able to overcome Libya's IADS by layering several effects through airpower: including airborne jamming, anti-radiation missiles, the bombing of SAM sites, and low-level precision strikes.⁴¹⁹ It was this aspect of airpower—the layering of effects to negate any possible defensive response from Libya—that led the U.S. to undertake this offensive strike.

7. Exposure—Air Warfare

The technological and geographic factors of air warfare collectively create the perception that a military can undertake offensive actions while minimizing risk to its attacking units. This facet of air warfare aligns with the exposure variable of the offense-

⁴¹⁶ See the selected targets in the first twenty-four hours of the war: Deptula, 1.

⁴¹⁷ U.S. Air Force, *AFD Vol I*, 73.

⁴¹⁸ Joseph T. Stanik, "Welcome to El Dorado Canyon," *Proceedings* 122 (1996): 61.

⁴¹⁹ Stanik, 58–59.

defense balance proposed in this thesis. Airpower's ability to limit exposure, and thus risk, tips the offense-defense balance toward the offense in air warfare. The technological and geographic factors of air warfare limit exposure in four ways: layering effects, varying altitude, reducing the EMS signature, and stand-off.

Already in the previous section of the air warfare analysis, airpower reveals how layering effects can protect attacking units by overwhelming a defensive system. In the course of overwhelming a defensive system, airpower mitigates the risk otherwise assumed by attacking units. For instance, the U.S. mitigated risk in Operations El Dorado Canyon and Deliberate Force by layering multiples effects: suppressing enemy SAMs through anti-radiation missiles, infrared countermeasures, or jamming equipment.⁴²⁰

Varying altitudes serves as a common method to protect attacking aircraft by either flying high to avoid the engagement zones of many ground-based threats or using low-level or terrain-masking to fly below RADAR coverage. In other words, a military may choose to employ these tactics to limit an adversary's ability to target its aircraft, decreasing exposure, and driving up perceptions that offensive strategies are feasible. For instance, NATO employed high-altitude attacks on Serbia, placing a 15,000-foot "hard-deck" restriction on participating aircraft to avoid the infrared SAMs and ADA batteries, as both of could only marginally threaten aircraft at higher altitudes.⁴²¹ In terms of low-level flying, one of the best examples emerged from the Six Days War. To gain surprise and enable its aircraft to reach their targets, the IDF flew its initial wave of attacks at very low levels toward Egypt and the Sinai Peninsula to under-fly the Arab RADAR coverage.⁴²² Low-level flying worked for the IDF, who lost no aircraft during the ingress of its initial attack and achieved surprise against their adversaries.

⁴²⁰ Stanik, "El Dorado Canyon."; In Operation Deliberate Force: "With their safety largely secured by their altitude, speed, and SEAD support, the pilots of [U.S.] aircraft had the luxury of maneuvering into the proper release 'basket' of each of their weapons": Owen, "Operation Deliberate Force," 220.

⁴²¹ Lambeth, *NATO's Air War for Kosovo*, 48.

⁴²² Gordon, "Air Superiority," 132.

Another conventional means of reducing the risk to attacking air units is the growing array of technical measures that modern air forces employ to counteract EMS tracking of their aircraft, the most famous of which is stealth technology. AMD relies heavily on the EMS to detect, identify, and track attacking aircraft and then guide munitions meant to destroy those aircraft.⁴²³ Denying an air defense the use of EMS helps reduce the exposure of attacking aircraft. Stealth technology, which employs low observable principles to avoid detection by RF signals, played a central role in the air offensives of Operations Desert Storm and Allied Force.⁴²⁴ In both operations, stealth aircraft led airstrikes with little fear of being shot down by the Iraqi and Serbian IADS, as both relied heavily on RF signals to defend against attacking aircraft.⁴²⁵ While stealth offers protection by minimizing the aircraft signature, an air offensive may also counteract EMS tracking of attacking aircraft by conducting an electronic attack of the defenses through jamming. This style of risk mitigation occurred during Operation El Dorado Canyon, when EF-111A aircraft and EA-6B aircraft conducted stand-off jamming of Tripoli's RADAR defenses, enabling the safe ingress of strike aircraft.⁴²⁶ Lastly, the EMS also encompasses the infrared light spectrum, which air defenses often use to track the intense heat sources emitted by aircraft. However, many air forces have discovered ways to protect offensive aircraft from infrared threats, including infrared countermeasures, which can defeat an infrared-guided missile by jamming the missile's infrared seeker.⁴²⁷ Thus, airpower technology offers several ways to reduce the EMS exposure of attacking aircraft.

⁴²³ U.S. Department of Defense, *JP 3-01*, III-20.

⁴²⁴ Avionics Department, *Electronic Warfare and Radar Systems Engineering Handbook*, 1–1.19; Rao and Mahulikar, "Integrated Review of Stealth Technology and Its Role in Airpower," 632–35.

⁴²⁵ F-117 at the lead of the attack on the Iraqi air defense system: Olsen, "Operation Desert Storm," 184; B-2 aircraft the first to penetrate Serb defenses on OAF opening night: Lambeth, *NATO's Air War for Kosovo*, 80; Rao and Mahulikar, "Integrated Review of Stealth Technology and Its Role in Airpower," 632–35.

⁴²⁶ Stanik, "El Dorado Canyon," 59.

⁴²⁷ U.S. Government Accountability Office, *Electronic Warfare: DOD Should Select Most Cost-Effective Infrared Countermeasure System* (Washington, DC: U.S. Government Accountability Office, 1998), 2, <https://www.gao.gov/archive/1998/ns98002.pdf>.

A third common way that airpower technology limits the exposure of attacking units is through stand-off capability, which currently involves two distinct approaches: weapon range or sending UAVs into harm's way. First, weapon range implies that the attacking aircraft can launch the weapon (typically a munition) from beyond the range of adversarial systems. As an example, NATO relied heavily on stand-off weapons for its opening volley during Operation Allied Force, launching the Tomahawk and air-launched cruise missiles to degrade the effectiveness of Serbia's air defenses before shorter-range strikes from crewed aircraft.⁴²⁸ Now that UAVs have grown in capability while falling in cost, they tend to offer an appealing method to create effects without putting troops in harm's way. UAVs can encompass a wide array of platforms, from remotely-piloted aircraft such as the Global Hawk to small pre-programmed drones. Moreover, these pilotless systems can produce an abundance of effects in air warfare, including attacks, surveillance, deception, jamming, or decoy.⁴²⁹ With the rise of stand-off technologies in air warfare, exposure of attacking units continues to fall, thereby increasing offensive inclinations.

8. Insulation—Air Warfare

While insulating factors do exist in air warfare, those factors do not tip the balance toward the defense, as opposing offensive aspects exist that overcome the defensive factors. In air warfare, insulation impacts the offense-defense balance through both technological or geographic factors, as outlined by AMD doctrine.⁴³⁰ At an increasing pace, technological factors serve as the insulation from airborne attacks, while geography only aids a select number of nation-states. The defensive technologies that best insulate are those that make targeting difficult, especially keen use of mobility and EMS passive detection techniques. Unfortunately, while these defensive techniques serve as an aid to insulation, they ultimately do not deter offensive air campaigns. Instead, they only complicate the targeting process and require additional measures to mitigate risk for the

⁴²⁸ Lambeth, *NATO's Air War for Kosovo*, 47.

⁴²⁹ U.S. Department of Defense, *JP 3-01*, IV-6.

⁴³⁰ U.S. Department of Defense, ix-x.

offense. In terms of geography, a reliable network of allies and vast oceans both represent geographic features that aid a select few countries. In contrast, countries with dispersed assets suffer from the burden of trying to protect a vast area.

Two technological factors help drive insulation in air warfare: defensive mobility and passive measures. However, for both factors, the over-arching purpose is the same—avoiding the detection of the offense. First, when defensive ground assets are mobile, and the host country includes a plethora of civilian vehicles, separating the desired ground targets from civilian vehicles becomes a daunting task.⁴³¹ The enormity of this task has the potential to impinge or possibly deter an offensive air campaign. Next, passive measures can also limit the ability of the offense to find and target air defenses, thereby increasing the difficulty of conducting an air offense. For an example of technology that aids passive defense, the more advanced countries have turned to passive detection within the EMS. Passive EMS detection involves tracking an offensive aircraft by avoiding the emission of any RF signals to detect aircraft and executing a receive-only tracking technique of the electronic signals emitted by the intruding aircraft.⁴³² While both of these technological advances do help to sway the offense-defense balance, both fail to address the problem of offensive stand-off or the decisive effects brought by an air offensive. Further, a keen air offense may find ways to overcome these defensive technologies.⁴³³

Next, historical examples demonstrate how a lack of geographic insulation can incite offensive inclinations in air warfare. The Six Days War and Iraq's invasion of Kuwait, in particular, illustrate this point. In both cases, the countries playing defense had virtually no geographical insulation. In the Six Days War, Israel bordered four of the Arab league nations—Egypt and Syria—and no significant terrain blocked Israel's surprise

⁴³¹ Alan J. Vick et al., *Aerospace Operations Against Elusive Ground Targets* MR-1398-AF (Santa Monica, CA: RAND Corporation, 2001), 57–64, https://www.rand.org/pubs/monograph_reports/MR1398.html.

⁴³² W. Stimson George et al., *Stimson's Introduction to Airborne Radar*, Third ed. (Edison, NJ: SciTech Publishing, 2014), 520–40.

⁴³³ Vick et al., *Aerospace Operations*, 66–80.

attack.⁴³⁴ This geographic disposition incited a pre-emptive attack from Israel on Arab Air Forces. Iraq's 1990 invasion of Kuwait also had to contend with virtually no geographical problems, as Kuwait bordered Iraq, had minimal terrain, and offered multiple attack vectors for the Iraqi air assaults.⁴³⁵ In a case in which geography aided the defense, Britain's Fighter Command assembled a celebrated air defense in 1940 during the Luftwaffe's attempt to bombard the British Isles into submission. A crucial part of the air defense included Britain's RADAR coverage that gave Fighter Command ample time to respond to a Luftwaffe air raid and the distance that the limited Luftwaffe needed to cover for each of its attacks.⁴³⁶ What the Battle of Britain ultimately shows is that a confluence of technology and geography *can* tip air warfare into the favor of the defense. However, given the current technology explored in the preceding paragraphs, it is difficult to say whether technology and geography can once again attain that level of air defense anywhere in the world.⁴³⁷

9. Criticality—Air Warfare

The use of airpower yields the perception that it can strike at critical nodes of an adversary's security apparatus—a point illustrated by the logical underpinnings of strategic air attack and historical examples of airstrikes on foreign leadership. This thesis defines criticality as the degree to which targetable objects appear necessary to an adversary's security or welfare, and targetable objects that appear critical stoke offensive inclinations. Consequently, airpower's capacity to strike critical infrastructure throughout a theater tips the offense-defense balance toward the offense in air warfare.

The logic of strategic attack—to focus airpower on the most critical items of the adversary—underlines how critical items appear exposed to offensive airpower, and the opening airstrikes of Operation Desert Storm and OIF exemplify this point. Since the early

⁴³⁴ Gordon, "Air Superiority," 133.

⁴³⁵ Malovany, *Wars of Modern Babylon*, 509–11.

⁴³⁶ Posen, *The Sources of Military Doctrine*, 94–104.

⁴³⁷ Perhaps, the United States represents one of the few places in the world where technology and geography pose considerable insulation for any would-be attackers.

days of airpower theory, strategic attack emerged as a tempting use of airpower, as Douhet suggests that it allows one to bypass an enemy's defenses and bomb the supporting populace into submission.⁴³⁸ In modern doctrine, theorists stress that airpower is inherently strategic, as it can, "hold an enemy's strategic centers of gravity and critical vulnerabilities directly at risk immediately and continuously."⁴³⁹ In the case of Operation Desert Storm, the Central Command (CENTCOM) commander General Schwarzkopf tasked his coalition air component to first and foremost conduct "a strategic air campaign to establish air superiority over Iraq and incapacitate its regime."⁴⁴⁰ The Iraqi air defense system and its regime's ability to command the Iraqi military appeared critical, and airpower offered a means to strike both of these items in Schwarzkopf's first phase of his campaign. Again, in OIF, F-117 aircraft carried out some of the initial strikes, and their repeated target over the first few days was Saddam Hussein, as he still appeared critical to Iraq's defense against the U.S. invasion.⁴⁴¹ Unfortunately, Saddam Hussein proved elusive though most of 2003, and while the USAF repeatedly struck targets that it believed to contain the Iraqi regime, the intelligence prompting each strike proved incorrect.⁴⁴² However, the point remains that airpower offers an avenue to attack critical items.

10. Resilience—Air Warfare

For the final variable, resiliency, airpower can often attain a high level of resilience in its defenses as covered in the "Insulation" section; however, its offensive assets tend to have a low level of resilience. Because of the low resilience that typifies offensive airpower, the offense-defense balance toward the offense as adversaries will perceive that they can gain an edge by striking the other's offensive assets, first. Resilience denotes the ability to recover from an offensive strike, and a perceived inability to recover stimulates

⁴³⁸ Douhet, *Command*, 31–83.

⁴³⁹ U.S. Air Force, *AFD Vol I*, 34.

⁴⁴⁰ Olsen, "Operation Desert Storm," 182.

⁴⁴¹ Murray, "Operation Iraqi Freedom," 287.

⁴⁴² Murray, 287.

offensive action. Both aircraft and pilots account for a vital part of an airpower's offensive capability, and both are vulnerable on the ground difficult to replace.

The low resiliency of aircraft and pilots emerges in history and theory. Aircraft parked on the ground make an easy target, which drove the IDF's surprise attack in the Six Days War. During the initial attack on the Arab League, the IDF targeted the parked aircraft to make it difficult for the Arab League to strike back at Israel.⁴⁴³ Because the fleet of aircraft was difficult to replace, the IDF quickly grasped air superiority through this strategy. Next, airpower theorists, such as Warden, emphasize the importance of maintaining a pool of trained personnel for air warfare, as it can take years to train individuals proficient in the needed skills.⁴⁴⁴ Furthermore, Warden offers a few different attack strategies to attrite an enemy's aircrew supply, thereby eliminating their airpower capability.⁴⁴⁵ The implication is that even though the passive and mobile insulating technologies of air defense help improve resiliency, offensive air assets generally achieve a relatively low resiliency level. This low level of offensive resilience tips the balance toward the offense.

11. Conclusion—Air Warfare

A review of the offense-defense variables suggests that air warfare indeed favors offensive actions, as argued by numerous airpower theorists. Airpower (a) permits the seizure of the information advantage while impacting an adversary's communications; (b) can produce layered and overwhelming effects on attack; (c) employs numerous methods to limit exposure; (d) often struggles to produce effective insulation from attack; (e) permits the striking of adversary's critical assets; and (f) the offensive air assets often lack resilience. Thus, this case study of the offense-defense balance in air warfare aligns the offense-defense theory within this thesis to airpower theorists in a paradigmatic fashion.

⁴⁴³ Gordon, "Air Superiority," 132.

⁴⁴⁴ Warden, *The Air Campaign*, 49–50.

⁴⁴⁵ Warden, 50.

D. IRREGULAR WARFARE

Even a short review of IW literature highlights its defining element—complexity. As a violent struggle for control of a population, IW presents a myriad of problems to any state facing an insurgency. Because IW involves violence, it typically necessitates some form of a military intervention to provide security. The complexity arises, in part, because IW has historically required a much broader role for militaries than merely fulfilling a “security” role. U.S. military doctrine acknowledges that IW requires an overlapping combination of efforts, including counterterrorism (CT), UW, foreign internal defense (FID), counterinsurgency (COIN), and stability operations.⁴⁴⁶ There is never one line of effort to win an IW campaign—a successful IW campaign relies on the full spectrum of a nation’s power, demanding fervent coordination between multiple agencies and foreign partners.⁴⁴⁷ Moreover, an IW campaign seldom runs its course in the short timeframes exhibited by air warfare. IW is inherently protracted and typically signifies an endurance test of both sides.

One of the foremost drivers of complexity within IW is the near absence of all the traditional distinctions found in “regular warfare,” including declarations of war, political boundaries, and the clear delineation of combatants from non-combatants.⁴⁴⁸ This attribute of IW extends to offense and defense. Rarely does either side—insurgency or state—undertake a strict offensive or defensive strategy. Instead, their campaigns tend to contain elements of both. An insurgency is likely to conduct operations that are offensive in nature, as well as defensive actions. Their offensive operations may include terrorist-style attacks or illegal activities to build revenue, while their defensive activities chiefly involve concealment. Likewise, state actors may also employ a mix of offensive and defensive operations. For instance, a state conducting counter-guerrilla operations may need to

⁴⁴⁶ U.S. Department of Defense, *IW JOC*, v2.0, 17. Because of the overlaps in IW, terms such as “insurgent” and “guerrilla” may be used interchangeably in the literature, but insurgent refers to any person seeking revolutionary change, while a guerrilla is an insurgent directly using violence.

⁴⁴⁷ U.S. Department of Defense, *JP 1, Change 1*, I-6.

⁴⁴⁸ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, (Arlington, VA: Potomac Institutes for Policy Studies, 2007), 7, <https://www.potomac institute.org/publications>.

conduct offensive raids to clear an area of insurgent activity, or it may require defensive actions, such as increasing security through the hardening of critical targets. However, an analysis of the offense-defense balance requires a distinction.

Hence, to analyze the offense-defense balance in IW, this thesis defines offensive IW as *initiating an insurgency*, while defensive IW comprises *undertaking a counterinsurgency*.⁴⁴⁹ The reason for this resonates from the central purpose of offense-defense theory, which is to identify a condition that can presage war. Generally speaking, the outbreak of an insurgency signifies the start of conflict and a move to alter the status quo, meaning that as the insurgency starts, so does the violence. It is the insurgents whose net campaign objectives are active in nature, and the state whose net objectives are passive. Further, U.S. doctrine defines insurgency as “the organized use of subversion and violence to seize, nullify, or challenge political control of a region.”⁴⁵⁰ The word “challenge” in this definition aligns the doctrine with this chapter’s distinction in the offensive and defensive roles of IW, as challenge implies a move to displace the reigning political power. Thus, an insurgency initiates the struggle for control of a population by taking the offensive and seeking change. For the offense-defense analysis in this section, the technological and geographic factors that tip the balance toward the offense are akin to those that enable insurgencies.⁴⁵¹

This distinction between offense and defense in IW extends beyond the internal strife of failing nation-states and directly intertwines with GPC. IW offers an attractive means for great powers to covertly seize the initiative against their competitors or gain an

⁴⁴⁹ This distinction resembles the same distinction made in a RAND report: Eric V. Larson et al., *Assessing Irregular Warfare: A Framework for Intelligence Analysis*, MG-668-A (Santa Monica, CA: RAND Corporation, 2008), 14, <https://www.rand.org/pubs/monographs/MG668.html>.

⁴⁵⁰ U.S. Department of Defense, *Joint Publication 3-24: Counterinsurgency* (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2018), I-1, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

⁴⁵¹ Admittedly, a whole host of factors play into the rise of insurgencies, including culture, conditions, governmental power, timing, etc. This analysis only aims to study how technology and geography may sway the IW offense-defense balance. For traditional studies on insurgencies, see: Chalmers A. Johnson, *Revolutionary Change* (Stanford, CA: Stanford University Press, 1982); Nathan Leites and Charles Wolf, Jr., *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts* (Santa Monica, CA: RAND Corporation, 1970).

edge on the international stage. Joint doctrine even emphasizes that irregular threats often emerge from state actors who employ irregular methods.⁴⁵² One of the consequences of GPC is the outbreak of multiple insurgencies facilitated by the dominant nation-states to subvert each other's influence. The United States is not innocent in this regard and has a long history of manipulating political conditions abroad by providing support to foreign paramilitary operations.⁴⁵³ Furthermore, U.S. military doctrine and public law both list UW as a core Special Operations activities, implying that the U.S. maintains a capability to enable foreign insurgencies.⁴⁵⁴ Finally, IW has played a direct role in the missteps of several great powers: Britain's fall in the American Revolution, the French empire's stumbling efforts in the Peninsular War, the failure of the U.S. in the Vietnam War, and the Soviet defeat in the Soviet-Afghan War.⁴⁵⁵ Though all of these historic examples emerge under different headlines, including guerrilla warfare, small wars, or COIN, each case fits the basic definition of IW—a struggle for control of a population. Because each of these events represents a significant failure on the part of a powerful nation-state, understanding the factors that can encourage IW campaigns is a valuable endeavor. How does the offense-defense balance figure into these decisions to launch IW campaigns?

1. The Key Attributes of Irregular Warfare

Before launching into the features of IW that directly impact the offense-defense balance, it is first essential to explore the concept of *controlling a population*, as it embodies the core struggle of IW. Generally speaking, IW is a competition between a state and an insurgency, and the two entities compete in two primary arenas: the battle for

⁴⁵² U.S. Department of Defense, *IW JOC*, v2.0, 9–10.

⁴⁵³ Though paramilitary operations imply that the support is covert in nature, the U.S. has declassified a string of these historical operations: William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington, KY: University Press of Kentucky, 2004).

⁴⁵⁴ U.S. Department of Defense, *JP 3-05*, xi; *Title 10 U.S.C. § 167*, 170.

⁴⁵⁵ Piers Mackesy, *The War for America, 1775–1783* (Cambridge, MA: Harvard University Press, 1964); Charles Oman, *A History of the Peninsular War: 1807–1809, From the Treaty of Fontainebleau to the Battle of Corunna*, Project Gutenberg e-book ed., VII vols., vol. I (Oxford, UK: Clarendon Press, 1902); Stanley Karnow, *Vietnam: A History* (New York: Penguin Books, 1984); Crile, *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History*.

political power and the manipulation of security. The political battle is typically one for legitimacy: a struggle to prove which side can meet the needs of the people. The crucial issues for a population resonate from their value inventory—or their values, norms, and expectations—guiding how the population determines when conditions are acceptable.⁴⁵⁶ If a ruling government fails to provide conditions that its population deems acceptable, a void opens, allowing an insurgency to question the state’s legitimacy. The noted COIN theorist David Galula writes that the state and insurgents then become locked in a contest to influence the neutral section of the population, expanding political control to edge out their opponents.⁴⁵⁷ In terms of security, both sides demonstrate their ability to provide meaningful security for their constituents while attempting to discredit their opponent’s ability to do the same. This competition to provide security sparks violent clashes and constitutes much of the violence associated with IW. In this context, U.S. doctrine clarifies what it means to establish adequate security in IW: “creating conditions that are predictable and acceptable—a clear set of rules that are consistently enforced under which [people] feel they can reasonably survive.”⁴⁵⁸ Whichever side convincingly offers this level of security tends to control not only the physical environment but also the resident population. When people sense that their well-being is at stake, they often cast aside their political preferences and orient to the side that credibly promises this level of control. As a ruling state fails to address the vital issue of security, a void opens for a nascent insurgency, and control of the population is up for grabs.

In terms of defining the two sides, IW is a struggle between a force-in-being (the state) and a growing insurgent force. The state inherently enjoys a force advantage while the insurgent force inherently enjoys an information advantage.⁴⁵⁹ This definition aligns

⁴⁵⁶ U.S. Department of Defense, *JP 3-24*, III-11.

⁴⁵⁷ David Galula, *Counterinsurgency Warfare: Theory and Practice* (London, UK: Praeger, 2006), 53–54.

⁴⁵⁸ U.S. Department of Defense, *JP 3-24*, IV-17.

⁴⁵⁹ Greg Wilson, “The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines,” in *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, ed. Michael Freeman and Hy Rothstein (Monterey, CA: Naval Postgraduate School, 2011), 28, <https://calhoun.nps.edu/handle/10945/780>.

with those at the beginning of this chapter, while also capturing the crux of the problem: the state's military force lacks an opposing fielded force to strike.⁴⁶⁰ The insurgent force is less powerful in terms of direct resources, training, and organization, meaning that one of their chief objectives during its nascent period is to survive and grow by establishing a political base.⁴⁶¹ The insurgent force may not outwardly fight for another state; however, that does not preclude it from acting as a proxy or gaining resources from established powers. Also, the information advantage enjoyed by the insurgents stems from its small size and ability to act on a minimal set of rules. Their networks and infrastructure lack the official brandings that characterize those of the state. For instance, the insurgent forces may conceal themselves and their weapons, while the state must accommodate its forces in bases and use the state budget to acquire weapons.

Two other facets of IW that pertain to the offense-defense balance is that IW unfolds in a protracted manner and favors the indirect approach. Insurgents often design their campaigns to be protracted, which gives them time to grow their operations, pursue long-term gains, and wear down the state.⁴⁶² In other words, insurgents exploit the benefits of time against the state, as a prolonged campaign may insidiously cause the population to believe the state incapable of addressing the insurgent problem. Lastly, IW lends itself to the indirect approach—avoiding direct conflict until the strategic conditions are so overwhelming that victory is assured.⁴⁶³ This feature of IW does not suggest that an insurgency or COIN campaign will avoid battle altogether; in fact, skirmishes are an

⁴⁶⁰ As a brief reminder: IW includes conflict that does not involve “regular” troops on both sides.

⁴⁶¹ This phase of a guerrilla war is termed the “strategic defensive” by Mao in his writings on guerrilla warfare, which does counter the ideas of offense and defense in this Chapter; however, the grand context is important: Mao Tse-tung, *Selected Military Writings of Mao Tse-tung* (Seattle, WA: Praetorian Press, 2011), 86–88, e-Book.

⁴⁶² Mao emphasizes that protracted wars benefit the guerrillas for these reasons: Mao Tse-tung, *Selected Military Writings*, 93–132; This warning is echoed in doctrine: U.S. Department of Defense, *JP 3-24*, II-1.

⁴⁶³ B.H. Liddell Hart, *Strategy*, Revised ed. (Auckland, NZ: Pickle Partners Publishing, 2016), Google Play, 377, <http://www.pp-publishing.com/>, e-Book.

essential part of both.⁴⁶⁴ However, the two sides spar indirectly, for instance, by undermining the messaging of the opposition or providing public services that the other is unable to provide. This indirect approach levels the playing field between a state and a growing insurgency. Because it is asymmetric, IW is a tempting method by which various actors can pursue offensive goals in the international system.

a. Technology

Because IW involves competition between a state and an insurgency, this same dichotomy offers a suitable way to view the technology of IW. States often employ technology to bolster surveillance, ensure unity of effort, and maintain supporting logistics. Perhaps the most significant frustration of a state during an IW campaign is its lack of information about the adversary. The adversary has no borders, wears no distinguishable markings, and its reach and resources are a constant question mark. In response to this issue, many governments have spent tremendous resources on technological systems to fill this information void, including the surge in U.S. spending on ISR platforms for the COIN campaigns in OIF and Operation Enduring Freedom (OEF).⁴⁶⁵ In the end, a state can gain information on its adversary; however, this only occurs as the insurgent grows in power, creating a paradox for the state. As the IW campaign intensifies, the state also needs a way to share information internally. As a complex and multifaceted effort, IW requires a uniform and persistent response from multiple government agencies, including the military, law enforcement, and political leaders. In terms of the specific military efforts, a common strategy is to embed or place its forces amongst the indigenous population to adopt an approach that understands the population.⁴⁶⁶ States employ information sharing systems to keep these efforts aligned, and cyberspace has increasingly filled this need for

⁴⁶⁴ T. E. Lawrence, *The Evolution of a Revolt*, Combat Studies Institute Reprint ed. (Fort Leavenworth, KS: Army University Press, 1920), 15, <https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/evolution-of-a-revolt.pdf>.

⁴⁶⁵ The U.S. push to produce ISR is detailed by former Defense Secretary Robert Gates in his memoir: Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Alfred A. Knopf, 2014), 140–49.

⁴⁶⁶ Eric T. Olson, “A Balanced Approach to Irregular Warfare,” *The Journal of International Security Affairs* 16 (2009).

many states.⁴⁶⁷ Lastly, IW requires the state to maintain control in its disparate regions and provide support to its population to keep adequate influence, leading to the need for effective logistics. Because insurgents can threaten logistical efforts, the state often leverages more protective transportation methods, such as air transport.⁴⁶⁸

An insurgency often leans on technology both to carry out its operations in a clandestine manner and as a mobilizing platform to build its legitimacy.⁴⁶⁹ A leading RAND monograph on rebellions views insurgencies as a system, converting its endogenous and exogenous inputs into outputs to enact violence on its target government, recruit and train new insurgents, and provide administration for the population that it controls.⁴⁷⁰ A systems view on insurgencies allows one to envision its technological processes and how best to disrupt its operations. It also underscores the importance of clandestine operations to an insurgency; they must train, communicate, and provide logistics in a manner that avoids detection by the state. To avoid detection, insurgents must appear like the rest of the country's populace, which encourages the use of technology that bears a striking resemblance to the rest of the country. If the rest of the populace uses mules for transport, then the insurgents' logistics must also heavily rely on mules. In terms of mobilizing platforms, insurgents often rely on those that allow them to reach a broad audience and those that allow them to coerce. The tools of cyberspace increasingly fill this role; however, the importance of weaponry continues unabated. Even if a population rallies around a grievance posted on the Internet, they eventually must form an insurgency around those with weapons.⁴⁷¹

⁴⁶⁷ U.S. Department of Defense, *JP 3-24*, III-14 - III-16, IV-7.

⁴⁶⁸ Air transport has long been an important component of IW, or, as IW was formerly known to the U.S. military, small wars: U.S. Marine Corps, *Small Wars Manual (Reprint of 1940 Edition)* (Washington, DC: Department of the Navy, 1940), 9–1.

⁴⁶⁹ Doctrine holds that these are some of the primary goals of an insurgency: U.S. Department of Defense, *JP 3-24*, II-1.

⁴⁷⁰ Leites and Wolf, *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts*, 34–35.

⁴⁷¹ Mao Tse-tung, *Selected Military Writings*, 135.

b. Geography

Geography is profoundly important within IW. It can provide the insurgents with sanctuary, complicate logistics, foment cultural divides, and determine how the violence unfolds. Each of these topics, individually, represent vastly important issues, leading to literature on each, and this section need not repeat the discussion here.⁴⁷²

However, one cognitively useful geographic issue for different IW campaigns is whether the insurgency is rural-based or urban-based. The 2006 version of the U.S. Army's Field Manual 3-24 dwells on this difference.⁴⁷³ In a rural-based insurgency, the movement tends to enjoy a relatively secure base of operations, owing to the geographically separated territories that afford the insurgents a pocket of control. An urban-based insurgency often requires a higher degree of clandestine operations and basing. In these cases, the insurgents tend to organize in a cellular fashion, as they lack territorial control to organize extensively. However, an urban-based insurgency is always within physical striking distance, posing many challenges for the state. Of course, this divide helps understand a basic geographic factor, and chances are high in today's urbanized world that an insurgency can contain elements of both: rural and urban.

2. Offense in Irregular Warfare

Already, this chapter defines offense in IW as initiating a violent insurgency, providing the necessary framework for an analysis of the offense-defense balance. The next vital question is how might insurgencies originate and then progress? On the question of

⁴⁷² J. J. Zasloff, *The Role of the Sanctuary in Insurgency: Communist China's Support to the Vietminh, 1946–1954*, RM-4618-PR (Santa Monica, CA: RAND Corporation, 1967), https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM4618.pdf; Graham H. Turbiville, Jr., *Logistic Support and Insurgency: Guerrilla Sustainment and Applied Lessons of Soviet Insurgent Warfare*, JSOU Report 05–4 (Hurlburt Field, FL: Joint Special Operations University, 2005), <https://www.hsdl.org/?abstract&did=476313>; Michael L. Davidson, "Culture and Effects-based Operations in an Insurgency" (SAMS thesis, U.S. Army Command and General Staff College, 2005), <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.866.204&rep=rep1&type=pdf>.

⁴⁷³ U.S. Army, *Field Manual 3-24: Counterinsurgency* (Washington, DC: Department of the Army Headquarters, 2006), 1–7, <https://www.hsdl.org/?abstract&did=468442>.

origins, theorists consistently maintain that insurgencies start with a cause.⁴⁷⁴ A cause provides a means for recruitment at a point when the insurgents otherwise lack any resources, and recruits often join at great personal risk. At the early stages of an insurgency, their most vital task is to grow, mobilizing to the point of gaining legitimacy.⁴⁷⁵ An insurgency's cause, and later its political goals, becomes more than just a means of facilitating mobilization; it becomes the insurgency's center of gravity. While a population's top priority is often physical security, other important issues can raise grievances, laying the foundation for an insurgency's cause. Doctrine suggests that these issues can range from human rights to community resources access (migration routes, grazing land), while the seminal COIN expert Robert Thompson reminds his readers that the cause may not emanate from a failure of government but from a foreign source (e.g., colonialism).⁴⁷⁶ Thompson further warns that a keen insurgency will always find some issue to grow resentment.⁴⁷⁷ His warning implies that if a state's opponents truly desire social unrest, it will endeavor to create the conditions that can produce a cause, thereby, fostering an insurgency.

From the cause, a revolution often progresses through three strategic stages as described by Mao Tse-tung: defensive, stalemate, and counteroffensive.⁴⁷⁸ Mao was a founding member of the Communist Party of China (CPC), which traces its revolutionary roots to the Tsinan Massacre in 1928, and he saw through China's revolutionary change when he stood in Tiananmen Square and proclaimed the formation of the People's Republic

⁴⁷⁴ Galula, *Counterinsurgency Warfare*, 11–13; Robert Thompson, *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam*, Studies in International Security (New York: Frederick A. Praeger, 1966), 21.

⁴⁷⁵ Gordon H. McCormick and Frank Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," *Third World Quarterly* 28, no. 2 (2007): 295–96, <https://doi.org/10.1080/01436590601153705>.

⁴⁷⁶ U.S. Department of Defense, *JP 3-24*, III-11; Thompson, *Defeating Communist Insurgency*, 21.

⁴⁷⁷ Thompson, 21.

⁴⁷⁸ Mao Tse-tung, *Selected Military Writings*.

of China in 1949.⁴⁷⁹ His writings on guerrilla warfare and revolution have since made him one of the quintessential sources on the topic, and some theorists have termed his approach “people’s war” or “protracted war.”⁴⁸⁰ The strategic defensive entails building support for the insurgency as the state has a stronger military. Strategic stalemate then arises as the insurgents gain an equal footing with the state, and the insurgency can focus on guerrilla warfare. Finally, the insurgents move to the counteroffensive when they believe their military strength greater than the state’s and can undertake conventional operations. This model provides a useful way to conceptualize an IW campaign; however, it is important to note how this model fits the rural environment of China in Mao’s time, alleviating the CPC of some of the clandestine concerns that can plague modern urban insurgencies.

In today’s global environment, insurgent networks have emerged that seek revolutionary change on a global scale and do not simply conform to a state’s borders.⁴⁸¹ Prominent examples of these groups include Al-Qaeda or the Islamic State (ISIS) as both operate pockets of resistance in multiple Middle Eastern countries. Their cause predominantly stemmed from the ideology espoused by religious nationalism, and their overarching “target” has often been secular nationalism, marking a sharp turn from the Cold War issue of communism versus democracy.⁴⁸² Though their cause failed to emanate from a single grievance, these networks often found local pockets of resistance and fed on their grievances, supplying resources as long as it undermined their international goals. In the end, these networks still took root in local movements that conformed to many of the

⁴⁷⁹ Mao traces the Communist movement in China to the Tsinan Massacre in 1928: Mao Tse-tung, *Selected Military Writings*, 2; 1 October 1949, Mao declares the formation of the People’s Republic of China: Walter Sullivan, “Reds Proclaim a Republic In China; Chou Is Premier,” *New York Times*, 2 October 1949, 1, <https://www.nytimes.com/1949/10/02/archives/reds-proclaim-a-republic-in-china-chou-is-premier-chinese-republic.html>.

⁴⁸⁰ Gordon H. McCormick, “People’s Wars,” in *Encyclopedia of Conflicts Since World War II*, ed. James Ciment et al. (Armonk, NY: Sharpe Reference, 1999), 23.

⁴⁸¹ U.S. Army, *FM 3-24 (2006)*, 1–4.

⁴⁸² Mark Juergensmeyer, *The New Cold War? Religious Nationalism Confronts the Secular State*, First Paperback ed., Comparative Studies in Religion and Society (Berkeley, CA: University of California Press, 1994).

historic methodologies of insurgencies, allowing states to wield COIN strategies that proved successful in the past.

3. Defense in Irregular Warfare

By now, this analysis of the offense-defense balance in IW makes clear that the counterinsurgent position equates to defense, given their stance that the status quo should prevail and no violent struggle should occur, at all. A potential misnomer from this delineation is that the counterinsurgent, as the net defender, conducts operations that are strictly reactionary. In other words, the insurgents are always the first movers, and the state requires overt threats to their legitimacy before any prompt into action can occur. This is an incorrect supposition. COIN heavily relies on active defense, which implies proactive steps to prepare for threats or bolster one's defense. By continual active engagement with its population, a state can set conditions that disallow an insurgency. Similarly, Thompson laments the term "counterinsurgency," as it also implies waiting for an insurgency to arise before addressing the problem.⁴⁸³ So, how might a state conduct COIN?

In response, Thompson offers his five principles of conducting COIN, which highlight how a state should compete in the struggle for political power.⁴⁸⁴ Thompson emphasizes a total government approach that focuses on winning over the population—a message echoed Galula in his four "Laws of Counterinsurgency Warfare."⁴⁸⁵ First, for Thompson, a state must have a clear political aim, meaning that they must continue to address the administrative needs of the country by maintaining or improving its institutions. Second, the government must abide by its own laws, or risk the slippery slope of appearing overly-authoritative. Third, the COIN effort must operate according to a unified plan across the various governmental agencies. Fourth, to address the root cause and win the political battle, the COIN should focus on the political subversion over the guerillas. Finally, as the insurgency adopts a guerilla element, the state should consolidate support in its base

⁴⁸³ Thompson, *Defeating Communist Insurgency*, 50.

⁴⁸⁴ Thompson's five principles: Thompson, 50–58.

⁴⁸⁵ Galula, *Counterinsurgency Warfare*, 50–55.

regions, first. As demonstrated by his principles, Thompson stresses that the main effort in COIN is engaging the population, convincing them that the state institutions are strong and can provide for the peoples' needs, more so than the insurgents can. Similarly, Galula's four laws of successful COIN emphasize the same theme, noting that the state must employ a multi-pronged political campaign once adequate security is in place.⁴⁸⁶ His second law, for instance, states that "support is gained through an active minority;" by active minority, Galula refers to those actively engaged in either supporting or countering the insurgents' cause, as opposed to the "neutral majority."⁴⁸⁷ Galula's second law implies that the state should indirectly engage the insurgents, by acting through the active minority that favors the state to expand control into the neutral portions of the population. In terms of messaging during the political battle, doctrine offers the idea of a "COIN narrative" to bridge the divide between the state and disaffected portions of the population. The COIN narrative should, "contextualize what the population experiences, legitimizing counterinsurgent actions and delegitimizing the insurgency ... to overwhelm the insurgency narrative."⁴⁸⁸ As a struggle for control of the population, the political contest inherent to IW is a critical aspect for the state.

While the political battle rages, a parallel contest to provide adequate security for the populace emerges, including the immediate needs and the undertaking of counteroffensives against the insurgents. In terms of immediate needs, Thompson's fifth principle stresses the importance of focusing first where the state is strongest, shoring up support in the well-developed regions to leverage their resources in the anti-guerilla campaign.⁴⁸⁹ The 2006 COIN Field Manual likens this to "stop [ping] the bleeding" in an analogy drawn from medical treatment: "[t]he goal is to protect the population, break the insurgents' initiative and moment, and set the conditions for further engagement."⁴⁹⁰ From

⁴⁸⁶ Galula, 55–56.

⁴⁸⁷ Galula, 53.

⁴⁸⁸ U.S. Department of Defense, *JP 3-24*, III-9.

⁴⁸⁹ Thompson, *Defeating Communist Insurgency*, 57.

⁴⁹⁰ U.S. Army, *FM 3-24 (2006)*, 5–2.

the initial actions, multiple approaches exist. U.S. doctrine emphasizes a systems-style approach, aiming to isolate the insurgents by expropriating their cause, cutting their logistics, and reducing their means of garnering finances.⁴⁹¹ Another approach includes the “clear-hold-build” concept, wherein security forces clear an area of overt insurgent activity, then maintain its security while re-building the state’s ability to meet the population’s needs.⁴⁹² If not carefully done, the security measures in IW can undermine the efforts of the state. As emphasized on the previous pages, the population must believe that the provided security amounts to an acceptable means of survival.

4. Is IW Offensive or Defensive? Expert Opinion and Data

Unfortunately, the IW literature does not present the clearest picture of whether the experts perceive IW as inherently offensive or defensive. With regard to the literature, Galula offers the only clear opinion: “There is, finally, a further reason to assume that the list of revolutionary wars is not closed. It is certainly easier to launch an insurgency than to repress it.”⁴⁹³ Because this analysis identifies insurgencies as the offensive side of IW, Galula’s view suggests that IW favors the offense. As a practical writer, Thompson does not offer a definitive estimation on the perceived ease of running either an insurgent or COIN campaign. He does open up his book by reminding readers that the insurgents’ struggle is an uphill battle that can deter the most intrepid insurgent.⁴⁹⁴ However, Thompson then admits that finding a cause to spur insurgencies is rarely a difficult task, and a convincing cause naturally builds momentum for insurgencies.⁴⁹⁵ Adding to this array of views, the Naval Postgraduate School’s Gordon McCormick and Frank Giordano contend that the initial stages of an insurgency are quite difficult, especially the task of

⁴⁹¹ U.S. Department of Defense, *JP 3-24*, III-13 - III-15.

⁴⁹² U.S. Army, *FM 3-24 (2006)*, 5-18 - 5-22.

⁴⁹³ Galula, *Counterinsurgency Warfare*, 99.

⁴⁹⁴ Thompson, *Defeating Communist Insurgency*, 13.

⁴⁹⁵ “There is always some issue which has an appeal to each section of the community, and, even if dormant, an inspired incident may easily revive it in an acute form”: Thompson, 21.

mobilizing the initial following.⁴⁹⁶ Thus, the scholarship on IW does not provide a consistent view on the relative ease of offense versus defense.

However, while the literature is not decisive on the matter, the balance sheet demonstrates that IW has become the preferred form of conflict, and the military view is that modern conditions both encourage and empower insurgencies. The aforementioned prevalence of IW, alone, speaks to this reality. The outbreak of over 80 IW-style campaigns since WWII is striking as a Correlates of War summation notes only 38 inter-state conflicts in that same time frame.⁴⁹⁷ The prevalence of IW-style conflicts suggests that there is no shortage for its demand, and actors show a propensity to initiate insurgencies to further their political goals. Moreover, the U.S. military view on IW emphasizes how actors may prefer assuming the insurgent role:

Thinking, highly adaptive actors will take advantage of the trends outlined above and employ a combination of methods to include criminality. Non-state actors will be a significant component of the future operating environment, and irregular wars will be more common than major regular or nuclear wars. Non-state actors will become increasingly powerful as they extend their reach and capabilities through globalization and advancing technology, including cyber-warfare; chemical, radiological, biological, or nuclear weapons; and sophisticated information campaigns ... Also of increasing concern are rogue states that use proxies, which allow the state to distance itself from actions and achieve strategic aims simultaneously.⁴⁹⁸

Put succinctly, modern conditions encourage insurgencies, greatly leveling their playing field with state actors. The military does not hold this view on its own; political leaders, CIA analysts, and present-day scholars reach this same assessment.⁴⁹⁹ As a result,

⁴⁹⁶ “As an empirical rule, mobilisation is generally quite difficult during the early stages of the struggle, when the insurgency is small”: McCormick and Giordano, “Things Come Together,” 295–96.

⁴⁹⁷ Sarkees and Wayman, “Resort to War: 1816–2007.”

⁴⁹⁸ U.S. Department of Defense, *IW JOC*, v2.0, 12.

⁴⁹⁹ White, “Some Thoughts on Irregular Warfare.”; Robert M. Gates, “A Balanced Strategy: Reprogramming the Pentagon for a New Age,” *Foreign Affairs* 88, no. 1 (2009): 32; Bruce Hoffman, “The ‘Cult of the Insurgent’: Its Tactical and Strategic Implications,” *Australian Journal of International Affairs* 61, no. 3 (2007): 312, <https://doi.org/10.1080/10357710701531503>.

the entering argument for the offense-defense balance in IW is that actors generally prefer the offense.

5. Information Advantage—IW

The information advantage is inherent for the offense—the insurgents—in IW. They have a small footprint and remain hidden, while the state’s security infrastructure is on full display.⁵⁰⁰ However, not only does the operational information favor insurgencies, modern technology now provides additional means for the insurgents to seize the initiative and manipulate the flow of information. Technological and geographic factors that elicit efforts to seize the information advantage tip the offense-defense balance toward the offense, and today’s flood of information levels the playing field for insurgents by permitting them access to common information tools while inundating the state. The information age has largely overwhelmed the world’s governments, and many states pay a hefty price to try to absorb the excessive amount of information. A review of the literature alongside recent examples reveals that modern technology and geography permit insurgencies to leverage the flow of information.

First, modern tools including social media allow for disinformation campaigns aimed at causing social unrest, while attempts by various governments to contain the public flow of information often frames them as overly-authoritarian. Disinformation campaigns serve as a tool to inject doubt and a lack of trust in our information systems.⁵⁰¹ Though they act on behalf of a specific government, Russian disinformation “trolls” demonstrate how modern technology allows any committed following to anonymously undermine a state’s message by injecting several versions of the same story into the information flow. On the flip side of this point, a state that chooses to sensor the flow of information to its citizenry runs the risk of appearing overly authoritarian.⁵⁰² For instance, the great firewall

⁵⁰⁰ Wilson, “The Mystic Diamond,” 28.

⁵⁰¹ Peter W. Singer and Emerson T. Brooking, *Like War: The Weaponization of Social Media* (Boston, MA: Houghton Mifflin, 2018).

⁵⁰² Freedom House, “Authoritarian Reach,” *Freedomhouse.org*, ed. Arch Puddington, Nate Schenkkan, and Sarah Cook 2020, accessed 3 April 2020, <https://freedomhouse.org/issues/authoritarian-reach>.

of China may appear to squelch out the information that displeases Chinese political leaders.⁵⁰³ However, the action, in and of itself, is a form of information that could hurt the state in a COIN campaign. Messaging still flows in one form or another, and attempts to position the state as the center-point of all traffic simply paints the state in an authoritarian light and produces innovative ways to bypass the state's information system.

Second, the digital age allows insurgent groups new avenues into recruitment, training, and financing, a point demonstrated by trans-regional terrorist groups, including Al-Qaeda and ISIS. The Internet now provides a path for insurgent groups to globally reach prospective terrorists and supporters, provide encouragement and assistance, and, thereby, boost their recruitment capability.⁵⁰⁴ Indeed, ISIS portrayed an acute ability to leverage social media in their recruitment efforts, even pulling from previously remote places, as one estimate placed over 750 Britons in Syria at the height of their caliphate.⁵⁰⁵ The agile nature of modern information flow has also given rise to non-state actors who organize in networks instead of the traditional hierarchical formation, led by "great revolutionary leaders."⁵⁰⁶ Insurgencies now often operate in multiple nodes, spurred on by ideology instead of physical leaders, and, as a result, can mold to changes in their environment. The Internet also provides insurgents the ability to pass training material, such as ideology or coaching, or even pass assignments. In 2003, Al-Qaeda had success running a virtual university, offering a collection of manuals and videos for their members abroad.⁵⁰⁷ Finally, cyberspace tools permit a myriad of ways to raise, spend, or hide their financial

⁵⁰³ Elizabeth C. Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown," *The Guardian*, 29 June 2018, <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>.

⁵⁰⁴ Dorothy E. Denning, "Terror's Web: How the Internet is Transforming Terrorism," in *Handbook of Internet Crime*, ed. Yvonne Jewkes and Majid Yar (New York: Routledge, 2011), 201–02, <https://www.routledgehandbooks.com/doi/10.4324/9781843929338>.

⁵⁰⁵ Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media," *Society* 54, no. 2 (2017): 138, <https://doi.org/10.1007/s12115-017-0114-0>.

⁵⁰⁶ John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 2001), 3–7, https://www.rand.org/pubs/monograph_reports/MR1382.html.

⁵⁰⁷ Denning, "Terror's Web," 203–04.

operations through information theft.⁵⁰⁸ For instance, a small collection of Al-Qaeda operatives amassed more than \$3.5 million in fraudulent credit card activity through cyberspace, showing how digital information can uplift a nascent insurgency as it grows in power.⁵⁰⁹

Finally, while cyberspace, social networks, urbanization and other modern phenomenon permit new ways for insurgents to interact with information, these items have simply added to the toolkit already available to insurgents.⁵¹⁰ Arquilla and Ronfeldt presaged these conditions by noting, “[o]lder technologies, like human couriers, and mixes of old and new systems may do the job in some situations.”⁵¹¹ Consequently, the growing means of passing information only increases the information pipelines that a state must observe to build an adequate intelligence picture.

6. Decisive Effects—IW

The offense-defense variable of “decisive effects” suggests that the offense-defense balance should tip toward defense in IW, due to the IW’s inherently protracted nature. However, because the prolonged campaigns negatively impact both the offense and defense in IW, the variable is effectively a wash. Recall that the notion of decisive effects denotes the extent to which technology and geography produce beliefs that offensive actions can overwhelm an enemy. While geography may lead an insurgency to believe that decisive actions are attainable, the technology of IW simply does not tip the balance in either direction. No technology exists that can influence, deter, coerce, or motivate an entire population in a decisive way to the extent needed by an IW campaign. The former USSOCOM commander Eric Olson argues that “[IW] operations are not decisive.

⁵⁰⁸ Denning, 206.

⁵⁰⁹ Brian Krebs, “Terrorism’s Hook Into Your Inbox,” *Washington Post*, 5 July 2007, <https://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html>.

⁵¹⁰ Denning notes six areas in which the Internet has created new avenues of approach for terrorists: Denning, “Terror’s Web.”; Singer and Brooking cover the 5 Ds of how social networks spread discord: dismiss, distort, distract, dismay, and divide: Singer and Brooking, *Like War*, 107.

⁵¹¹ Arquilla and Ronfeldt, “Advent of Netwar,” 11.

Enduring results come from the indirect approaches.”⁵¹² Moreover, doctrine underscores how no one line of effort wins an IW campaign; it requires a series of parallel efforts.⁵¹³ In other words, the decisive effects in IW are a confluence of conditions, leaders, cultures, organizations, and technologies; victory only comes after years of enduring efforts. These arguments apply to both the insurgent and COIN campaigns—the offense and defense—nullifying the impact of decisive effects on the offense-defense balance in IW.

Almost by definition, both insurgencies and COIN campaigns are protracted, and no single stroke can overwhelm either side of an IW engagement. Influencing a population requires a concerted and “long-haul” approach.⁵¹⁴ Galula and Thompson both note how the prospective long-haul can deter either side of an IW contest. Galula writes, “Protracted guerrilla activity, so cheap to carry out and so expensive to suppress, may eventually produce a crisis in the counterinsurgent camp, but it could just as well alienate the population and disintegrate the [insurgent’s] united front.”⁵¹⁵ Meanwhile, Thompson paints a grim picture for the insurgent in the opening lines of his book, illustrating the hardships that specifically face each insurgent. Over the course of a long IW struggle, many insurgents abandon their cause as they, “become disillusioned with the cause or plain exhausted with the protracted struggle.”⁵¹⁶ The drawn-out nature just becomes too much for many insurgents and even can deter them at the beginning of the struggle. In short, IW theorists underscore that the protracted nature of IW can hurt both sides.

The overarching use of technology in IW is not to assist the insurgent to achieve decisive effects, and modern technology has not changed that reality. The chief purpose of an insurgent’s technology is to conceal and prolong the campaign, not conduct an overwhelming strike. Obtaining technology that could quickly win battles only draws the

⁵¹² Olson, “A Balanced Approach to Irregular Warfare,” 3.

⁵¹³ U.S. Department of Defense, *IW JOC*, v2.0, 17.

⁵¹⁴ R. W. Komer, *The Malayan Emergency in Retrospect: Organization of A Successful Counterinsurgency Effort*, R-957-ARPA (Santa Monica, CA: RAND Corporation, 1972), v, <https://www.rand.org/pubs/reports/R957.html>.

⁵¹⁵ Galula, *Counterinsurgency Warfare*, 36.

⁵¹⁶ Thompson, *Defeating Communist Insurgency*, 13.

attention of the state and generally does not serve an insurgency, as intended. Advanced cyber weapons remain the tool of well-resourced state actors, while improvised bombs may appear threatening but lack the ability to completely nullify the capability of a state's military. For now, the technology does not produce decisive effects that can tip the offense-defense balance.

This section must briefly address how geography may lead to impressions that an insurgency may win a decisive victory. Multiple IW theorists stress the importance of having a secure area to build capability for the insurgents. For his part, Galula offers a typology of insurgent territories that reflect how many insurgencies must boost their territorial control to overcome the state's influence.⁵¹⁷ In an "occupied area," the COIN forces are in control, and the insurgents may only operate underground. From there, the insurgents may create a contested area ("guerrilla area"), an area that they fully control and enjoy unimpeded mobility ("guerrilla base"), or even an actual "regular base" or military-style garrison. If, from the onset of an IW campaign, the insurgents can claim a series of guerrilla bases or areas, the case-specific geography may build the perception that the insurgency can decisively win an IW campaign. Rural areas or particularly rugged terrain often accompanies these sorts of situations. However, these cases are not necessarily the rule in IW, meaning that the variable of "decisive effects" does not sway the IW offense-defense balance in either direction.

7. Exposure—IW

The exposure variable heavily favors the offense in IW, as the technological and geographic factors of IW allow insurgents to attack while assuming virtually no exposure. In the context of the offense-defense balance, exposure refers to the degree that technological and geographic factors allow units to attack with minimal risk. In IW, because the insurgents are also part of the population, their attacking units are also part of the terrain (geography). In most cases, the state does not know who the insurgents are until they attack. Further, the offensive side of IW also subsumes the insurgent efforts to

⁵¹⁷ Galula, *Counterinsurgency Warfare*, 37–38.

influence the neutral population, and those actions may occur without any state knowledge. Thanks to modern technology, insurgents now have increased capabilities to launch attacks or exert their influence over a population without betraying their identity. Thus, the prevailing lack of exposure to the geographic and technological factors of IW heavily moves the offense-defense balance toward the offense.

A range of geographic factors potentially limit the exposure of insurgencies; however, the predominant factors are sanctuaries and local terrain. In the context of IW, a sanctuary in IW is an insurgent safe haven, allowing them the ability to conduct vital tasks including recovery, logistics, training, or leadership activities.⁵¹⁸ One of the textbook examples of a sanctuary is that enjoyed by the Taliban in Pakistan, greatly aiding their insurgent aims in Afghanistan since their fall from power in 2001.⁵¹⁹ The Pakistan sanctuary has granted the Taliban considerable freedom of maneuver in their Afghanistan campaign and also provided a valuable means of surviving the U.S.-led “surge” in 2009 that amounted to a large-scale counteroffensive. In terms of local terrain, insurgents often possess a profound knowledge of the local area that they can leverage to create conditions favorable for their operations. For example, during the battles of Fallujah in 2004, Al-Qaeda deftly exploited the urban terrain to seemingly match the otherwise overpowering capability of the U.S. military by creating ambushes and remaining largely concealed.⁵²⁰ While a plethora of other examples abound, the geography generally aids the insurgents’ offensive campaigns in IW.

Insurgents have long found clever ways to employ technology to attack conventional forces with low exposure. That trend continues today through innovations such as improvised explosive devices (IEDs), low-cost commercial systems like UAVs, and the connective benefits of cyberspace. IEDs are home-made explosives that insurgents conceal then trigger remotely through a range of methods, including a cell-phone call,

⁵¹⁸ U.S. Army, *FM 3-24 (2006)*, 1–16. Traditionally, sanctuaries were only physical; however, many increasingly view the many corners of cyberspace as virtual sanctuaries.

⁵¹⁹ Matt Waldman, “System Failure: The Underlying Causes of U.S. Policy-Making Errors in Afghanistan,” *International Affairs* 89, no. 4 (2013): 827–28, <https://doi.org/10.1111/1468-2346.12047>.

⁵²⁰ Hoffman, *Conflict in the 21st Century*.

timer, or target-activation. The Al-Qaeda insurgency in Iraq greatly impacted OIF efforts by allowing its operatives to remain hidden while attacking coalition soldiers.⁵²¹ UAVs, on the other hand, represent a low-cost commercial option that permits insurgencies the ability to produce physical or psychological effects from relatively great range. A series of UAV incidents in London confirmed these effects, as a UAV nearly struck an airliner at Heathrow in 2014 and illegal drone flights also plagued important landmarks in the city throughout 2015.⁵²² Finally, cyber-attacks represent a tempting option for insurgents who can leverage the physical ease of operating in cyberspace to terrorize a population or state operations. One of the first instances of this nature arose in Sri Lanka in 1997, as the self-styled Internet Black Tigers barraged Sri Lankan embassies with roughly 800 emails per day, which overloaded the embassy's email in the nascent days of cyber security.⁵²³

8. Insulation—IW

In IW, the defense suffers from an intrinsic lack of insulation, as the information advantage enjoyed by insurgents allow them to maneuver in the operational theater in a way that greatly threatens the state. Moreover, an important aspect of the insurgents' information advantage stems from the fact that state's security apparatus and infrastructure are on full display for the insurgents to target, deepening the insulation problem for the defense in IW.⁵²⁴ The offense-defense variable insulation represents the degree to which technological and geographic factors appear to shield the defense from attack, and the lack of insulation in IW tips the offense-defense balance toward the offense. Geography typically provides no insulation for the defense in IW, while only a great amount of resources occasionally produces technology that can insulate the defense. Even then, the insulating technology seldom shields the population from insurgent influence.

⁵²¹ Hoffman, "The 'Cult of the Insurgent'," 325.

⁵²² Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications*, Strategic Studies Institute Papers (Carlisle Barracks, PA: Army War College Press, 1998), https://ssi.armywarcollege.edu/ssi_pubs/.

⁵²³ Denning, "Terror's Web," 198–99.

⁵²⁴ Wilson, "The Mystic Diamond," 28.

One of the basic assumptions of IW is that it entails an internal struggle for control of the population, meaning that the insurgents and state presumptively share much of the same space as the target population. As a result, the state may encounter great difficulties in locating insurgents to provide an insulative shield over the population. Generally speaking, the insurgents are among the population. In a departure from the other examples, a case study in the U.S. illustrates this aspect of IW. In 2002, the Washington, DC snipers unleashed a 22-day terror campaign on the city's residents.⁵²⁵ Because the two snipers blended in and were a part of the populace, a wave of fear swept through the area as the complete lack of insulation left the city's residents and government landmarks exposed. Until the investigation tightened around the snipers, they could target with relative impunity. Though the DC snipers represent a small-scale case, the parallel with a mass insurgency is apparent—the geographic factors of IW place insurgents, the state, and the population in the same space, and the visibility of the state and its population yield no insulation.

Because the offense and defense generally reside in the same space in IW, only costly technologies may improve insulation. An example is the Iron Dome rocket defense system in Israel. A Congressional Research Service report describes the Iron Dome as, “a short-range antirocket system ... [and its] targeting system and radar are designed to fire its Tamir interceptors only at incoming projectiles that pose threats to the area being protected (generally, strategically important sites, including population centers).”⁵²⁶ Such a system purports to offer security to the population; however, it comes at a price. The Iron Dome system runs a hefty price, and Israel even accepts financial assistance from the U.S. to keep its system relevant to modern rocket threats.⁵²⁷ Further, it is an imperfect system, which can have a substantial impact on a population. For instance, a 2019 conflict between Israel and Palestinian militant groups in the Gaza Strip saw two days of intense rocket

⁵²⁵ Hoffman, “The ‘Cult of the Insurgent’.”

⁵²⁶ Jeremy M. Sharp, *U.S. Foreign Aid to Israel*, RL33222 (Washington, DC: Congressional Research Service, 2019), 12, <https://fas.org/sgp/crs/mideast/RL33222.pdf>.

⁵²⁷ The 2019 U.S. defense appropriations provided \$70 million for the Iron Dome: Sharp, *U.S. Foreign Aid to Israel*, summary page.

attacks, and while the Iron Dome achieved an 86% interception rate, rockets did get through killing three Israelis.⁵²⁸ The ever-evolving landscape of IW often proves difficult for insulating technology, showing how the defense typically suffers a lack of insulation.

9. Criticality—IW

Can an insurgency achieve strategic effects by striking assets critical to a population's welfare? Yes; Al-Qaeda achieved strategic effects in 1998 with the African embassy bombings and again in 2001 with the 9/11 attack on the World Trade Center.⁵²⁹ Can insurgencies deal a devastating blow to military operations by striking assets critical to security? Yes; the bombings of the Beirut Marine barracks in 1983 and Camp Chapman in 2009 demonstrate that they can.⁵³⁰

Clearly, the historical trend of IW suggests the offense can strike critical assets. In the context of the offense-defense balance, criticality implies that targetable objects appear necessary to a population's security or welfare, and the technological and geographic factors prompt these perceptions. In terms of target selection, insurgent often choose to strike critical assets that represent a critical ideal, as opposed to the practical use of their targets. Whereas airpower may target the C2 infrastructure of an opposing military, insurgencies may strike a target to spread a message, such as fear. Al Qaeda's terrorist-style attacks were a message meant to show the vulnerability of the U.S. The geographic factors of IW build the perception that the offense can strike critical items. The previous section on "insulation in IW" illustrates this point, and, to briefly summarize, the geography of an IW campaign tends to intermix the offense and defense within the same borders, placing critical assets of a population within striking distance of the offense. On the other hand, the technological factors of IW present an interesting question, as most

⁵²⁸ Sharp, *U.S. Foreign Aid to Israel*, 13.

⁵²⁹ Tod Hoffman, *Al Qaeda Declares War: The African Embassy Bombings and America's Search for Justice* (Lebanon, NH: University Press of New England, 2014), 1–66; Parker and Stern, "Blindsided? September 11 and the Origins of Strategic Surprise."

⁵³⁰ Benis M. Frank, *U.S. Marines in Lebanon 1982–1984* (Washington, DC: U.S. Marine Corps History and Museums Division, 1987), 1–3; The Camp Chapman bombing: Joby Warrick, *The Triple Agent* (New York: Vintage Books, 2012).

states are adept at safe-guarding their critical items through technical means. However, the above examples reveal how cunning innovation can, at times, lead to successful strikes on critical assets. Consequently, the geographical factors of IW coupled with concentrated innovation ultimately tips the balance toward the offense.

The technology that insurgents rely on to strike critical assets revolve around target selection and concealment. The first important step is finding an important asset that lacks adequate security, as the state fails to recognize its importance or fails to protect it. Prior to the 1998 embassy bombings, for instance, the U.S. did not always position its embassies to achieve a perimeter, and explosions could easily shred the windows and barricades.⁵³¹ Next, the insurgents rely on common-use technology to convince the state to ease its security measures. Car bombs, box cutters, and suicide vests all underscore this point, providing concealment to allow a clandestine infiltration. The defensive technology becomes more important in this case, as common-use items are plentiful to help conceal an attack, and security personnel must introduce advanced scanning technology or screening measures to spot an intrusion. Ultimately, innovations arise to help bypass the security measures in some locations, leading to the striking of critical items.

Of note, cyber-attacks typically do not threaten the critical infrastructure in IW; instead strategic cyber-attacks belong in a category outside of IW, such as GPC. In brief, the cyber defenses of critical infrastructure have improved to the point that strategic cyber-attacks require the resources of a state. The Stuxnet case-study illustrates this point, as its undertaking required massive resources, suggesting the actions of a state-level actor.⁵³² This thesis further explores Stuxnet in the following chapter and further underscores how a strategic cyber-attack implicates state involvement, as opposed to the hand of an insurgency.

⁵³¹ Eric Adams, "How the U.S. Prepares Its Embassies for Potential Attacks," *Wired*, 3 January 2020, <https://www.wired.com/story/how-us-prepares-embassies-potential-attacks/>.

⁵³² Valeriano, Jensen, and Maness, *Cyber Strategy*, 40; Jasper, *Strategic Cyber Deterrence*, 42; Brantly, *The Decision to Attack*, 142–43; Slayton, "What Is the Cyber Offense-Defense Balance?," 95.

10. Resilience—IW

Because IW is a population-centric struggle, assessing the resiliency tends to require a case-by-case analysis. Further, IW resilience intertwines with its lack of decisive effects, meaning that this offense-defense variable is effectively a “wash” for IW. In the context of the offense-defense balance, resilience signifies the ability to recover from an attack, and a high level of perceived resiliency tips the balance toward the defense. Modern technology exhibits a remarkable level of resilience. Contemporary logistics, construction capabilities, and the use of redundant systems collectively produce a remarkable capacity for states to recover from attacks. However, IW does not require states to recover in a rapid fashion as insurgents generally cannot conduct an overwhelming attack, as this chapter discusses in “decisive effects.” Resiliency in IW relates more to the long-term psychological ability of a population to endure a prolonged war, which is more a signaling and deterrence issue than it is an offense-defense balance issue.⁵³³

Furthermore, even a brief review of IW history illustrates that resilience is a case-by-case issue, as the offensive actions of insurgents have produced drastically population responses—even given the same population in a different time. After the 1983 Beirut Marine barracks bombing for instance, the U.S. response was to withdraw its peace-keeping forces from Lebanon just a few short months later as congressional support diminished.⁵³⁴ Just a few years later, the 1996 Khobar Tower bombings did not convince the U.S. to withdraw troops from Saudi Arabia. Instead, the U.S. forces relocated to the more secure Prince Sultan Air Base near Al-Kharj and continued operations despite daunting logistical difficulties.⁵³⁵ Such disparities in IW resilient efforts show that offense-defense resiliency is currently a wash, and may better align with a discussion of deterrence.

⁵³³ For a discussion of deterrence in IW, see: Robert Trager and Dessislava P. Zagorcheva, “Deterring Terrorism: It Can Be Done,” *International Security* 30, no. 3 (2005), <https://doi.org/10.1162/016228805775969564>.

⁵³⁴ Frank, *U.S. Marines in Lebanon*, 106–15.

⁵³⁵ Perry D. Jamieson, *Khobar Towers: Tragedy and Response* (Washington, DC: Air Force History and Museums Program, 2008), 182–83.

11. Conclusion—IW

A review of the offense-defense variables indicates that IW favors offensive actions, a point asserted in military circles and substantiated by the vast number of IW conflicts. However, the theory is not conclusive across all variables, suggesting that those variables that do favor the offense in IW are overwhelming. IW is also an interesting case study, as its nature requires an offense-defense analysis to identify its offensive (insurgent) and defensive (state) roles. In sum, IW (a) inherently grants insurgencies the information advantage, while technology encourages manipulation of public information; (b) lacks decisive effects for both the offense and defense; (c) allows the insurgency to avoid nearly all exposure; (d) grants the state practically no insulation; (e) permits the striking of adversary's critical assets; and (f) fails to show a consistent mark of resiliency. The offense-defense variables of decisive effects and resiliency ultimately prove a “wash”—inconclusively tipping the offense-defense balance in either direction. However, the overwhelming advantage granted the offense its information advantage, exposure avoidance, and the defensive lack of insulation suggests that the IW offense-defense balance favors the offense. The implication is that international actors may view insurgencies as a highly attractive strategy. In terms of GPC, that may mean an uptick in UW campaigns.

E. CONCLUDING THOUGHTS ON AIR WARFARE AND IW

The air warfare and IW case studies demonstrate the explanatory power of the offense-defense theory outlined in this thesis. Air warfare doctrine and its theorists consistently argue that airpower is offensive, and the analysis in this chapter supports this claim. For IW, both the international trends and doctrine warn that IW conflicts are on the rise because of technology and other modern conditions, and the offense-defense analysis again reinforces the prevailing views.

While the theory produces an analysis of air warfare that categorically found air warfare offensive, IW does not render a compelling case for two of the offense-defense variables: decisive effects and resiliency. Nevertheless, the central point is that an offense-defense analysis is a sum of all the variables, and offensive IW convincingly tips the

balance in the other three variables: information advantage, exposure, and insulation. Another way that airpower and IW differ is that the offense-defense analysis of IW requires the identification of the offensive and defensive roles. This requirement arose from the net effect that insurgencies and counterinsurgencies have on the status quo. In general, insurgencies incite a campaign for revolutionary change while the counterinsurgencies attempt to quell the campaign.

The final question of this chapter is whether the analysis of air warfare and IW reveals any variables that warrant inclusion in the offense-defense theory proposed in this thesis. Only one variable emerges as a likely candidate: precision. Precision plays a keen role in air warfare, allowing the offense to strike accurately with confidence that the ordnance will hit the correct target while minimizing collateral damage. In this regard, precision technology may encourage offensive inclinations. While valid, precision ultimately relies heavily on accurate information and falls neatly under two other variables: decisive effects and criticality. Without accurate intelligence, precision strikes are apt to hit the wrong target, rendering precision as a function of information. When intelligence is accurate, the decisive effect that airpower brings to bear is precision, as airpower can accurately strike the targets that it sets out to strike. The notion of criticality further underscores this point, as precision allows airpower to target the vital assets of a population. To view the issue from another perspective, consider precision in cyber conflict--the topic of the coming chapter. The task of constraining effects to a precise target is profoundly onerous for OCO, requiring accurate intelligence and immense analytical resources to avoid collateral damage and conceal the hand of the attacker.⁵³⁶ Despite these difficulties, OCO still demonstrates an ability to produce decisive effects and target critical items, and precision is a consideration of those variables.⁵³⁷ In effect, the offense-defense variables in this thesis already cover the essential aspects of the offense-defense balance

⁵³⁶ Conti and Raymond, *On Cyber*, 196–206.

⁵³⁷ As early as 1988, the Morris Worm demonstrated how cyber effects can quickly infect unintended targets, as the Worm effectively shut down 10% of the systems on the Internet at the time: U.S. Government Accountability Office, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, DC: U.S. Government Accountability Office, 2006), 20–21, <https://www.gao.gov/assets/260/250483.pdf>.

without adding variables, including precision. The theory is ripe for analyzing other forms of conflict.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE CYBER OFFENSE-DEFENSE BALANCE

Finally, mutual fear of big weapons may produce, instead of peace, a spate of smaller wars

—Kenneth Waltz, *Man, the State, and War*⁵³⁸

Through a critical review of the offense-defense literature, the study herein develops a framework to assess the offense-defense balance and applies that framework to air warfare and IW. The resulting examinations suggest that the framework does provide utility while gleaning insights into modern forms of conflict. Consequently, this chapter moves to fulfill the initial line of inquiry underpinning this article—assessing the cyber offense-defense balance. To properly frame the discussion, this assessment proceeds in the same manner as the air warfare and IW examinations, beginning with the key issues and terms.

An appropriate starting point for cyber conflict is the “stability-instability paradox,” which is a noted theory amongst International Relations scholars. Its premise is that the ominous nature of modern warfare—especially in the nuclear age—largely deters war amongst the great powers but unleashes a flood of low-intensity conflict in its place.⁵³⁹ This concept makes sense in the anarchic international system, where competition and coercion are political fixtures that come hand-in-hand with conflict. Moreover, the Correlates of War dataset suggests that the theory has merit, as the frequency of conflict rose by over forty percent in the latter half of the twentieth century from the first half.⁵⁴⁰ The frequent occurrence of conflict in the international system is a telltale sign that the system is unstable, stemming from unchecked escalations. IR theory warns that as

⁵³⁸ Waltz, *Man, the State, and War*, 236.

⁵³⁹ S. Paul Kapur, “India and Pakistan’s Unstable Peace: Why Nuclear South Asia Is Not Like Cold War Europe,” *International Security* 30, no. 2 (2005), <https://doi.org/10.1162/016228805775124570>.

⁵⁴⁰ In summing all inter-state, extra-state, and intra-state wars, 1900–1949 witnessed 135 wars while 1950–1999 bore 193: Sarkees and Wayman, “Resort to War: 1816–2007.”; This statistic is telling as it correlates with the Soviet’s first atomic bomb test in 1949 at the Semipalatinsk test site, initiating the nuclear bi-polarity of the Cold War: Ed Ou, “Under a Nuclear Cloud,” *The Virginia Quarterly Review* 87, no. 4 (2011): 52.

escalations unfold under conditions that encourage aggression, a crisis can easily amplify into conflict, exemplifying the international instability.

In cyber conflict, the idea is more or less the same as it is in traditional IR theory. The cyber interactions of state or non-state actors can appear threatening, sparking escalations and instability in the ecosystem. With the advent of the digital age, cyberspace simply provides a convenient venue for the stability-instability paradox to unfold, as online skirmishes, or “incidents,” have increasingly become the norm.⁵⁴¹ One of the more troubling forms that these incidents take is that of unwelcome intrusions into the strategically important government networks or critical infrastructure, regardless of the intrusion’s success.⁵⁴² At initial glance, such intrusions may appear a relatively benign action in international relations; however, the frequency and severity of such intrusions have given rise to increased cyber posturing and provokes the instability.⁵⁴³ Amidst these growing concerns, scholars and analysts, alike, often ask if the cyber offense-defense balance plays a role. Perhaps the relative ease of cyber-attacks—or at least the perception therein—is to blame for the lack of international stability? As the stakeholders formulate a coherent cyber strategy, this question continues to haunt the process.

A. WHAT IS CYBER CONFLICT?

To ensure relevance to the discussion of cyberspace and international stability, it is important to proceed on a fitting definition of cyber conflict. Such a definition must acknowledge how cyberspace interconnects with information warfare and C2. This thesis defines “*cyber conflict*” as *the struggle in and through cyberspace for control of*

⁵⁴¹ For a list of the growing “incidents” in cyberspace, see Appendix 3 of: Valeriano, Jensen, and Maness, *Cyber Strategy*, 230–46; For an authoritative definition of an “incident,” see: National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800–53 Revision 4 (Gaithersburg, MD: National Institute of Standards and Technology, 2013), B-9, <https://csrc.nist.gov/publications/sp>.

⁵⁴² This concept underpins much of Buchanan’s argument in his book: Buchanan, *Cybersecurity Dilemma*, 3; To garner a sense of the volume of intrusions, see: Kaplan, *Dark Territory*, 214; Eng and Jones, “OPM Chief Says Government Agency Thwarts 10 Million Hack Attempts a Month.”

⁵⁴³ John Arquilla, “Cyberwar Is Already Upon Us: But Can It Be Controlled?,” *Foreign Policy*, 27 February 2012, <http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/>.

*information and the integrity of public and governmental control systems.*⁵⁴⁴ As in the other case studies of this thesis, cyber conflict is about control—control of information and control of, well, the control systems.

First, the cybersecurity experts Gregory Conti and David Raymond help convey the importance of information to cyber conflict, while the doctrinal “layers of cyberspace” illustrates the operational environment linking information to cyberspace.⁵⁴⁵ Conti and Raymond write, “[w]e use *cyber* to mean attacking, defending, or collecting information from other computers...We consider *cyberspace* as the sum of the computing systems, networks, and data which permeate our global environment.”⁵⁴⁶ Cyber conflict (which Conti and Raymond refer to simply as “cyber”) has taken center stage in information warfare because cyberspace has become the modern means of storing and trading information. Entrusting cyberspace with our data has proven a double-edged sword. Every bit of data in cyberspace is vulnerable to theft or exploitation, thereby driving the need to include information operations in the discussion of cyber conflict.⁵⁴⁷ In terms of the cyberspace environment, information emanates from three interrelated layers: the physical network, logical network, and cyber-persona.⁵⁴⁸ The physical layer includes the infrastructure and equipment, the logical layer pertains to the code that drives the networks and its components, and the cyber-personas encompasses the user accounts (as an entity or a single individual) and their relationships to each other and to the various networks.⁵⁴⁹ Controlling the information in and through cyberspace accounts for a significant portion of the concepts underpinning cyber conflict.

⁵⁴⁴ For a doctrinal definition of cyberspace and cyberspace security, see: U.S. Department of Defense, *JP 3-12*, GL-4.

⁵⁴⁵ Conti and Raymond, *On Cyber*; U.S. Department of Defense, *JP 3-12*, I-2 - I-4.

⁵⁴⁶ Conti and Raymond, *On Cyber*, 3–4.

⁵⁴⁷ To understand the interconnected nature of information and cyberspace in the DOD, see: U.S. Department of Defense, *JP 3-12*, vii-xii; For an example information at risk in cyberspace, see: Koppel, *Lights Out*, 7.

⁵⁴⁸ U.S. Department of Defense, *JP 3-12*, I-3.

⁵⁴⁹ U.S. Department of Defense, I-2 - I-4.

Cyberspace also impacts the security of many nations because of its relationship with vital C2 systems, driving the need to include the integrity of C2 systems in the cyber conflict definition. Any effort to hinder the DOD's access to cyberspace is akin to an attempt at obstructing the DOD from its vital capabilities, and military doctrine and academic literature alike both stress this point.⁵⁵⁰ Further, the definition of cyber conflict must broadly consider C2 beyond its military context. It should also include the supervisory control and data acquisition (SCADA) systems that maintain our vital infrastructure and public works. The public and military both rely on these systems to maintain the security and welfare of the population; therefore, cyber conflict must include the maintenance and operations to sustain their integrity.⁵⁵¹ Broadening C2 to include civilian control systems underscores cyberspace's relevance to international stability.

B. THE KEY ATTRIBUTES OF CYBER CONFLICT

Cyberspace is new and radically different from the physical warfighting domains. The literature offers characteristics of cyber conflict that make it unique:⁵⁵²

- Its environment is man-made, and its environment changes rapidly, as a result
- The low cost of entry allows for a gamut of actors
- The other warfighting domains—and many civilian entities—have come to rely on it
- It lacks any norms leaving a significant “gray” zone on state interactions

⁵⁵⁰ U.S. Department of Defense, *JP 3-12*, xi; Brantly, *The Decision to Attack*, 1.

⁵⁵¹ Clarke and Knake, *Cyber War*, 97–101; Koppel, *Lights Out*, 8–10.

⁵⁵² On the low cost of entry: U.S. Department of Defense, *JP 3-12*, I-2; On the fluid nature of the environment, see: Singer and Friedman, *Cybersecurity and Cyberwar*, 154; On the gray area of cyber conflict: Singer and Friedman, 122–26; On the lack of appropriate norms: Martha Finnemore and Duncan B Hollis, “Constructing Norms for Global Cybersecurity,” *American Journal of International Law* 110, no. 3 (2016): 425–27; Impacts civilian and military domains: Brantly, *The Decision to Attack*, 1; Also, of note, cyber's man-made environment is chiefly owned and operated by the private sector: Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 16.

Each attribute, taken separately, does not represent completely novel problems. Peter Singer and Allan Friedman point out how similar attributes of the air and sea domains flummoxed states when they first entered the warfighting arena.⁵⁵³ The perplexing part of these attributes is that they collectively result in more troubling problems. For instance, the varying nature of the cyberspace environment coupled with its large quantity of actors has made attributing cyber-attacks to the responsible party a daunting task—even impossible at times.⁵⁵⁴ The problem of attribution then causes further problems, including a strain on the interactions of states, which is already difficult enough given the lack of norms in cyberspace. The issues raised by these attributes have required dynamic thinking and brought significant changes to the U.S. DOD.⁵⁵⁵

⁵⁵³ Singer and Friedman, *Cybersecurity and Cyberwar*.

⁵⁵⁴ Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, no. 1–2 (2015), <https://doi.org/10.1080/01402390.2014.977382>.

⁵⁵⁵ U.S. Cyber Command, “U.S. Cyber Command History,” 2019, accessed 21 August 2019, <https://www.cybercom.mil/About/History/>.

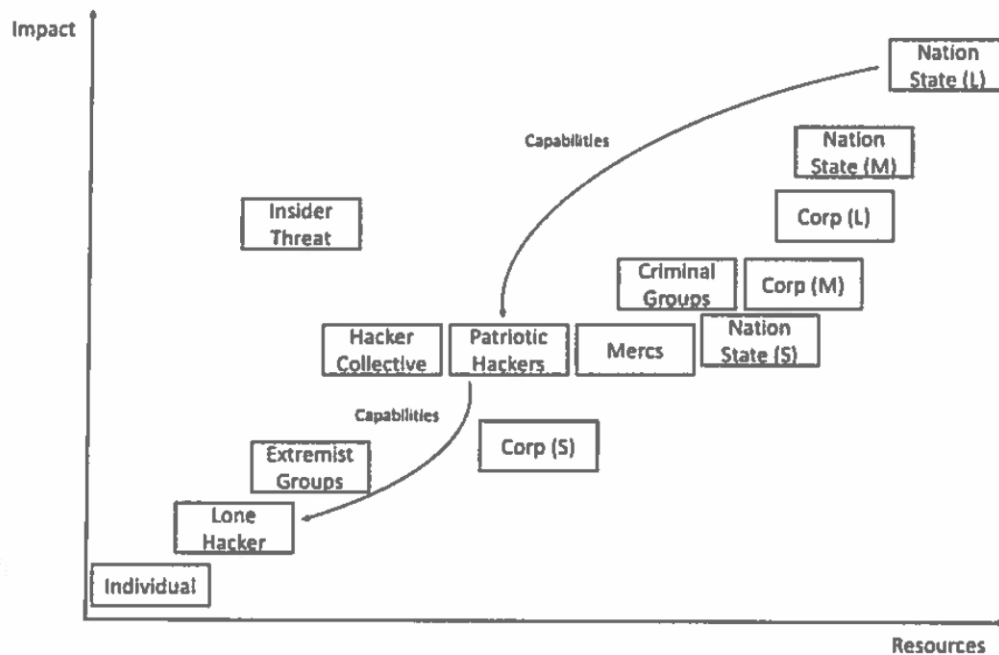


Figure 3. Conti and Raymond's Chart Depicting the Primary Actors in Cyber Conflict⁵⁵⁶

One area in which the literature on cyber conflict has had relative success is in categorizing the various actors and their strategies. This success stems from the trend that cyber actors and their strategies fall rather neatly into the time-tested categories created by IR literature. In Figure 3, Conti and Raymond portray the relationship between the various actors in cyberspace, their resources, and their impact on the cyber realm.⁵⁵⁷ For instance, state actors continue to hold the most sway in cyberspace as they hold the greatest resources and have access to the foremost technologies and people.⁵⁵⁸ Figure 3 underscores how cyberspace has not upset the general hierarchy of international actors nor the relationship of resources and power, despite its asymmetric nature. Furthermore, states generally have adopted strategies that greatly resemble traditional strategies to cope with cyber conflict:

⁵⁵⁶ Source: Conti and Raymond, *On Cyber*, 16.

⁵⁵⁷ Conti and Raymond, 16.

⁵⁵⁸ Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2018), 12.

cyber coercion, cyber deterrence, and covert signaling to name a few.⁵⁵⁹ The prominent IR theorist Joseph Nye aptly describes the interplay of strategy and cyberspace: “cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. Cyberpower can be used to produced preferred outcomes within cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace.”⁵⁶⁰ Recall that cyber conflict ultimately centers on maintaining control in or through cyberspace. To expand or entrench their control, the actors of cyberspace wield their respective cyber power. It is this interaction that produces the clashes of cyber conflict and necessitates cyber strategy.

While the traditional hierarchy of actors generally remains intact, Nye reminds us that cyberspace has created a “diffusion of power,” drastically leveling the playing field and allowing asymmetric approaches in conflict.⁵⁶¹ Less prominent actors have the ability to quickly assume power, which also creates an evolving list of actors. One of the most important aspects of cyberspace, itself, is how it is chiefly owned and operated by the private sector.⁵⁶² As an example, corporations like social media platforms and Internet Service Providers (ISPs) have emerged over the past few decades as immensely powerful actors who play a vital role in cyber conflict.⁵⁶³ While both are relatively new to the broader IR stage, social media platforms hold great sway over the modern flow of information, and ISPs are critical to the overall health of cyberspace. This diffusion of power originates from a number of underlying factors in cyber conflict. Some theorists emphasize that the new technology is the prominent factor driving these changes (e.g. “Radical Leveling Technologies”), while others emphasize how new forms of power (e.g.,

⁵⁵⁹ For traditional uses of strategies, see: Nye Jr, *The Future of Power*, 18–22; For traditional uses of strategy in the cyber domain, see: Valeriano, Jensen, and Maness, *Cyber Strategy*; Jasper, *Strategic Cyber Deterrence*.

⁵⁶⁰ Nye Jr, *The Future of Power*, 123.

⁵⁶¹ Nye Jr, 113.

⁵⁶² Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 16.

⁵⁶³ To understand the reach of ISPs, see: Clarke and Knake, *Cyber War*, 74–82; and, Singer and Friedman, *Cybersecurity and Cyberwar*, 2.

the “Information Revolution”) act as the guiding force.⁵⁶⁴ The bottom line is that the diffusion of power forces the powerful actors to readily acknowledge others that may have lacked relevance in the past.

In cyber conflict, proxies have once again found prominence, as cyberspace and GPC have provided a venue for their employ not seen since the end of the Cold War. Proxies are a class of actors whose interests overlap with the more powerful actors to a sufficient degree that powerful actors will employ them directly or indirectly as an instrument of power. While proxies are certainly far from a new phenomenon, the attributes of cyberspace play perfectly into the use of proxies, leading to a growth in their utilization. The employment of cyber proxies is especially acute in countries where corporate cyber work is not well-compensated.⁵⁶⁵ Cyber proxies offer particular utility for more powerful actors because the proxies can conduct operations that benefit their employer, concealing the hand of the more powerful actors in certain situations.⁵⁶⁶ Consequently, the cyber proxy phenomenon has deepened the attribution problem in cyberspace. The net effect is often a “gray” battle for control of the cyber domain that produces a disquieting number of incidents, leaving the world unsure of its trust in cyberspace.

1. Technology in Cyber Conflict

Cyberspace is the central technology of cyber conflict. Though there is no clear intent to do so, the overarching trend in cyberspace is to introduce mechanisms that expand its influence over the management of information and the control of modern life. First, though cyberspace increasingly connects humans with machines, it remains chiefly as a vehicle for the storage and transmission of information.⁵⁶⁷ The evolving technology primarily serves the purpose of increasing data capacity, analyzing larger datasets, boosting

⁵⁶⁴ “Radical Leveling Technologies”: Jennifer J. Snow, “Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies” (Graduate Thesis, Naval Postgraduate School, 2015); “Information Revolution”: Nye Jr, *The Future of Power*, 114–18.

⁵⁶⁵ Maurer, *Cyber Mercenaries*, 81–106.

⁵⁶⁶ Maurer, 6–22.

⁵⁶⁷ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 9–28.

the speed of transmission, and securing the data. A key part of the movement and access to information revolves around the ideas of trust and authentication, and technology moves to improve those items.⁵⁶⁸ Though cybersecurity has made strides in authentication, anonymity and attribution problems continue to plague cyberspace.⁵⁶⁹

As mentioned, the other dominant use of cyberspace has become to control the machines and systems that run daily life, and this control has increasingly become automated. In his description of cyberspace trends, Tim Maurer describes this relationship: “[f]irst, more and more machines—including cars and control systems in industry—are changing from closed manual and mechanical systems to interoperable digital systems. Second, more and more of these digital devices are connected to the Internet.”⁵⁷⁰ Cyber conflict leverages the rapid assessment and reliability of artificial intelligence to produce quick and accurate actions to enhance control of the systems linked to cyberspace.⁵⁷¹ Simply put, automation grows at a telling rate, slowly assuming many of the roles previously done by humans.⁵⁷²

2. Geography in Cyberspace

One of the trends in cyber literature is the notion that cyberspace transcends all geographic concerns, implying that borders and distances do not hinder cyber operations. The message is that all actors are in constant striking distance of each other, and the playing field is completely level for all geographic locations. This section presents the case that

⁵⁶⁸ “The notion of consent and authorization is a good baseline conceptualizing hacking generally”: Maurer, *Cyber Mercenaries*, 7.

⁵⁶⁹ U.S. Department of Defense, *JP 3-12*, I-12.

⁵⁷⁰ Maurer, *Cyber Mercenaries*, 7.

⁵⁷¹ Zachary Fryer-Biggs, “Coming Soon to a Battlefield: Robots That Can Kill,” *The Atlantic*, 3 September 2019, <https://www.theatlantic.com/technology/archive/2019/09/killer-robots-and-new-era-machine-driven-warfare/597130/>.

⁵⁷² One analysis estimates that 47% of the total U.S. employment is likely to be automated over the next decade: Carl Benedikt Frey and Michael A. Osborne, “The Future of Employment: How Susceptible Are Jobs to Computerisation?,” *Technological Forecasting & Social Change* 114 (2017): 268, <https://doi.org/10.1016/j.techfore.2016.08.019>.

geography does matter in cyber conflict, and the overarching trend is to further spread the influence of cyberspace to the far corners of the globe.

Geography in cyber conflict is salient in three primary ways: the physical hardware, the distance that data must travel, and the government's ability to impact access. Though it is not always apparent, the physical hardware that powers the Internet resides somewhere, physically. For instance, undersea communication cables connect ISPs throughout the world to assist in reaching the far corners of the globe.⁵⁷³ Also, spyware meant to collect and relay data must send that data to a server or ISP somewhere, meaning that eventually the information becomes correlated with a location.⁵⁷⁴ Next, when data travels, it does not do so instantaneously, though it may appear so to humans. While data does move at a high rate of speed, it does reach the closest server first. This phenomenon contributes to some of the concerns for investors and high-frequency trading, which leverages short cable connections and algorithms to more rapidly sense trends and then execute financial trades quicker than the competitors located further from Wall Street's servers.⁵⁷⁵ Finally, the actors of cyber conflict may also experience political limitations from their host country. In 2019, Iran reacted to a surge in violent political demonstrations by enacting a week-long internet black-out on its population, and the citizens of China famously operate in cyberspace under fairly extensive censoring.⁵⁷⁶ The DOD acknowledges these geographic challenges in its doctrine, noting how its cyberspace operations often rely on physically disparate infrastructure and information technology products increasingly include foreign

⁵⁷³ Michael Sechrist, *Cyberspace in Deep Water: Protecting Undersea Communications Cables By Creating an International Public-Private Partnership*, (Cambridge, MA: Harvard University Belfer Center for Science and International Affairs, 2010), <https://www.belfercenter.org/publication/cyberspace-deep-water-protecting-undersea-communications-cables-creating-international>.

⁵⁷⁴ Singer and Friedman, *Cybersecurity and Cyberwar*, 59.

⁵⁷⁵ High frequency traders and the issue of speed reached mainstream consciousness through Michael Lewis' book on the topic: Michael Lewis, *Flash Boys: A Wall Street Revolt* (New York: W.W. Norton, 2014); For a more technical view into high frequency trading: Peter Gomber and Martin Haferkorn, "High-Frequency-Trading," *Business & Information Systems Engineering* 5, no. 2 (2013), <https://doi.org/10.1007/s12599-013-0255-7>.

Economy, "The Great Firewall of China."⁵⁷⁶ Farnaz Fassihi, "Iran Blocks Nearly All Internet Access," *New York Times*, 17 November 2019, <https://www.nytimes.com/2019/11/17/world/middleeast/iran-protest-rouhani.html>.

supply chains.⁵⁷⁷ Both of these examples show how geography creates risk for those in cyber conflict.

C. OFFENSE IN CYBER CONFLICT

This thesis defines offense in cyber conflict as those cyber actions intended to gain unauthorized access or produce denial effects of external cyber systems, meaning those systems not controlled by the actor. The reader may note the length of this definition, and it bears reason to provide justification. First, this definition aligns with the overarching doctrinal definition of OCO (emphasis added): “OCO are [cyberspace operations] missions *intended to project* power in and through foreign cyberspace through actions taken in support of CCDR or national objectives.”⁵⁷⁸ The word “intended” subsumes both successful and unsuccessful attempts, while the word “project,” though vague, implies movement onto external systems. Furthermore, doctrine further supports this definition as “gaining access” and “producing denial effects” relate to the two key actions of doctrinal OCO: exploitation and attack, respectively.⁵⁷⁹ Second, this definition emphasizes the importance of external cyber actions and effects. The importance of external cyber actions draws into focus through Belk and Noyes’ proposed ontology on OCO: “[w]e define external cyber actions as those cyber actions with effects on systems not owned or operated by the actor.”⁵⁸⁰ Their ontology also brings up the importance of effects, and, as the previous chapters highlight, modern firepower amounts to the projection of effects, and denial effects are an important part of cyber-attack. Third, and perhaps most important, the proposed definition of this section fits the context of offense-defense theory. Because offense-defense theory relates to war and strategy, it also relates to power. Maurer emphasizes the important tie between power and gaining access to external cyber systems: “[t]he necessary condition for cyber power as used in this book is *unauthorized access*. The

⁵⁷⁷ U.S. Department of Defense, *JP 3-12*, I-12 - I-13.

⁵⁷⁸ U.S. Department of Defense, II-5.

⁵⁷⁹ U.S. Department of Defense, II-3 - II-7.

⁵⁸⁰ Belk and Noyes, *On the Use of Offensive Cyber Capabilities*, 18.

notion of consent and authorization is a good baseline for conceptualizing hacking generally.”⁵⁸¹ Further, attempted intrusions and exploitation should align with the offense in cyber conflict. Buchanan underscores the escalatory effect that cyber intrusions can have on international relations.⁵⁸² He argues that though intrusions may be viewed as a defensive maneuver by the intruder, the actor controlling the network with the unauthorized entry does not view it that way. Each intrusion does not come with a defensive explanation that satisfies the target; the target views the intrusion as threatening and, therefore, offensive.⁵⁸³ As demonstrated by the discussion, considerable nuance surrounds the definition of cyber offense; thankfully, numerous sources have contributed to the efforts of clarifying the terms.

Admittedly, the proposed definition of offense in cyber conflict does not fit many of the descriptions that others propose, specifically the doctrinal view on what may constitute defense. In the context of the offense-defense balance, there is an important reason. U.S. doctrine proposes a concept that it terms “defensive cyberspace operations-response actions” (DCO-RA).⁵⁸⁴ DCO-RA includes cyber-attack and exploitation, which makes sense in a counter-offensive scenario. However, the doctrine implies that DCO-RA may include these types of operations when imminent danger threatens the U.S. or its allies. Taken at face value, an attack when under imminent danger from an outside source does not sound like defense, at all; rather, it bears all the trappings of a pre-emptive attack.⁵⁸⁵ In the context of the offense-defense balance, a pre-emptive attack is almost the epitome of a balance that favors the offense. It is an implicit admission that a defensive strategy is simply inadequate and employing an offensive strategy is necessary for success. Perhaps

⁵⁸¹ Maurer, *Cyber Mercenaries*, 7.

⁵⁸² Buchanan, *Cybersecurity Dilemma*, 3.

⁵⁸³ Buchanan, 96–100.

⁵⁸⁴ U.S. Department of Defense, *JP 3-12*, II-4.

⁵⁸⁵ Chapter two of this thesis presents the idea of pre-emption and reminding the reader here may help: the political theorist Michael Walzer argues that pre-emption becomes when a state is in imminent danger and waiting to act can only amplify its risk: Walzer, *Just and Unjust Wars*, 77–82.

defining DCO-RA to include pre-emptive actions in doctrine helps frame the successful thinking of the joint force; however, it does not fit in offense-defense theory.

Finally, OCO unfold through three important concepts: the general objectives, offensive process, and the importance of deception to the cyber offense. First, Belk and Noyes succinctly outline the general objectives of OCO: “[o]ffensive objectives are those seeking to coerce rival action, impose harm, or degrade rival capabilities.”⁵⁸⁶ OCO seek to alter the status quo in some way or create favorable conditions for the offense. As Belk and Noyes also emphasize, it may include something as seemingly benign as scanning an adversary’s ports for vulnerabilities.⁵⁸⁷ In terms of the offensive process, a Lockheed Martin white paper presents a seven-step “cyber kill chain,” meant to help the defense conceptualize how an attack may progress.⁵⁸⁸ While meant to help a cyber defender understand the vulnerable points in the attack, it also reveals how the offense obtains the intended objectives. Finally, deception is a vital part of OCO given the current nature of cyberspace and operating environment. As Gartzke and Lindsay argue, “attackers who fail to be deceptive will find that the vulnerabilities on which they depend will readily be patched and access vectors will be closed.”⁵⁸⁹

D. DEFENSE IN CYBER CONFLICT

Defense in cyber conflict are those actions taken to secure the internal or supported systems of an actor. While this may include counter-offensive or countermeasures, it excludes pre-emptive attack or exploitation. Belk and Noyes define defense through both internal cyber actions and defensive objectives: internal cyber actions are those, “with effects only on systems operated by the actor,” and defensive objectives are, “those seeking

⁵⁸⁶ Belk and Noyes, *On the Use of Offensive Cyber Capabilities*, 21.

⁵⁸⁷ Belk and Noyes, 19.

⁵⁸⁸ The seven steps of the kill chain are: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives: Hutchins, Cloppert, and Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, 4–5.

⁵⁸⁹ Gartzke and Lindsay, “Weaving Tangled Webs,” 326.

to secure one's own systems, and preserve freedom of operation.”⁵⁹⁰ Countermeasures are also vitally important to cyber defense as they provide response options for the defense to eliminate and mitigate offensive effects.⁵⁹¹ They also become a vital element of deterrence options, owing to the high cost that some countermeasures can impose on an attacker.⁵⁹²

Based on the previous section, it should not come as a surprise that this definition departs from doctrine and emerging views across the strategic landscape. For instance, the Cyberspace Solarium Commission (CSC) recommends that the DOD continue its actions to “defend forward” from U.S. and partner networks, while the supporting agencies must help to remove barriers to this strategy.⁵⁹³ Defending forward, though congruent with the current cyber environment, still amounts to an admission that defense requires external cyber actions to secure the networks that one already controls. Hence, for the offense-defense theory, defending forward aligns with the offense.

In terms of conceptualizing defense in cyber conflict, DCO falls neatly within the traditional defense categories. First, the literature classifies DCO as either active—those measures that require proactive steps—or passive—those measures that do not require initiative.⁵⁹⁴ To illustrate the difference: an example of passive cyber defense is a firewall (set in place and allowed to defend on its own), while an example of active cyber defense is attack analysis, much like the widely-used “kill chain” method.⁵⁹⁵ Also like OCO, DCO relies heavily on deception—a vital concept in conventional defense.⁵⁹⁶ DCO has grown

⁵⁹⁰ Belk and Noyes, *On the Use of Offensive Cyber Capabilities*, 19–21.

⁵⁹¹ U.S. Department of Defense, *JP 3-12*, II-4.

⁵⁹² Much like the countermeasures recommended by the “layered cyber deterrence” strategy from: Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 7.

⁵⁹³ Cyberspace Solarium Commission, 116.

⁵⁹⁴ For active and passive defense, see: Jasper, *Strategic Cyber Deterrence*, 165–90; Dorothy E. Denning and Bradley J. Strawser, “Active Cyber Defense: Applying Air Defense to the Cyber Domain,” in *Cyber Analogies*, ed. John Arquilla and Emily O. Goldman (Monterey, CA: Naval Postgraduate School, 2014), <https://calhoun.nps.edu/handle/10945/40037>.

⁵⁹⁵ Hutchins, Cloppert, and Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*.

⁵⁹⁶ Gartzke and Lindsay, “Weaving Tangled Webs.”

to rely on a few successful tactics that rely on deception, including honeypots and sinkholes.⁵⁹⁷ Hence, traditional warfare terms have provided a ready-made framework for the cyber security establishment.

E. DO THE EXPERTS PERCEIVE CYBER CONFLICT AS OFFENSIVE OR DEFENSIVE?

Over the past decade, many prominent voices have raised concerns that cyber conflict has suffered from an over-emphasis on offense, which offense-defense theory predicts will lead to aggressive behavior and likely escalations.⁵⁹⁸ To briefly gain a sense of how offense dominates the domain, consider how cyber defense often has to utilize offensive tactics to raise its effectiveness.⁵⁹⁹ A key part of cyber defense often involves performing intrusions into an adversary's network to collect intelligence and maintain an awareness of impending threats.⁶⁰⁰ Simply put, the prevalence of cyber intrusions is indicative of the belief that cyberspace only rewards those who undertake offensive actions. Valeriano, Jensen, and Maness continue to maintain the “dyadic cyber incident and dispute dataset” (DCID), and the dataset has done nothing but grow since the publishing of their book in 2018.⁶⁰¹ The actors of cyber conflict do not appear deterred by the cost of cyber intrusions, and the incidents only continue. The prevalence of cyber intrusions for both offense and defense makes distinguishing the two difficult—another factor that offense-defense theory warns as being dangerous.

While offense-defense theory does suggest a high likelihood of aggression in cyberspace, the cyber offense-defense balance remains an open debate. Peter Singer and Allan Friedman contend that cyber-attacks are highly complex—requiring great expertise

⁵⁹⁷ Gartzke and Lindsay, “Weaving Tangled Webs,” 326; Jasper, *Strategic Cyber Deterrence*, 169–70.

⁵⁹⁸ For the over-emphasis of offense, see: Singer and Friedman, *Cybersecurity and Cyberwar*, 153–65; Clarke and Knake, *Cyber War*, 144–59; Kaplan, *Dark Territory*, 280–85; Koppel, *Lights Out*; Bumiller and Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S..”

⁵⁹⁹ Buchanan, *Cybersecurity Dilemma*, 31–74.

⁶⁰⁰ To understand how cyber defense is difficult to distinguish from cyber offense, see: Buchanan, 51–74.

⁶⁰¹ Valeriano, Jensen, and Maness, *Cyber Strategy*, 247.

to prepare and the patience to navigate the “cyber kill chain mentioned in the previous section—and often have uncertain outcomes.⁶⁰² Another strategist that has written extensively on cyber issues—Thomas Rid—argues that cyber offense is relatively weak. Rid points out that cyber weapons often suffer from a short half-life which rapidly diminishes their utility once created, while the market for network defense has taken on a burst of energy in the past few years.⁶⁰³ Both of these elements suggest that defense may be gaining an equal footing with offense. However, the sheer volume of incidents is certainly not conclusive proof that offense is dominant. For instance, many of the incidents may represent such a benign threat that the defense simply does not mind absorbing the plethora of attacks. In short, the debate remains undecided, and this thesis moves to conduct an analysis of the cyber offense-defense balance.

F. INFORMATION ADVANTAGE—CYBER CONFLICT

Cyberspace, the OE of cyber conflict, has become the principal source of information for the world. It connects everyone, and militaries have come to rely on these benefits to share information and augment their foreign collection capabilities.⁶⁰⁴ The result is that offensive actions in cyber conflict create the perception that actors can seize the information advantage. The information advantage is the operational edge gained by controlling the flow of information, and technology that builds the perception that the information advantage is within reach creates offensive inclinations. Thus, the close tie between information and cyberspace tips offense-defense balance toward the offense. The literature, U.S. doctrine, and recent examples all illustrate this point.

First, the literature emphasizes how cyber conflict has further strengthened the high demand for information during the IT-RMA. Chapter III of this thesis dives into the current RMA, which leverages C4I technology and practices along with advanced targeting systems to strike the adversary’s critical capabilities. In their analysis of how cyber conflict

⁶⁰² Singer and Friedman, *Cybersecurity and Cyberwar*, 154–55.

⁶⁰³ Rid, *Cyber War Will Not Take Place*, 168–69.

⁶⁰⁴ U.S. Department of Defense, *JP 3-12*, I-1.

has impacted the military strategy, Valeriano, Jensen, and Maness determine that the tools of cyberspace assist in C4I tasks, which hinge on the flow of information.⁶⁰⁵ They reach this determination through an analysis of cyber incidents involving the U.S. The data suggests that the U.S. leverages cyber tools to gain information superiority in order to enable offensive operations.⁶⁰⁶ Hence, the literature underscores how OCO enables actors to seize the information advantage, tipping the balance towards the offense.

Now, U.S. doctrine underscores the belief that the technology of cyber conflict enables the information advantage. The 2018 DOD Cyber Strategy emphasizes this point: “Computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control.”⁶⁰⁷ This view has further cemented through the recent Cyberspace Solarium Commission—an interagency panel to develop U.S. cyber strategy.⁶⁰⁸ The military recognizes the enormous impact that cyber conflict has on information, as the tenets of military power, including command and control, intelligence, and information warfare, all intertwine extensively with cyberspace.⁶⁰⁹ Undertaking offensive actions aids in control of the information flow through this environment—a point realized by other major powers throughout the world. For instance, China has made keen use of its advanced persistent threat (APT) cyber groups to collect foreign security information, while Chinese national companies have made inroads towards controlling key information supply chains.⁶¹⁰ Likewise, Russia has also demonstrated a deft ability to

⁶⁰⁵ In their analysis, the authors use the phrase “reconnaissance-strike” to describe the IT-RMA: Valeriano, Jensen, and Maness, *Cyber Strategy*, 171–80.

⁶⁰⁶ “The collection of incidents ... fits how the United States conducts its operations according to strategic doctrine: gain information superiority, identify the optimal targets, and conduct a precision strike at the right moment”: Valeriano, Jensen, and Maness, 180.

⁶⁰⁷ Mattis, *2018 DOD Cyber Strategy*, 1.

⁶⁰⁸ “For U.S. warfighting, in particular, cyber options enable the Joint Force to gain an information advantage, exercise global command and control, and execute strikes at long range”: Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 112.

⁶⁰⁹ U.S. Department of Defense, *JP 3-12*, xi-xii.

⁶¹⁰ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 9–10.

manipulate information via cyber means, including information warfare-style campaigns to isolate its military opponents and operations to inject doubt into western institutions.⁶¹¹

Further, recent telling examples illustrate the tie between offensive action in cyber conflict and the information advantage. In June 2013, news broke of a contractor at the National Security Agency (NSA) named Edward Snowden, who had revealed the existence of a U.S.-led surveillance and data-mining program entitled PRISM.⁶¹² While the aftermath of the story focused mostly on the NSA's actions and the ethics of whistleblowing, another important theme emerges in an offense-defense analysis: the U.S.'s desire to seize an unprecedented information advantage through offensive operations in cyberspace. The Snowden documents revealed more than 61,000 intrusive cyber operations and an active surveillance program aimed at maintaining situational awareness on all digital traffic involving U.S. servers.⁶¹³ Though not as damning and expansive as the Snowden documents, several open-source examples also reveal China's preference for going on the offensive to maintain an information edge. In an operation that ran from 2008 to 2014, for instance, Chinese operatives collected digital copies of U.S. defense platforms, including the C-17 transport aircraft.⁶¹⁴ The knowledge of foreign defense material provides China aware of the total threat environment that the country faces. Finally, Russia has also demonstrated the value of leveraging offensive cyber operations to manipulate the information environment. In the Russo-Georgia War in 2008, Russia's multi-domain invasion included a massive distributed denial of service (DDOS) attack and cyber defacement campaign that isolated Georgia and its population at a point that information was crucial for support of the war. The cyber-attacks limited the Georgian government

⁶¹¹ Cyberspace Solarium Commission, 11–12.

⁶¹² Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post*, 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," 7 June 2013, <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

⁶¹³ Kaplan, *Dark Territory*, 228–35.

⁶¹⁴ *Plea Agreement for Defendant Su Bin*, No. SA CR 14–131, (22 March 2016), 7–15. <https://www.justice.gov/opa/file/834936/download>.

response and helped Russia achieve marked domestic support, while also winning over large swaths of Georgians during the short campaign.⁶¹⁵ Similarly, the offensive cyber operations of Russia proved effective at sowing discord in the U.S., as Russian hacks during the 2016 Presidential campaign further demonstrated how cyber conflict may impact the information battlespace.⁶¹⁶ In sum, examples abound showing how actors undertake cyber operations to try to seize the information advantage.

G. DECISIVE EFFECTS—CYBER CONFLICT

Unfortunately, it is unclear whether the present conditions in cyber conflict permit actors to achieve decisive effects in cyber conflict, rendering this offense-defense variable a “wash.” In the context of the offense-defense balance, the decisive effects variable signifies the degree to which technological and geographic factors build the perception that the offense is able to completely overwhelm the defense. Though offensive cyber operations possess many of the same strategic abilities that airpower purports to offer—including the simultaneous layering of effects throughout a theater—the extent to which those effects can overwhelm an opponent is not evident in the literature or doctrine. If cyber weapons do possess the ability to render decisive effects, it is not through rapid or overt attacks. Rather, OCO deploy slowly and often produce effects in a subtle way, leaving the effectiveness a cyber offensive as a question mark in the open-source literature. However, the clearest indicator that the strategic effectiveness of cyber-attacks is inconclusive emanates from the DCID analysis of Valeriano, Jensen, and Maness, who note, “[s]tates seeking to leverage cyber actions to achieve decisive effects are likely to be disappointed.”⁶¹⁷ States are likely realizing that they cannot produce decisive cyber effects without paying a great cost, putting this reality at odds with the strategic discussion of a

⁶¹⁵ Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 96–127.

⁶¹⁶ Ellen Nakashima and Shane Harris, “How the Russians hacked the DNC and passed its emails to WikiLeaks,” *Washington Post*, 13 July 2018, https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

⁶¹⁷ Valeriano, Jensen, and Maness, *Cyber Strategy*, 203.

“cyber pearl harbor” and the persisting fears that catastrophic vulnerabilities exist in the cyber domain.⁶¹⁸

A review of open-source literature, doctrine, and historical events purveys that the efficacy of strategic cyber-attacks is inconclusive, and the discussion begins with the “fearful” side of the aisle—the view that actors can achieve decisive effects. In 1997, the DOD launched a two-week exercise called Eligible Receiver.⁶¹⁹ The purpose of Eligible Receiver was to employ red teams to find weaknesses in U.S. defenses, and, though the DOD had used the exercise to explore other strategic concerns in the past, the 1997 iteration explored cyber weaknesses. The exercise tested the weaknesses of both critical infrastructure and military networks, and the results both remain startling and demonstrate how cyber-attacks may deliver decisive results.⁶²⁰ The red team was able to penetrate each tested network within a matter of days, including the command center that the president uses to transmit orders during wartime.⁶²¹ The results of cyber analysis like Eligible Receiver carried forward into the start warnings of Richard Clarke, who warns that the U.S. is vulnerable to a degree that it may suffer from “self-deterrence.”⁶²² Further, scholars at Naval Postgraduate School, who warn that a “cyber Pearl Harbor” could achieve a *fait accompli* as cyber effects may coerce a target while simultaneously fail to mobilize the target population as Pearl Harbor did in 1941.⁶²³ Similar fears also arise in the Cyberspace Solarium report, as the authors raise concerns that a sophisticated cyber power may choose to hold a rival’s critical infrastructure at risk.⁶²⁴ Finally, U.S. doctrine suggests that cyber

⁶¹⁸ James J. Wirtz, “The Cyber Pearl Harbor,” in *Cyber Analogies*, ed. John Arquilla and Emily O. Goldman (Monterey, CA: Naval Postgraduate School, 2014), 7, <https://calhoun.nps.edu/handle/10945/40037>.

⁶¹⁹ Kaplan, *Dark Territory*, 65–72.

⁶²⁰ Kaplan, 67.

⁶²¹ Kaplan, 68–69.

⁶²² Clarke and Knake, *Cyber War*, 156.

⁶²³ Emily O. Goldman, John Surdu, and Michael Warner, “The Cyber Pearl Harbor Analogy: An Attacker’s Perspective,” in *Cyber Analogies*, ed. John Arquilla and Emily O. Goldman (Monterey, CA: Naval Postgraduate School, 2014), 26–27, <https://calhoun.nps.edu/handle/10945/40037>.

⁶²⁴ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 8.

effects can create strategic effects; however, because doctrine is open-source, it does not elaborate, further.⁶²⁵

On the other side of the aisle, both the literature and historical events suggest that the concerns of decisive cyber effects are excessive. First, Arquilla points to the historical record of failures in the strategic attack paradigm, as strategic attack during WWII demonstrated that war-time populations tend to show resiliency and not submit to such attacks.⁶²⁶ Next, cyber incident data from the DCID reveals that while cyber coercion has shown some success, it is not any more successful than other coercive instruments.⁶²⁷ Further, cyber coercion generally produces results when emanating from a great power like the U.S., suggesting that the implied military might behind the cyber-attack may have produced results, as much as the cyber-attack, itself.⁶²⁸ Lindsay and Gartzke echo the sentiment that cyber effects are not decisive by themselves; rather, cyber effects produce results over a concerted campaign, that may require a prolonged effort.⁶²⁹ Rid also chimes in this debate, noting how mass sabotage has yet to unfold, and cyber weapons are precise in nature, meaning that actors target the specific actions of their adversaries, like Stuxnet targeted uranium enrichment.⁶³⁰ Finally, the best example of a strategic attack conducted purely in cyberspace is that of a mass cyber denial attack and website defacement against Estonia in 2007. Estonia, a country that relies heavily on cyberspace for much of its critical infrastructure, endured the months-long attack and ultimately did not make any concessions associated with the attack motivation.⁶³¹ In sum, the open-source record of OCO does not amount to a conclusive take on its ability to produce decisive effects.

⁶²⁵ U.S. Department of Defense, *JP 3-12*, IV-19.

⁶²⁶ Arquilla, "The Computer Mouse that Roared," 42.

⁶²⁷ Valeriano, Jensen, and Maness, *Cyber Strategy*, 203.

⁶²⁸ Valeriano, Jensen, and Maness, 203.

⁶²⁹ Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (New York: Oxford University Press, 2018).

⁶³⁰ Rid, *Cyber War Will Not Take Place*, 50–79.

⁶³¹ Valeriano, Jensen, and Maness, *Cyber Strategy*, 124–27.

H. EXPOSURE—CYBER CONFLICT

The offense-defense variable of exposure likely explains the offensive tendencies within cyber conflict more than any other. Those who wield OCO often pay an insignificant cost that fails to deter such actions, and even the most audacious acts tend to enact only a political cost that fails to produce lasting behavior change. Recall that exposure refers to the perception that militaries can undertake offensive actions while minimizing risk in the context of the offense-defense balance. In the case of cyber conflict, this analysis views “militaries” as cyber actors. Because the OCO requires minimal exposure for cyber actors, the lack of risk tips the cyber offense-defense balance towards the offense.

The minimal exposure of cyber actors undertaking OCO stems from three important attributes of cyber conflict: the low price-of-entry, the attribution problem, and physical stand-off. First, doctrine warns how superiority in cyberspace is impractical given the low price-of-entry and the subsequent immersion of cyber actors.⁶³² Thanks to globalization, Internet connectivity has spread to the corners of the globe, giving nearly everyone the tools to enter the playing field. From this interconnected environment, a difficult attribution problem has arisen for cyber defenders—it is quite difficult to find evidence that conclusively identifies the perpetrators of cyber-attacks. Moreover, once the victims of cyber-attacks locate evidence, coordinating the analysis and presenting it in a persuasive manner are both challenging tasks, as well.⁶³³ Adding to the attribution problem is the wide involvement of cyber proxies in cyber conflict, who further conceal the hand of the attack benefactor.⁶³⁴ Finally, cyber conflict is inherently a stand-off mode of conflict; few circumstances in cyber conflict require the offense to stand in range of the defense. The risk to attacking units in cyberspace only emerges when the attackers operate from a physical location making them vulnerable to capture or must physically access equipment.

Some emerging cyber defense strategies appear to impose some risk on the attacking units in cyber conflict; however, the strategies—including layered cyber

⁶³² U.S. Department of Defense, *JP 3-12*, I-2.

⁶³³ Rid and Buchanan, “Attributing Cyber Attacks,” 7.

⁶³⁴ Maurer, *Cyber Mercenaries*, 22–23.

deterrence and active cyber defense—largely fail to pose a physical threat to attackers. Instead, both of these strategies only impose time and resource costs on potential attackers. Layered cyber deterrence recently emerged from the Cyberspace Solarium, and the overall aim is to shape behavior, deny benefits, and impose costs through a “defend forward” strategy.⁶³⁵ Denying benefits and imposing costs refers to securing likely targets in a strategy akin to deterrence by denial, while also remaining prepared to recover from attacks and retaliate in kind, when necessary.⁶³⁶ Thus, layered cyber deterrence purports to hold cyber attackers at risk; however, that risk is largely existential. The primary risk for attacking units in layered cyber deterrence is the resources spent trying to break target security or the “in-kind” response (e.g., hack back) that does not physically threaten the attacking unit. The other cyber strategy that imposes risk on cyber-attackers is active cyber defense, which the cyber strategist Scott Jasper defines as, “the real-time detection, analysis, and mitigation of network security breaches combined with the *aggressive use of legal countermeasures* beyond network and state territorial boundaries ... The promise of active cyber defense is to deny benefits through systemic resilience and *impose cost through tailored disruption*.”⁶³⁷ While this also apes of defending forward, it also implies counteroffensive actions. Jasper also recommends use of embedded malware on target files to find the offenders and use of honeypots, or decoy files, as part of an active defense strategy.⁶³⁸ While layered cyber deterrence and active cyber defense both raise the level of risk for attacking units in cyber conflict, the risk is still markedly lower than the risk shouldered by attacking units in other modes of conflict.

I. INSULATION—CYBER CONFLICT

The insulating features that can offer protection in the physical domains do not have an analogous feature in cyber conflict that has proven effective. Firewalls and similar

⁶³⁵ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 7.

⁶³⁶ Cyberspace Solarium Commission, 26–30.

⁶³⁷ Emphasis added: Jasper, *Strategic Cyber Deterrence*, 165–66.

⁶³⁸ Jasper, 169–78.

passive cyber security measures do not offer sufficient insulation in cyberspace. In terms of geographic concerns, some countries also suffer from even less insulation in cyber conflict as their cyber infrastructure may rely on an adversary in the international system. The offense-defense variable of insulation refers to technological or geographic factors that appear to effectively shield defensive units. The general lack of effective insulation in cyber conflict tips the cyber offense-defense balance towards the offense.

The lack of insulation in cyberspace is a factor of crumbling passive defenses, the sheer volume of attacks, and, in some cases, geographical factors of the infrastructure. Passive defenses refer to those cybersecurity measures meant to operate without active prompting from cyber defenders through concealment or hardening of infrastructure, and typical examples include firewalls or encryption.⁶³⁹ Unfortunately, the determination and skill of cyber attackers has proven passive cyber defense insufficient. Former Assistant Secretary of Defense William Lynn notes, as much, concerning firewalls: “In cyberspace, the offense has the upper hand ... Adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions. In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun.”⁶⁴⁰ Similarly, encryption discourages many attacks; however, hackers continue to find innovative ways to overcome the security measure in their way.⁶⁴¹ Jasper points out that part of the reason for the failures of passive defense is the sheer volume of attacks.⁶⁴² Even if only 0.001 percent of one million attacks are successful at breaking the firewalls or encryption, ten attacks still produced success: “highly publicized data breaches at Sony Pictures, JP Morgan Chase, Anthem Health Service, and the OPM expose a failure of cyber defenses at civilian

⁶³⁹ Robert M. Lee, “The Sliding Scale of Cyber Security,” in *SANS Institute Reading Room* (North Bethesda, MD: SANS Institute, 2015), 2, <https://www.sans.org/reading-room>.

⁶⁴⁰ Lynn III, “Defending a New Domain,” 99.

⁶⁴¹ Lily Hay Newman, “A Decade-Old Attack Can Break the Encryption of Most PCs,” *Wired*, 14 September 2018, <https://www.wired.com/story/cold-boot-break-pc-encryption/>.

⁶⁴² Jasper, *Strategic Cyber Deterrence*, 130–31.

companies and government agencies of all sizes.”⁶⁴³ Finally, the Russo-Georgian War provides an example of how geography may further pinch the cyber insulation for select countries. At the time Russia’s invasion of Georgia, roughly half of Georgia’s cyber infrastructure passed through Russia.⁶⁴⁴ In other words, Georgia was highly reliant on Russia for its cyber connectivity, making Georgia a soft target for Russia in terms of its offensive cyber campaign. If Georgia had hoped to wage an information campaign against Russia during the war, it would have to find a way other than through its Internet providers in Russia. Hence, geography can further impact the insulation of cyber conflict, tipping the balance further towards the offense.

J. CRITICALITY—CYBER CONFLICT

While the precise nature of critical infrastructure vulnerability is a sensitive and, thus, classified topic, the open-source record indicates that actors on the international stage perceive an ability to target objects critical to their opponents via cyberspace. In the context of the offense-defense balance, criticality represents the degree to which targetable objects appear vital to a population’s security or welfare. Cyber conflict purports to allow the targeting of both critical infrastructure and the C4I systems on which modern militaries now rely. This tie between cyberspace and critical systems tips causes the criticality variable to tip the cyber offense-defense balance towards the offense. Already, this chapter covers the doctrinal belief that cyber effects can produce strategic effects; however, this statement does not reveal the targeting process of OCO, leaving the reader to guess the form that critical targets may take in cyber conflict.⁶⁴⁵ Thankfully, the historical record and investigative journalism provide a means to conceptualize the types of targets that strategic cyber conflict may hold at risk.

Three particular examples—the Stuxnet case study, the Eligible Receiver exercise, and the 2015 Ukrainian power outage—provide a means to grasp the various critical assets

⁶⁴³ Jasper, 130.

⁶⁴⁴ Russell, *Cyber Blockades*, 97.

⁶⁴⁵ U.S. Department of Defense, *JP 3-12*, IV-19.

that OCO may target. First, the Stuxnet case represents a landmark case in cybersecurity and cyber strategy scholarship. First uncovered in 2010, Stuxnet was a malicious computer code designed to target uranium enrichment centrifuges at Iran's Natanz nuclear facility, aiming to degrade or, in some cases, destroy the centrifuges.⁶⁴⁶ The code did this by specifically manipulating the air-gapped Siemens controllers at Natanz to run the centrifuges at speeds incommensurate with proper enrichment and, at times, spin fast enough to damage the centrifuges.⁶⁴⁷ Of note, the Stuxnet authors wrote it to only impact the controllers at Natanz then self-destruct in 2012.⁶⁴⁸ To say that the Stuxnet code demonstrated a high level of sophistication would be an understatement, and because it required the resources of a sophisticated state actor, the international consensus generally holds the U.S. and Israel responsible.⁶⁴⁹ To the Western world, uranium enrichment appeared vitally important to Iran.⁶⁵⁰ Many politicians and scholars debate the rationale behind Iran's enrichment, with explanations such as national pride, economic benefits, and a deterrence capability rising in the discussion.⁶⁵¹ What is clear is that Iran is willing to endure hardship to continue its uranium enrichment program. Despite the nuclear Non-Proliferation Treaty and painful sanctions centered on the enrichment, Iran has continued the enrichment to its own detriment, underscoring the importance of facilities like Natanz to Iran's regime.⁶⁵² In sum, the Natanz enrichment facility appeared critical to Iran, and OCO offered a means of targeting that critical asset.

⁶⁴⁶ Singer and Friedman, *Cybersecurity and Cyberwar*, 114–18; On the discovery of Stuxnet: Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *Washington Post*, 2 June 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

⁶⁴⁷ Singer and Friedman, *Cybersecurity and Cyberwar*, 114–18.

⁶⁴⁸ Singer and Friedman, 116.

⁶⁴⁹ Valeriano, Jensen, and Maness, *Cyber Strategy*, 197–99.

⁶⁵⁰ Barack Obama, *National Security Strategy* (Washington, DC: The White House, 2010), 23–26, <http://nssarchive.us/>.

⁶⁵¹ Uriel Abulof, "Revisiting Iran's Nuclear Rationales," *International Politics* 51, no. 3 (2014): 405, <https://doi.org/10.1057/ip.2014.9>.

⁶⁵² Stern Roger, "The Iranian Petroleum Crisis and United States National Security," *Proceedings of the National Academy of Sciences* 104, no. 1 (2007), <https://doi.org/10.1073/pnas.0603903104>.

The 1997 Eligible Receiver exercise represents another clear example of how cyber conflict can target critical assets. The reader is already familiar with the case study from this chapter—the DOD’s red teaming exercise revealed multiple weaknesses in cybersecurity throughout America’s critical infrastructure and the DOD’s vital computer networks. Of note, the exercise penetrated the C2 centers necessary to decision-making during national emergencies. Effective C2 lies at the heart of military operations, and cyber-attacks that threaten the unity of command pose a disquieting facet of cyber conflict.⁶⁵³ It is difficult to understate the criticality of C2 in modern warfare, and an actor that perceives an avenue to target C2 systems faces a tempting prospect.

One of the lingering fears on the fringes of U.S. consciousness is a coordinated cyber-attack that disrupts our power grids, a topic investigated in Ted Koppel’s *Lights Out*.⁶⁵⁴ That fear became a reality for 225,000 Ukrainians in December 2015; thankfully, it lasted less than six hours.⁶⁵⁵ Though direct attribution has proven elusive, the consensus amongst Ukrainians and several prominent U.S. politicians is that Russia and its proxies were behind the attacks.⁶⁵⁶ The attacks came at a sensitive time between Russia and Ukraine, as the Russian annexation had occurred in 2014, and Ukraine had made significant progress in cutting its dependence on Russia for energy.⁶⁵⁷ While conclusively judging the criticality of the power grid to the security and welfare of Ukraine may prove impossible, the record does indicate that Ukraine’s move towards energy independence partly hinged on their ability to demonstrate credibility as a reliable energy custodian to the rest of

⁶⁵³ Unity of command is a central principle of joint operations: U.S. Department of Defense, *JP 3-0, Change 1*, I-2.

⁶⁵⁴ Koppel, *Lights Out*, 4–16.

⁶⁵⁵ Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, (North Bethesda, MD: SANS Institute, 2016), iv-vi, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

⁶⁵⁶ Donghui Park, Julia Summers, and Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, (Seattle, WA: University of Washington School of International Studies, 2017), <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>.

⁶⁵⁷ Park, Summers, and Walstrom, *Cyberattack on Critical Infrastructure*; Kofman et al., *Lessons from Russia’s Operations in Crimea and Eastern Ukraine*.

Europe.⁶⁵⁸ Moreover, the simple fact that Ukraine had undertaken steps toward energy independence suggested that it viewed the power grid as a critical national asset. The cyber-attack that temporarily cut power to swaths of the country served as a signal from Russia that it could influence life through Ukraine. It is also evidence that OCO can impact something as critical to national welfare as the power grid, swinging the cyber offense-defense balance toward the offense.

K. RESILIENCE—CYBER CONFLICT

As resilience denotes the ability to recover from an attack, the global trend of rapid innovation in cyberspace has unfortunately hurt the resilience of cyber conflict. To cage the cyber resilience discussion, NIST defines resilience as, “[t]he ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption.”⁶⁵⁹ At first glance, cyber resilience amounts to a case-by-case issue as the unit-level of analysis suggests that some states and organizations may easily recover from an attack, while others may suffer prolonged consequences. Richard Clarke further emphasizes this variance in cyber resilience with his “overall cyber war strength” analysis.⁶⁶⁰ For instance, when Clarke published his book in 2010, he rated the U.S. twice as dependent on cyberspace as China, suggesting that U.S. resilience to cyber-attack was much lower than that of China, emphasizing the case-by-case point. However, this analysis ultimately concludes that the general resiliency of cyber conflict is relatively low as the global trend remains clamoring to integrate cyberspace into daily life before pausing to worry about the security risks. Because of the low resiliency in cyber conflict, the cyber offense-defense balance tips toward the offense.

Over the past few years, a few separate commissions have labeled cyber resiliency as insufficient, including Cyberspace Solarium Commission and the 2018 Public-Private

⁶⁵⁸ Park, Summers, and Walstrom, *Cyberattack on Critical Infrastructure*.

⁶⁵⁹ Ross et al., *SP 800–160 Vol 2*, 62.

⁶⁶⁰ Clarke and Knake, *Cyber War*, 148.

Analytic Exchange Program on cyber resilience.⁶⁶¹ While the public and private sectors have realized strides toward resiliency through information sharing and investigative commissions, the problem remains.⁶⁶² The predominant factor hurting resiliency is the onslaught of new threats and vulnerabilities that endlessly arise, and the needed solutions simply do not materialize fast enough.⁶⁶³ The Public-Private Exchange specifically lists four overarching cybersecurity trends that continue to impair cyber resilience:⁶⁶⁴

1. Lengthy technology refresh cycles
2. The limited number of vendors supporting critical infrastructure
3. Proprietary code forces the use of outdated systems
4. Vendors do not always have to design with security as the priority

Collectively, these trends can produce a cyber incident from which companies may struggle to recover. For example, many airlines still use a reservation system that includes software created in the 1960s on the COBOL programming language—an outdated language with few programmers left that are well-versed in its use.⁶⁶⁵ In the event of a cyber incident involving the airline reservation systems, recovery teams may find themselves scrambling to locate someone proficient in COBOL, adding to the recovery time. While these four trends may center on resiliency in the U.S., similar problems haunt cybersecurity worldwide. For instance, the Stuxnet case study applies here, as well: coding in the Natanz controls relied on “hard-coded” default passwords to simplify the installment process.⁶⁶⁶ This shortcut reveals a vendor that did not design with security as one of its

⁶⁶¹ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 1; Public-Private Analytic Exchange Program, *Cyber Resilience and Response*, (Washington, DC: Office of the Director of National Intelligence, 2018), 1, https://www.dni.gov/files/PE/Documents/2018_Cyber-Resilience.pdf.

⁶⁶² Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 21.

⁶⁶³ Cyberspace Solarium Commission, 21.

⁶⁶⁴ Public-Private Analytic Exchange Program, *Cyber Resilience and Response*, 4.

⁶⁶⁵ Public-Private Analytic Exchange Program, 20.

⁶⁶⁶ Public-Private Analytic Exchange Program, 20–21.

priorities, and the Iranian enrichment facility paid the price. Cyber conflict has just begun its resiliency journey, and the record suggests that resiliency is currently low in cybersecurity. Hence, the cyber offense-defense balance still tips toward the offense.

L. CONCLUSION—CYBER CONFLICT

The cyber offense-defense balance analysis of this chapter finds that cyber conflict indeed favors the offense, implying that the technology and geography associated with cyber conflict encourage aggressive action. To sum up, cyberspace (a) is the foremost information platform, prompting adversaries to leverage cyber weapons to seize the information advantage; (b) has not conclusively demonstrated whether OCO can produce decisive effects; (c) almost completely limits the physical exposure of its attacking units; (d) fails to produce lasting insulation through its passive defenses; (e) has engendered several cyber-attacks of critical assets throughout the world; and (f) has not encouraged adequate resilience. Overall, cyber conflict encourages offensive actions in the international system. Data suggesting that cyberspace is, in fact, a relatively restrained environment is likely right; the analysis in this chapter simply concludes that reasons outside the offense-defense balance encourage any restraint present in cyberspace.

VI. CONCLUSION

A. TOWARD RELEVANT DEFINITIONS: OFFENSE-DEFENSE THEORY AND BALANCE

An applicable definition of the offense-defense theory must cut through the excess nuance that plagues the theory and tie directly to the offense-defense balance. Without a direct tie to the balance, the definition only builds confusion as it muddles the central concept of the theory--that conditions spark preferences for offense or defense, which carry corresponding implications. Two primary problems have haunted theorists tackling the offense-defense theory in the past: the divide between perception and reality and the issue of differentiating between offense and defense. First, this thesis argues that the objective truth, or reality of the offense-defense balance, is irrelevant; it is the *perceptions that are important* to the offense-defense balance because it is the perceptions that breed conflict.⁶⁶⁷

Next, differentiating between offense and defense further implies two additional issues that this thesis addresses: that of differentiating weapons and differentiating strategies.⁶⁶⁸ Weapon differentiation has been problematic for offense-defense theorists, as the critics point out that all weapons can often serve either offensive or defensive purposes. In short, there is no purely defensive weapon. This well-trodden point has merit, and this thesis contends that attempting to integrate offense-defense differentiation into the definition undermines the balance, and differentiation issues arise in several issues, including weapons or postures. Therefore, a clear definition of the offense-defense theory excludes differentiation. Defensive posturing may serve an essential role during crisis diplomacy; however, it only serves as a detractor in determining the balance and ought to be held as a parallel issue to the theory. Instead, offense-defense theory ought to strictly

⁶⁶⁷ “Objective [offense-defense balance] is a theoretical hoax”: Tang, “Offence-Defence Theory,” 216; “With offense-defense balance it is perception, not reality that is most important”: Buchanan, *Cybersecurity Dilemma*, 104.

⁶⁶⁸ A subset of the weapon differentiation is posturing. In this logical argument, the word posturing can fit where the word “weapon(s)” is used.

predict a set of behaviors based on the balance, which this thesis moves to determine based on a net sum of perceptual variables that describe technological and geographic factors. As the term implies, these variables change over time, altering the perceptions of those determining strategy.

The second issue of differentiation—that of strategies—also necessitates discussion in this section. Critics argue that modern conflict too often blurs the lines of offense and defense, even to the degree that distinguishing between them is impractical. This argument potentially undermines the offense-defense theory by suggesting that trying to categorize strategies as either offensive or defensive and determining a dominant side is a meaningless effort. These arguments ignore the fact that military operations have always had blurred lines; even Clausewitz famously admits this when he describes the merits of defense.⁶⁶⁹ Offense and defense pertain to the net sum of a campaign, and intellectual effort allows one to assign these roles. Further, modern warfare has prompted some academics to point out that militaries must execute offensive maneuvers just to accomplish defensive goals. For instance, cyber conflict requires intrusions to gather intelligence and bolster defenses.⁶⁷⁰ Such arguments do not undermine the categories of offense and defense. Instead, claiming that militaries must undertake offense just to obtain a viable defense is a tacit admission on two fronts: (1) there is a divide, and (2) offense is the dominant form of conflict.

Cutting through the nuance leads to the relevant definition offered in this thesis. The offense-defense balance identifies a *condition in the international system*. At its core, the offense-defense theory describes how strategy changes based on the *perceptions of decision-makers* about *military capability*.⁶⁷¹ Two particular factors sway these

⁶⁶⁹ See opening quote in chapter 2: Clausewitz, *On War*, 357.

⁶⁷⁰ Buchanan, *Cybersecurity Dilemma*, 72.

⁶⁷¹ The IR scholar Shiping Tang refers to the perceptions as the “subjective offense-defense theory”: Tang, “Offence-Defence Theory,” 240; Quester relates how offense-defense issues revolve around military capabilities: Quester, *Offense and Defense*, 2.

perceptions: *technology and geography*.⁶⁷² Conditions favoring an offensive strategy are those that render offensive actions to appear more effective or dominant to defensive actions, or vice versa.⁶⁷³ These conditions signify the *balance* between offense and defense, or the relative weight that individuals give to either the offense or defense. In turn, the balance brings two distinct implications. When the balance favors *offense*, the actors are *prone to aggression*, and escalation is likely; when the balance favors *defense*, actors *favor the status quo*.⁶⁷⁴ Because the theory underscores a condition in the international system, it does not conclusively indicate that a conflict is imminent. Instead, it merely implies that conditions may exist that can foster an outbreak of conflict. This definition eliminates the need to concern oneself with the “reality” of the balance and the issue of weapon differentiation.

B. THE FACTORS AND VARIABLES OF THE OFFENSE-DEFENSE BALANCE

What are those conditions tipping the offense-defense balance? The literature generally agrees that the balance tips as the result of military capability, and military capability stems from technology and geography.⁶⁷⁵ The analysis in this thesis offers pertinent definitions of technology and geography and then distills six variables that tip the balance, producing an analytical framework for the offense-defense balance. *Technology* is the sum of devices, components, practices, and skills meant to fulfill a human purpose, while *geography* refers to the spatial conditions that affect the employment of capabilities.⁶⁷⁶ Ultimately, the offense-defense balance tips as the result of six variables:

⁶⁷² Jervis, “Cooperation,” 194; Quester, *Offense and Defense*, 2; Van Evera, “Offense, Defense, and the Causes of War,” 16–19; Snyder, *The Ideology of the Offensive*, 19–22.

⁶⁷³ Another phrase that is common in the offense-defense theory literature is “relative ease” of offense or defense. This phrase is more useful if the underlying assumption is that states have an overall preference for conquest or war. See, for instance: Lieber, “Grasping the Technological Peace.”; Van Evera, “Offense, Defense, and the Causes of War,” 5.

⁶⁷⁴ Jervis, “Cooperation,” 187–211.

⁶⁷⁵ Quester, *Offense and Defense*, 2; Jervis, “Cooperation,” 194.

⁶⁷⁶ See chapter three for the references feeding these definitions.

the information advantage, decisive effects, exposure, insulation, criticality, and resilience. This thesis defines these variables in the following way:⁶⁷⁷

5. *Information advantage*: the degree to which modern technological and geographic factors build the perception that its users either enjoy an operational advantage conferred by the flow of information or believe that they can rapidly seize such an advantage.
6. *Decisive effects*: the degree to which technological and geographic factors generate perceptions that offensive actions are likely to nullify, undermine, or wholly overcome adversaries or their defenses.
7. *Exposure*: the degree to which technological and geographic factors enable perceptions that offensive actions require the assumption of risk for the attacking units.
8. *Insulation*: the degree to which technological and geographic factors appear to either disallow or shield any defensive units or nonbelligerent objects from an adversary's attacks.
9. *Criticality*: the degree to which targetable objects appear necessary to a population's security or welfare.
10. *Resilience*: the degree to which technology and geography offer the ability to recover from an attack.

An increase in each of these variables can sway the offense-defense balance one way or the other. Table 3 succinctly summarizes how these variables impact the balance.

⁶⁷⁷ Note that doctrinal or other definitions of each variable abound in the literature. These definitions apply directly to the offense-defense balance context.

Table 3. The Factors and Variables of Offense-Defense Theory⁶⁷⁸

	Item	Definitions/Considerations	
Factors	Technology	Means to fulfill a human purpose	
	Geography	Spatial conditions that impact operations	
Variables	Item	Perception	An increase aids...
	Information advantage	Can manipulate the information	Offense
	Decisive effects	Nullifies or overwhelms defenses	Offense
	Exposure	Offense requires risk	Defense
	Insulation	Disallows or shields from attacks	Defense
	Criticality	Targetable items appear necessary	Offense
	Resilience	Ability to recover from attacks	Defense

C. TESTING THE VARIABLES

Before moving directly to cyber conflict and leveraging the offense-defense variables to assess the cyber offense-defense balance, this thesis demonstrates the robustness and applicability of the variables across a range of conflict. It does this by testing air warfare and IW, arriving at the results in Tables 4 and 5.

Table 4. Offense-Defense Analysis of Air Warfare

<u>Air Warfare</u>				Overall: <i>Offense</i>		
Variable	Information Advantage	Decisive Effects	Exposure	Insulation	Criticality	Resiliency
Favors	Offense	Offense	Offense	Offense	Offense	Offense

Predominantly, air warfare theorists emphasize that airpower is inherently offensive—a view shared by U.S. doctrine, as well. The offense-defense analysis of air warfare agrees with this assessment, implying that airpower builds the perception that it rewards those seizing the initiative. It does this primarily through mounting its decisive

⁶⁷⁸ Proposed in chapter three of this thesis

effects on the critical C2 assets of the adversary, which simultaneously allows it to manipulate the information flow in an air war.

Table 5. Offense-Defense Analysis of Irregular Warfare

<u>Irregular Warfare</u>				Overall: <i>Offense</i>		
Variable	Information Advantage	Decisive Effects	Exposure	Insulation	Criticality	Resiliency
Favors	Offense	Inconclusive	Offense	Offense	Offense	Inconclusive

IW is an interesting case study, as its unconventional nature requires an assignment of roles before an analysis of the offense-defense balance, unlike air warfare and cyber conflict. Based on the offense-defense theory definition from this thesis, the IW analysis considers the insurgency as the offensive role and the state as the defensive roles, unlike air warfare. Specifically, the offense-defense balance identifies a systemic condition that threatens the status quo, and because the overall campaign goal of an insurgency is to alter the status quo, it best fulfills the role of offense in an analysis of the balance.⁶⁷⁹ The IW offense-defense balance analysis also found two of the variables inconclusive: decisive effects and resiliency. This peculiarity emanates from a lack of evidence and inherently protracted nature of IW campaigns. However, the gains made up for the offense in the other variables--information advantage, exposure, and insulation--convincingly tip the IW offense-defense balance toward the offense. Fostering insurgencies has emerged as a trending strategy in international competition, which aligns with both the balance analysis and the predominant view of many IW theorists.⁶⁸⁰

Collectively, the case studies in Chapter IV—air warfare and IW—demonstrate how one may analyze the offense-defense balance using the variables in Table 3. Perhaps the most significant concern from Tables 4 and 5 is that the analysis did not find any

⁶⁷⁹ Chapter 4 further underscores this case study design.

⁶⁸⁰ Specifically, those trends are a vector away from major war towards competition in the “gray zone.” Some of the data associated with these trends are further explored in chapter 4.

defense-favoring variables. This outcome raises a few critiques. First, analysts may ask if the proposed variables of this thesis may be insufficient or prone to find the offense dominant. Second, at a deeper level, some critics may argue that the offense-defense theory contains fundamental flaws, sparking these lopsided findings. However, this thesis contends that these findings are consistent with modern trends in warfare. Actors continue to maneuver themselves into the offensive role of conflict, avoiding defensive campaigns when conditions permit. Thankfully, preferences for offensive strategies have not produced any recent wars amongst the world's great powers. The likely explanation for the drought in major wars is that factors external to the offense-defense balance—such as effective deterrence strategies and meaningful diplomacy—are producing results. Unfortunately, the world does suffer from conflict and violent competition below the threshold of armed conflict, especially major war. In this vein, IW and cyber conflict both continue, unabated; accordingly, conditions in IW and cyber conflict warrant investigation.

D. THE CYBER OFFENSE-DEFENSE BALANCE

Finally, through the offense-defense variables and the resulting analytical framework, this thesis assesses the cyber offense-defense balance. Already, the reader is familiar with the opinions of a few well-positioned experts: cyber conflict favors the offense. The growing number of “incidents” between states and significant non-state actors in cyberspace further underlines this point.⁶⁸¹ Ultimately, the analysis of Chapter V agrees with this point—the cyber offense-defense balance tips toward the offense. An essential factor in this conclusion is the definition of cyber offense. This thesis proceeds with the U.S. doctrinal view cyber offense, which includes exploitation and attacks and, therefore, includes actions like attempted intrusions, which are both commonplace and escalatory in net effect. Finding that the balance favors the offensive side of the scale derives mainly from the information advantage proffered by offensive cyber actions. Moreover, the

⁶⁸¹ For a list of the growing “incidents” in cyberspace, see Appendix 3 of: Valeriano, Jensen, and Maness, *Cyber Strategy*, 230–46; For an authoritative definition of an “incident,” see: National Institute of Standards and Technology, *SP 800–53 Revision 4*, B-9.

attacking units of OCO can proceed with minimal to no exposure, and cyberspace builds the perception that the critically-needed items of large populations are targetable.

Table 6. Offense-Defense Analysis of Cyber Conflict

<u>Cyber Conflict</u>				Overall: <i>Offense</i>		
Variable	Information Advantage	Decisive Effects	Exposure	Insulation	Criticality	Resiliency
Favors	Offense	Inconclusive	Offense	Offense	Offense	Offense

E. THE IMPLICATIONS AND A LOOK TO THE FUTURE

The central implication of this work is that technology continues to incite particular behaviors within the international system. Admittedly, this implication is broad and nearly impossible to operationalize. One of the enduring critiques of the offense-defense theory is that it remains abstract, and past efforts to operationalize it have failed.⁶⁸² However, such critiques do not eliminate the need to build a better understanding of the environment, and the offense-defense balance aptly frames the dialogue and promotes comprehension. The strategies developed by the world's military members play a central role in international relations, and the failure of any military to understand how their weaponry guides decision-making can set the stage for disaster.

Choosing to overlook the conditions described by the offense-defense theory implies that military innovation brings no harm, and strategy curated for the sensible employment of new technologies is unnecessary. Stretching this flawed view to its logical extreme infers that the world is wrong to fear the next atomic bomb, in whatever form it may arrive—including a digital form. The analogy to nuclear strategy is fitting, as the Cold War (should have) taught the world that frightening innovations remain under lock and key only because of prudent strategy and careful diplomacy. In terms of cyber conflict, the

⁶⁸² Attempts to operationalize the theory have actually fallen flat, as demonstrated at the Disarmament Conference of 1932. One of the foremost tellings of this international conference can be found in: Boggs, *Attempts to Define and Limit*, 7–17.

prospect that international actors prefer offensive strategies should also prompt alarm. The offense-defense theory predicts that the relative weakness of cyber defense practically invites cyber-attacks, and the world's critical infrastructure offers a tempting set of targets—a point that Lynn and Clarke strive to emphasize. Given these implications and the growing debate about the cyber offense-defense-balance, identifying the conditions that could tip the scale can only advance this vital discourse.

In 2020, the congressionally-mandated Cyberspace Solarium Commission (CSC) brought together many of the leading strategists of cyber conflict to address the lapse in U.S. cybersecurity policy.⁶⁸³ The result is a report that offers impactful strategy while highlighting some of the key concerns from this thesis:⁶⁸⁴

The reality is that we are dangerously insecure in cyber ... A major cyberattack on the nation's critical infrastructure and economic system would create chaos and lasting damage ... To prevent this from happening, our report outlines a new cyber strategy and provides more than 75 recommendations for action across the public and private sectors ... we were all united by the recognition that the status quo is not getting the job done. The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility.

Looking through the lens of the CSC, there is reason to believe that the cyber offense-defense balance can tip toward the defense. The CSC repeatedly warns that the private sector's ownership of the attractive targets in cyberspace results in poor defensive intelligence, a lack of insulation, and increased vulnerability of critical assets.⁶⁸⁵ To combat this issue, the commission first aims to reduce the information advantage gleaned by OCO, through recommending the creation of a Joint Collaborative Environment and an integrated cyber center under the Cybersecurity and Infrastructure Security Agency

⁶⁸³ *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115–232, Title 16 Sec. 1652, 115th Congress, 2nd Session (13 Aug 2018). <https://www.congress.gov/bill/115th-congress/house-bill/5515/>.

⁶⁸⁴ Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, v-vi.

⁶⁸⁵ Cyberspace Solarium Commission, 96.

(CISA).⁶⁸⁶ These venues can share relevant threat and security information between the public and private sectors, keeping pace with the innovations of malicious actors. Second, the report suggests a host of security measures that increases insulation while reducing access to critical assets, including laws that hold vendors responsible for their goods' security, a cloud security certification, and tighter control over critical infrastructure.⁶⁸⁷ Finally, in a move that may ultimately tip the balance back toward the defense, the CSC report echoes the Obama administration's push for resiliency.⁶⁸⁸ This push comprises plans to develop Continuity of the Economy, codified distress indicators, funding for response and recovery, and a promotion of digital literacy.⁶⁸⁹ Digital literacy throughout the population can serve the dual purpose of combating disinformation campaigns that aim to tip the information advantage. Though time may tell if the U.S. cybersecurity community adopts the CSC recommendations, the will to improve defenses is evident.

The will to avoid conflict is further evident in a phrase maligned throughout this thesis: defend forward.⁶⁹⁰ Though the phrase tacitly admits that defense, alone, is inadequate, it also carries a tone of restraint. Yes—defending forward entails projecting power; however, it is not a purposeful stride to enact suffering. As long as the cyber offense-defense balance promotes perceptions that offense is the dominant strategy, the international community should expect actors to maintain a proactive stance, giving rise to strategies like defend forward. In this light, playing defense on the adversary's turf is the mentality that may elicit a respite from soaring tensions.

⁶⁸⁶ Cyberspace Solarium Commission, 5–6.

⁶⁸⁷ Cyberspace Solarium Commission, 4–5.

⁶⁸⁸ Obama, *PPD-21*; Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report*, 54.

⁶⁸⁹ Cyberspace Solarium Commission, 4–5.

⁶⁹⁰ Cyberspace Solarium Commission, 24.

LIST OF REFERENCES

- Abulof, Uriel. "Revisiting Iran's Nuclear Rationales." *International Politics* 51, no. 3 (2014): 404–15. <https://doi.org/10.1057/ip.2014.9>.
- Adams, Eric. "How the U.S. Prepares Its Embassies for Potential Attacks." *Wired*, 3 January 2020. <https://www.wired.com/story/how-us-prepares-embassies-potential-attacks/>.
- Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel*. Stanford, CA: Stanford University Press, 2010.
- Allison, Graham, Dimitri Simes, and James Thomson. *America's National Interests: A Report from the Commission on America's National Interests*. Cambridge, MA: Belfer Center for Science and International Affairs, 1996. <https://www.belfercenter.org/publication/americas-national-interests-report-commission-americas-national-interests-1996>.
- Ambrose, Stephen E. *D-Day, June 6, 1944: The Climactic Battle of World War II*. New York: Simon & Schuster, 1994.
- Arnold, Henry H. *Global Mission*. First ed. New York: Harper & Brothers, 1949.
- Arquilla, John. "The Computer Mouse that Roared: Cyberwar in the Twenty-First Century." *The Brown Journal of World Affairs* 18, no. 1 (2011): 39–48.
- . "Cyberwar Is Already Upon Us: But Can It Be Controlled?" *Foreign Policy*, 27 February 2012. <http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/>.
- . "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers." *Communications of the ACM* 54, no. 10 (2011): 58–65. <https://doi.org/10.1145/2001269.2001287>.
- Arquilla, John, and David Ronfeldt. "The Advent of Netwar (Revisited)." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt, 1–28. Santa Monica, CA: RAND Corporation, 2001. https://www.rand.org/pubs/monograph_reports/MR1382.html.
- . "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–65. <https://doi.org/10.1080/01495939308402915>.
- . "A New Epoch—and Spectrum—of Conflict." In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 1–20. Santa Monica, CA: RAND Corporation, 1997.

- Arthur, W. Brian. *The Nature of Technology: What It Is and How It Evolves*. New York: Penguin Books, 2009.
- Avionics Department. *Electronic Warfare and Radar Systems Engineering Handbook*. NAWCWD TP 8347, Fourth ed. Point Mugu, CA: Naval Air Warfare Center Weapons Division, 2013. <https://apps.dtic.mil/docs/citations/ADA617071>.
- Awan, Imran. "Cyber-Extremism: Isis and the Power of Social Media." *Society* 54, no. 2 (2017): 138–49. <https://doi.org/10.1007/s12115-017-0114-0>.
- Becker, Miriam D. "Strategic Culture and Ballistic Missile Defense: Russia and the United States." *Airpower Journal* 8, no. 1 (Special Edition) (1994): 57–68. <https://www.airuniversity.af.edu/ASPJ/Archived-Editions/>.
- Belk, Robert, and Matthew Noyes. *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive U.S. Cyber Policy*. Cambridge, MA: Harvard University Belfer Center for Science and International Affairs, 2012. belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy.
- Boggs, Marion W. *Attempts to Define and Limit "Aggressive" Armament in Diplomacy and Strategy*. The University of Missouri Studies. Edited by H. M. Belden, Henry E. Bent, E. B. Branson, A. H. R. Fairchild, Martin L. Faust, Addison Gulick, John G. Heinberg et al. Columbia, MO: University of Missouri, 1941.
- Brantly, Aaron F. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Studies in Security and International Affairs. Edited by William W. Keller and Scott A. Jones. Athens, GA: The University of Georgia Press, 2016.
- Brennan, Donald G. "Strategic Alternatives: I." *New York Times*, 24 May 1971. <https://www.nytimes.com/1971/05/24/archives/strategic-alternatives-i.html>.
- Brodie, Bernard. *Strategy in the Missile Age*. R-335. Santa Monica, CA: RAND Corporation, 1959. https://www.rand.org/pubs/commercial_books/CB137-1.html.
- Buchanan, Allen, and Robert O. Keohane. "The Preventive Use of Force: A Cosmopolitan Institutional Proposal." *Ethics & International Affairs* 18, no. 1 (2004): 1–22. <https://doi.org/10.1111/j.1747-7093.2004.tb00447.x>.
- Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford University Press, 2016.
- Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*, 11 October 2012. <https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>.

- Bunker, Robert J. *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications*. Strategic Studies Institute Papers. Carlisle Barracks, PA: Army War College Press, 1998. https://ssi.armywarcollege.edu/ssi_pubs/.
- Burrows, William E. “Ballistic Missile Defense: The Illusion of Security.” *Foreign Affairs* 62, no. 4 (1984): 843–56.
- Butterfield, Herbert. *History and Human Relations*. London, UK: Collins Clear-Type Press, 1951.
- Callwell, C. E. *Small Wars: Their Principles and Practice*. Third ed. Lincoln, NE: University of Nebraska Press, 1996.
- Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. *The Diamond Model of Intrusion Analysis*. ADA586960. Hanover, MD: Center for Cyber Threat Intelligence and Threat Research, 2013. <http://www.activeresponse.org/fundamental-intrusion-analysis-reading-list>.
- Carr, E. H. *The Twenty Years’ Crisis, 1919–1939: An Introduction to the Study of International Relations*. 1981 Printing of the Second ed. London, UK: Macmillan Press, 1946.
- Carter, John R. *Airpower and the Cult of the Offensive*. Air University CADRE Papers. Maxwell AFB, AL: Air University Press, 1998. <https://www.airuniversity.af.edu/AUPress/CADRE-Papers/>.
- Caulaincourt, Armand de. *With Napoleon in Russia*. Edited by Jean Hanoteau and Goerge Libaire. Mineola, NY: Dover Publications, 2005.
- Central Intelligence Agency, “The Office of Strategic Services: Morale Operations Branch,” *CIA News and Information* (Featured Story), Updated 30 April 2013 2010, accessed 5 March 2020, <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-morale-operations.html>.
- “Chapter I: Purposes and Principles.” In *Charter of the United Nations*. San Francisco, CA: The United Nations Conference, 1945. <https://www.un.org/en/charter-united-nations/index.html>.
- “Chapter Two: Comparative Defence Statistics.” *The Military Balance* 120, no. 1 (2020): 21–27. <https://doi.org/10.1080/04597222.2020.1707962>.
- Cheung, Tai Ming, Thomas G. Mahnken, and Andrew L. Ross. *Assessing the State of Understanding of Defense Innovation*. San Diego, CA: The Study of Innovation and Technology in China, 2018. <https://escholarship.org/uc/item/3wt3613v>.

- Christensen, Clayton M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Revised ed. Boston, MA: Harvard Business School Press, 1997.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat To National Security and What To Do About It*. First ed. New York: Ecco Publishing, 2010.
- Clausewitz, Carl von. *On War*. Edited and Translated by Michael Howard and Peter Paret. Indexed ed. Princeton, N.J: Princeton University Press, 1984.
- Coll, Steve. *Ghost Wars: The Secret History of the CIA, Afghanistan, and bin Laden, From the Soviet Invasion to September 10, 2001*. New York: Penguin Press, 2004.
- Conant, Eve. "6 of the World's Most Worrisome Disputed Territories." *National Geographic*, 28 March 2014.
<https://www.nationalgeographic.com/news/2014/3/140328-disputed-territories-geography-russia-crimea>.
- Congressional Budget Office. *Tactical Combat Forces of the United States Air Force: Issues and Alternatives*. Washington, DC: Congressional Budget Office, 1985.
<https://www.cbo.gov/sites/default/files/99th-congress-1985-1986/reports/85-cbo-008.pdf>.
- Conti, Gregory, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press, 2017.
- Cotterell, Arthur, Roger Lowe, and Ian Shaw. *Leadership: Lessons from the Ancient World*. Chichester, UK: John Wiley & Sons, 2006.
- Crile, George. *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History*. New York: Atlantic Monthly Press, 2003.
- Cyberspace Solarium Commission. *U.S. Cyberspace Solarium Commission Final Report*. Arlington, VA: The Cyberspace Solarium Commission, 2020.
<https://www.solarium.gov/>.
- Daugherty, William J. *Executive Secrets: Covert Action and the Presidency*. Lexington, KY: University Press of Kentucky, 2004.
- Davidson, Michael L. "Culture and Effects-based Operations in an Insurgency." SAMS thesis, U.S. Army Command and General Staff College, 2005.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.866.204&rep=rep1&type=pdf>.

- Davies, Michael C., and Frank G. Hoffman. "Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?" *Small Wars Journal*, 10 June 2013. <https://smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework>.
- Davis, James, Bernard Finel, Stacie Goddard, Stephen Van Evera, Charles Glaser, and Chaim Kaufmann. "Taking Offense at Offense-Defense Theory." *International Security* 23, no. 3 (1998): 179. <https://doi.org/10.2307/2539342>.
- De Mesquita, Bruce Bueno. *The War Trap*. New Haven, CT: Yale University Press, 1981.
- Denning, Dorothy E. "Terror's Web: How the Internet is Transforming Terrorism." In *Handbook of Internet Crime*, edited by Yvonne Jewkes and Majid Yar, 194–213. New York: Routledge, 2011. <https://www.routledgehandbooks.com/doi/10.4324/9781843929338>.
- Denning, Dorothy E., and Bradley J. Strawser. "Active Cyber Defense: Applying Air Defense to the Cyber Domain." In *Cyber Analogies*, edited by John Arquilla and Emily O. Goldman, 64–75. Monterey, CA: Naval Postgraduate School, 2014. <https://calhoun.nps.edu/handle/10945/40037>.
- Department of Defense Authorization Act for Fiscal Year 1987*. Pub. L. No. 99–661, Title 10 U.S.C. § 167. 99th Congress, 2nd Session, 14 Nov 1986. <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg3816>.
- Deptula, David A. *Effects-Based Operations: Change in the Nature of Warfare*. Arlington, VA: Aerospace Education Foundation, 2001. <http://www.ausairpower.net/PDF-A/AEF-AFA-Effect-Based-Operations-D.A.Deptula-2001.pdf>.
- DePuy, William E. "Active Defense (n.d.)." In *Selected Papers of General William E. DePuy*, edited by Richard M. Swain, Donald L. Gilmore and Carolyn D. Conway, 141–42. Fort Leavenworth, KS: Combat Studies Institute, 1995. <https://www.armyupress.army.mil/Books/CSI-Press-Publications/Doctrine/#books-doctrine>.
- . "Implications of the Middle East War on U.S. Army Tactics, Doctrine and Systems." In *Selected Papers of General William E. DePuy*, edited by Richard M. Swain, Donald L. Gilmore and Carolyn D. Conway, 75–112. Fort Leavenworth, KS: Combat Studies Institute, 1995. <https://www.armyupress.army.mil/Books/CSI-Press-Publications/Doctrine/#books-doctrine>.

- . “Letter to Creighton Abrams (January 1974).” In *Selected Papers of General William E. DePuy*, edited by Richard M. Swain, Donald L. Gilmore and Carolyn D. Conway, 69–74. Fort Leavenworth, KS: Combat Studies Institute, 1995.
<https://www.armyupress.army.mil/Books/CSI-Press-Publications/Doctrine/#books-doctrine>.
- Douhet, Giulio. *The Command of the Air*. Edited by Donna Budjenska. Translated by Dino Ferrari. Maxwell AFB, AL: Air University Press, 2019.
https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0160_DOUHET_THE_COMMAND_OF_THE_AIR.pdf.
- Economy, Elizabeth C. “The Great Firewall of China: Xi Jinping’s Internet Shutdown.” *The Guardian*, 29 June 2018.
<https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>.
- Eng, James, and Wendy Jones. “OPM Chief Says Government Agency Thwarts 10 Million Hack Attempts a Month.” news release, 16 June, 2015,
<https://www.nbcnews.com/tech/security/opm-chief-says-government-agency-thwarts-10-million-hack-attempts-n376476>.
- Examining the Equifax Data Breach: Hearing Before the Committee on Financial Services, U.S. House of Representatives*. Serial No. 115–46. 115th Congress, 1st Session, 5 October 2017. <https://www.govinfo.gov/app/details/CHRG-115hhrg30242/CHRG-115hhrg30242>.
- Falls, Cyril. “Geography and War Strategy.” *The Geographical Journal* 112, no. 1/3 (1948): 4–15. <https://doi.org/10.2307/1789151>.
- Farrell, Theo. “Strategic Culture and American Empire.” *The SAIS Review of International Affairs* 25, no. 2 (2005): 3–18.
<https://doi.org/10.1353/sais.2005.0033>.
- Fassihi, Farnaz. “Iran Blocks Nearly All Internet Access.” *New York Times*, 17 November 2019. <https://www.nytimes.com/2019/11/17/world/middleeast/iran-protest-rouhani.html>.
- Fearon, James D. “Counterfactuals and Hypothesis Testing in Political Science.” *World Politics* 43, no. 2 (1991): 169–95. <https://doi.org/10.2307/2010470>.
- . “Rationalist Explanations for War.” *International Organization* 49, no. 3 (1995): 379–414. <https://doi.org/10.1017/S0020818300033324>.
- Feickert, Andrew. *U.S. Special Operations Forces (SOF): Background and Issues for Congress*. RS21048. Washington, DC: Congressional Research Service, 2019.
<https://fas.org/sgp/crs/natsec/RS21048.pdf>.

- Finnemore, Martha, and Duncan B Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425–79.
- Frank, Benis M. *U.S. Marines in Lebanon 1982–1984*. Washington, DC: U.S. Marine Corps History and Museums Division, 1987.
- Freedom House, "Authoritarian Reach," *Freedomhouse.org*, ed. Arch Puddington, Nate Schenkkan and Sarah Cook 2020, accessed 3 April 2020, <https://freedomhouse.org/issues/authoritarian-reach>.
- Frey, Carl Benedikt, and Michael A. Osborne. "The Future of Employment: How Susceptible Are Jobs to Computerisation?." *Technological Forecasting & Social Change* 114 (2017): 254–80. <https://doi.org/10.1016/j.techfore.2016.08.019>.
- Fronza, Michael P. "Hannibal: Tactics, Strategy, and Geostrategy." Chap. 14 In *A Companion to the Punic Wars*, edited by Dexter Hoyos, Blackwell Companions to the Ancient World, 242–59. Malden, MA: Wiley-Blackwell, 2011.
- Fryer-Biggs, Zachary. "Coming Soon to a Battlefield: Robots That Can Kill." *The Atlantic*, 3 September 2019. <https://www.theatlantic.com/technology/archive/2019/09/killer-robots-and-new-era-machine-driven-warfare/597130/>.
- Fulghum, David A. "F-117 Pilots, Generals Tell Congress About Stealth's Value in Gulf War." *Aviation Week & Space Technology* 134, no. 18 (1991): 66–67.
- Gaddis, John Lewis. *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War*. Revised and Expanded ed. New York: Oxford University Press, 2005.
- Galula, David. *Counterinsurgency Warfare: Theory and Practice*. London, UK: Praeger, 2006.
- Garfinkel, Ben, and Allan Dafoe. "How Does the Offense-Defense Balance Scale?." *Journal of Strategic Studies* 42, no. 6 (2019): 736–63. <https://doi.org/10.1080/01402390.2019.1631810>.
- Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2 (2015): 316–48. <https://doi.org/10.1080/09636412.2015.1038188>.
- Gates, Robert M. "A Balanced Strategy: Reprogramming the Pentagon for a New Age." *Foreign Affairs* 88, no. 1 (2009): 28–40.
- . *Duty: Memoirs of a Secretary at War*. New York: Alfred A. Knopf, 2014.

- Gellman, Barton, and Laura Poitras. "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." *Washington Post*, 7 June 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.
- General Counsel of the U.S. Department of Defense. *Department of Defense Law of War Manual (Updated 2016)*. Washington, DC: U.S. Government Printing Office, 2015. https://permanent.access.gpo.gov/gpo71097/DOD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf.
- Geroski, Paul. *The Evolution of New Markets*. New York: Oxford University Press, 2003.
- Glaser, Charles L. *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton, NJ: Princeton University Press, 2010.
- Glaser, Charles L., and Chaim Kaufmann. "What is the Offense-Defense Balance and How Can We Measure It?." *International Security* 22, no. 4 (1998): 44. <https://doi.org/10.2307/2539240>.
- Godfrey-Smith, Peter. *Theory and Reality: An Introduction to the Philosophy of Science*. Chicago, IL: University of Chicago Press, 2003.
- Goldman, Emily O., John Surdu, and Michael Warner. "The Cyber Pearl Harbor Analogy: An Attacker's Perspective." In *Cyber Analogies*, edited by John Arquilla and Emily O. Goldman, 26–32. Monterey, CA: Naval Postgraduate School, 2014. <https://calhoun.nps.edu/handle/10945/40037>.
- Goldwater-Nichols Department of Defense Reorganization Act of 1986. Pub. L. No. 99–433, Title 10 U.S.C. § 161. 99th Congress, 2nd Session, 1 Oct 1986. <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg992>.
- Gomber, Peter, and Martin Haferkorn. "High-Frequency-Trading." *Business & Information Systems Engineering* 5, no. 2 (2013): 97–99. <https://doi.org/10.1007/s12599-013-0255-7>.
- Gordon, Shmuel L. "Air Superiority in the Israel-Arab Wars, 1967–1982." Chap. 6 In *A History of Air Warfare*, edited by John Andreas Olsen, 127–56. Washington, DC: Potomac Books, 2010.
- Gray, Colin S. *Another Bloody Century: Future Warfare*. New Haven, CT: Phoenix Press, 2007.
- . *Weapons Don't Make War: Policy, Strategy, and Military Technology*. Lawrence, KS: University Press of Kansas, 1993.

- Greenwald, Glenn, and Ewen MacAskill. "NSA Prism program taps in to user data of Apple, Google and others." 7 June 2013.
<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
- Hagel, Charles T. *Quadrennial Defense Review*. Washington, DC: Office of the Secretary of Defense, 2014. <https://dod.defense.gov/News/Special-Reports/QDR/>.
- Hahn, Otto. *Otto Hahn: A Scientific Autobiography*. Translated by Willy Ley. New York: Charles Scribner's Sons, 1966.
- Hallion, Richard P. "Air and Space Power: Climbing and Accelerating." Chap. 16 In *A History of Air Warfare*, edited by John Andreas Olsen, 371–93. Washington, DC: Potomac Books, 2010.
- Hart, B.H. Liddell. *Strategy*. Revised ed. Auckland, NZ: Pickle Partners Publishing, 2016. e-Book, Google Play. <http://www.pp-publishing.com/>.
- Haulman, Daniel L. "The Yamamoto Mission." *Air Power History* 50, no. 2 (2003): 30–37.
- Herz, John H. "Idealist Internationalism and the Security Dilemma." *World Politics* 2, no. 2 (1950): 157–80. <https://doi.org/10.2307/2009187>.
- Hoffman, Bruce. "The 'Cult of the Insurgent': Its Tactical and Strategic Implications." *Australian Journal of International Affairs* 61, no. 3 (2007): 312–29.
<https://doi.org/10.1080/10357710701531503>.
- Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institutes for Policy Studies, 2007.
<https://www.potomacinstitute.org/publications>.
- Hoffman, Tod. *Al Qaeda Declares War: The African Embassy Bombings and America's Search for Justice*. Lebanon, NH: University Press of New England, 2014.
- Horowitz, Michael C. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, NJ: Princeton University Press, 2010.
- Hosmer, Stephen T. *The Conflict Over Kosovo: Why Milosevic Decided to Settle When He Did*. MR-1351-AF. Santa Monica, CA: RAND Corporation, 2001.
https://www.rand.org/pubs/monograph_reports/MR1351.html.
- Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Bethesda, MD: Lockheed Martin Corporation, 2010.

- Intriligator, Michael D., and Dagobert L. Brito. "Can Arms Races Lead to the Outbreak of War?." *Journal of Conflict Resolution* 28, no. 1 (1984): 63–84.
<https://doi.org/10.1177/0022002784028001004>.
- Jamieson, Perry D. *Khobar Towers: Tragedy and Response*. Washington, DC: Air Force History and Museums Program, 2008.
- Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Lanham, MD: Rowman & Littlefield, 2017.
- Jensen, Benjamin M. *Forging the Sword: Doctrinal Change in the U.S. Army*. Stanford, CA: Stanford University Press, 2006.
- Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214. <https://doi.org/10.2307/2009958>.
- . *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.
- John S. McCain National Defense Authorization Act for Fiscal Year 2019. Pub. L. No. 115–232, Title 16 Sec. 1652. 115th Congress, 2nd Session, 13 Aug 2018.
<https://www.congress.gov/bill/115th-congress/house-bill/5515/>.
- Johnson, Chalmers A. *Revolutionary Change*. Stanford, CA: Stanford University Press, 1982.
- Jones, Andrew. *Human Geography: The Basics*. The Basic Series. New York: Routledge, 2012.
- Jones, Daniel M., Stuart A. Bremer, and J. David Singer. "Militarized Interstate Disputes, 1816–1992: Rationale, Coding Rules, and Empirical Patterns." *Conflict Management and Peace Science* 15, no. 2 (1996): 163–213.
<https://doi.org/10.1177/073889429601500203>.
- Juergensmeyer, Mark. *The New Cold War? Religious Nationalism Confronts the Secular State*. Comparative Studies in Religion and Society. First Paperback ed. Berkeley, CA: University of California Press, 1994.
- Kagan, Donald. *The Outbreak of the Peloponnesian War*. Ithaca, NY: Cornell University Press, 1969.
- Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.
- Kapur, S. Paul. "India and Pakistan's Unstable Peace: Why Nuclear South Asia Is Not Like Cold War Europe." *International Security* 30, no. 2 (2005): 127–52.
<https://doi.org/10.1162/016228805775124570>.

- Karnow, Stanley. *Vietnam: A History*. New York: Penguin Books, 1984.
- Keaney, Thomas A. "Surveying Gulf War Airpower." *Joint Force Quarterly* 2 (1993): 25–36. Published electronically 3rd Quarter (August) 1993.
<https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-2.pdf>.
- Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7–40.
https://doi.org/10.1162/ISEC_a_00138.
- King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press, 1994.
- Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. RR-1498. Santa Monica, CA: RAND Corporation, 2017.
https://www.rand.org/pubs/research_reports/RR1498.html.
- Komer, R. W. *The Malayan Emergency in Retrospect: Organization of A Successful Counterinsurgency Effort*. R-957-ARPA. Santa Monica, CA: RAND Corporation, 1972. <https://www.rand.org/pubs/reports/R957.html>.
- Koppel, Ted. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. First ed. New York: Crown Publishers, 2015.
- Kosso, Peter. *Reading the Book of Nature: An Introduction to the Philosophy of Science*. New York: Cambridge University Press, 1992.
- Krebs, Brian. "Terrorism's Hook Into Your Inbox." *Washington Post*, 5 July 2007.
<https://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html>.
- Kreis, John F. *Air Warfare and Air Base Air Defense, 1914–1973*. Washington, DC: Office of Air Force History, 1988.
- Krepinevich, Andrew F., Jr. *The Army and Vietnam*. Baltimore, MD: John Hopkins University Press, 1986.
- . "Cavalry to Computer: The Pattern of Military Revolutions." *The National Interest*, 1 September 1994. <https://nationalinterest.org/article/cavalry-to-computer-the-pattern-of-military-revolutions-848>.
- Lambeth, Benjamin S. *NATO's Air War for Kosovo: A Strategic and Operational Assessment*. MR-1365-AF. Santa Monica, CA: RAND Corporation, 2001.
https://www.rand.org/pubs/monograph_reports/MR1365.html.

- . “Operation Enduring Freedom, 2001.” Chap. 11 In *A History of Air Warfare*, edited by John Andreas Olsen, 255–78. Washington, DC: Potomac Books, 2010.
- . “The Technology Revolution in Air Warfare.” *Survival* 39, no. 1 (1997): 65–83. <https://doi.org/10.1080/00396339708442897>.
- Larson, Eric V., Derek Eaton, Brian Nichiporuk, and Thomas S. Szayna. *Assessing Irregular Warfare: A Framework for Intelligence Analysis*. MG-668-A. Santa Monica, CA: RAND Corporation, 2008. <https://www.rand.org/pubs/monographs/MG668.html>.
- Lawrence, T. E. *The Evolution of a Revolt*. Combat Studies Institute Reprint ed. Fort Leavenworth, KS: Army University Press, 1920. <https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/evolution-of-a-revolt.pdf>.
- Lee, Robert M. “The Sliding Scale of Cyber Security.” In *SANS Institute Reading Room*. North Bethesda, MD: SANS Institute, 2015. <https://www.sans.org/reading-room>.
- Lee, Robert M., Michael J. Assante, and Tim Conway. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. North Bethesda, MD: SANS Institute, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Leites, Nathan, and Charles Wolf, Jr. *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts*. Santa Monica, CA: RAND Corporation, 1970.
- Levy, Jack S. “The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis.” *International Studies Quarterly* 28, no. 2 (1984): 219–38. <https://doi.org/10.2307/2600696>.
- Lewis, Michael. *Flash Boys: A Wall Street Revolt*. New York: W.W. Norton, 2014.
- Lieber, Keir A. “Grasping the Technological Peace: The Offense-Defense Balance and International Security.” *International Security* 25, no. 1 (2000): 71–104. <https://doi.org/10.1162/016228800560390>.
- . “Mission Impossible: Measuring the Offense-Defense Balance with Military Net Assessment.” *Security Studies* 20, no. 3 (2011): 451–59. <https://doi.org/10.1080/09636412.2011.599193>.
- . “The Offense-Defense Balance and Cyber Warfare.” In *Cyber Analogies*, edited by John Arquilla and Emily O. Goldman, 96–107. Monterey, CA: Naval Postgraduate School, 2014. <https://calhoun.nps.edu/handle/10945/40037>.

- Lindsay, Jon R., and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." Chap. 9 In *Coercion: The Power to Hurt in International Politics*, edited by Kelly M. Greenhill and Peter Krause, 179–203. New York: Oxford University Press, 2018.
- Luttwak, Edward N. "The Operational Level of War." *International Security* 5, no. 3 (1980): 61–79. <https://doi.org/10.2307/2538420>.
- Lynn-Jones, Sean M. "Offense-Defense Theory and Its Critics." *Security Studies* 4, no. 4 (1995): 660–91. <https://doi.org/10.1080/09636419509347600>.
- Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (2010): 97–108.
- Mack, Andrew. "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict." *World Politics* 27, no. 2 (1975): 175–200. <https://doi.org/10.2307/2009880>.
- Mackesy, Piers. *The War for America, 1775–1783*. Cambridge, MA: Harvard University Press, 1964.
- Mahnken, Thomas G. "Uncovering Foreign Military Innovation." *Journal of Strategic Studies* 22, no. 4 (1999): 26–54. <https://doi.org/10.1080/01402399908437768>.
- Malone, Patrick J. "Offense-Defense Balance in Cyberspace: A Proposed Model." Graduate Thesis, Naval Postgraduate School, 2012. <http://hdl.handle.net/10945/27863>.
- Malovany, Pesach. *Wars of Modern Babylon: A History of the Iraqi Army from 1921 to 2003*. Translated by Ronna Englesberg. Lexington, KY: University Press of Kentucky, 2017.
- Mao Tse-tung. *Selected Military Writings of Mao Tse-tung*. Seattle, WA: Praetorian Press, 2011. e-Book.
- Marshall, Andrew W. *Some Thoughts on Military Revolutions (Second Version)*. Washington, DC: Office of the Secretary of Defense, 1993. <https://stacks.stanford.edu/file/druid:yx275qm3713/yx275qm3713.pdf>.
- Mason, Tony. "Operation Allied Force, 1999." Chap. 10 In *A History of Air Warfare*, edited by John Andreas Olsen, 225–52. Washington, DC: Potomac Books, 2010.
- Mattis, James N. *Summary of the 2018 Department of Defense Cyber Strategy*. Washington, DC: Office of the Secretary of Defense, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

- . *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*. Washington, DC: Office of the Secretary of Defense, 2018.
<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
- Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. New York: Cambridge University Press, 2018.
- McCormick, Gordon H. "People's Wars." In *Encyclopedia of Conflicts Since World War II*, edited by James Ciment, Kenneth L. Hill, David MacMichael and Carl Skutsch, 25–34. Armonk, NY: Sharpe Reference, 1999.
- 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>.
- Mearsheimer, John J. *Conventional Deterrence*. Cornell Studies in Security Affairs. Edited by Robert J. Art and Robert Jervis. Ithaca, NY: Cornell University Press, 1983.
- . *The Tragedy of Great Power Politics*. Updated ed. New York: W. W. Norton & Company, 2014.
- Meilinger, Phillip S. *10 Propositions Regarding Air Power*. Washington, DC: Air Force History and Museums Program, 1995.
- . "Supremacy in the Skies." *Air Force Magazine* 99, no. 2 (2016): 46–50. Published electronically February. <https://www.airforcemag.com/issue/2016-02/>.
- Mele, Christopher. "Data Breaches Keep Happening. So Why Don't You Do Something?" *New York Times*, 1 August 2018.
<https://www.nytimes.com/2018/08/01/technology/data-breaches.html>.
- Miles, Richard. "Hannibal and Propaganda." Chap. 15 In *A Companion to the Punic Wars*, edited by Dexter Hoyos, Blackwell Companions to the Ancient World, 260–79. Malden, MA: Wiley-Blackwell, 2011.
- Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*. Fifth ed. New York: Alfred A. Kopf, 1978.
- Morrow, John H., Jr. "The First World War, 1914–1919." Chap. 1 In *A History of Air Warfare*, edited by John Andreas Olsen, 3–25. Washington, DC: Potomac Books, 2010.

- Muller, Richard R. “The Air War in the Pacific, 1941–1945.” Chap. 3 In *A History of Air Warfare*, edited by John Andreas Olsen, 53–80. Washington, DC: Potomac Books, 2010.
- Munier, Bertrand R. “A Guide to Decision-Making Under Uncertainty.” In *Risk, Decision and Rationality*, edited by Bertrand R. Munier, Theory and Decision Library: Mathematical and Statistical Methods. Dordrecht, Holland: D. Reidel Publishing Company, 1988.
- Murray, Williamson. “Operation Iraqi Freedom, 2003.” Chap. 12 In *A History of Air Warfare*, edited by John Andreas Olsen, 279–96. Washington, DC: Potomac Books, 2010.
- Nakashima, Ellen, and Shane Harris. “How the Russians hacked the DNC and passed its emails to WikiLeaks.” *Washington Post*, 13 July 2018.
https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.
- Nakashima, Ellen, and Joby Warrick. “Stuxnet was work of U.S. and Israeli experts, officials say.” *Washington Post*, 2 June 2012.
https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.
- National Defense Authorization Act for Fiscal Year 2017*. Pub. L. No. 114–328, Title 10 U.S.C. § 167b. 114th Congress, 2nd Session, 23 Dec 2016.
<https://www.govinfo.gov/app/details/PLAW-114publ328/>.
- National Defense Authorization Act for Fiscal Year 2020*. Pub. L. No. 116–92, Title 9 U.S.C. § 9081. 116th Congress, 1st Session, 20 Dec 2019.
<https://www.congress.gov/bill/116th-congress/senate-bill/1790>.
- National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800–53 Revision 4. Gaithersburg, MD: National Institute of Standards and Technology, 2013. <https://csrc.nist.gov/publications/sp>.
- Naval Center for Cost Analysis, “NCCA Inflation Indices and Joint Inflation Calculator,” (web page), Updated April 2019, accessed 22 Jan 2020,
<https://www.ncca.navy.mil/tools/inflation.cfm>.
- Newman, Lily Hay. “A Decade-Old Attack Can Break the Encryption of Most PCs.” *Wired*, 14 September 2018. <https://www.wired.com/story/cold-boot-break-pc-encryption/>.
- Nye, Joseph S., Jr., and William A. Owens. “America’s Information Edge.” *Foreign Affairs* 75, no. 2 (1996): 20–36. <https://doi.org/10.2307/20047486>.

- Nye Jr, Joseph S. *The Future of Power*. New York: Public Affairs Press, 2011.
- Obama, Barack. *National Security Strategy*. Washington, DC: The White House, 2010. <http://nssarchive.us/>.
- . *Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience*. Washington, DC: The White House (Office of the Press Secretary), 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- Olsen, John Andreas. “Operation Desert Storm, 1991.” Chap. 8 In *A History of Air Warfare*, edited by John Andreas Olsen, 177–200. Washington, DC: Potomac Books, 2010.
- Olson, Eric T. “A Balanced Approach to Irregular Warfare.” *The Journal of International Security Affairs* 16 (2009).
- Oman, Charles. *A History of the Peninsular War: 1807–1809, From the Treaty of Fontainebleau to the Battle of Corunna*. Project Gutenberg e-book ed. VII vols. Vol. I, Oxford, UK: Clarendon Press, 1902.
- Ou, Ed. “Under a Nuclear Cloud.” *The Virginia Quarterly Review* 87, no. 4 (2011): 50–69.
- Overy, Richard. “The Air War in Europe, 1939–1945.” Chap. 2 In *A History of Air Warfare*, edited by John Andreas Olsen, 27–52. Washington, DC: Potomac Books, 2010.
- Owen, Robert C. “Operation Deliberate Force, 1995.” Chap. 9 In *A History of Air Warfare*, edited by John Andreas Olsen, 201–24. Washington, DC: Potomac Books, 2010.
- Pace, Steve. *The Projects of Skunk Works: 75 years of Lockheed Martin’s Advanced Development Programs*. Minneapolis, MN: Voyageur Press, 2016.
- Park, Donghui, Julia Summers, and Michael Walstrom. *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*. Seattle, WA: University of Washington School of International Studies, 2017. <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>.
- Parker, Charles F., and Eric K. Stern. “Blindsided? September 11 and the Origins of Strategic Surprise.” *Political Psychology* 23, no. 3 (2002): 601–30. <https://doi.org/10.1111/0162-895X.00300>.

- Pattison, William D. "The Four Traditions of Geography." *Journal of Geography* 89, no. 5 (1990): 202–06. <https://doi.org/10.1080/00221349008979196>.
- Peacock, Lindsay T. *Strategic Air Command*. London, UK: Arms & Armour Press, 1988.
- Perry, William J. "Let Wisdom Guide Our Use of the Military." *Navy Times*, 8 May 1995.
- Plea Agreement for Defendant Su Bin*. No. SA CR 14–131. 22 March 2016. <https://www.justice.gov/opa/file/834936/download>.
- Posen, Barry R. *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. Cornell Studies in Security Affairs. Edited by Robert J. Art and Robert Jervis. Ithaca, NY: Cornell University of Press, 1984.
- . "The Struggle against Terrorism: Grand Strategy, Strategy, and Tactics." *International Security* 26, no. 3 (2002): 39–55. <https://doi.org/10.1162/016228801753399709>.
- Pranow, J. B. *Greenland and its Strategic Importance*. AD-A137 433. Washington, DC: Naval Intelligence Support Center Translation Division, 1983. <https://apps.dtic.mil/docs/citations/ADA137433>.
- Priebe, Miranda, Alan J. Vick, Jacob L. Heim, and Meagan L. Smith. *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*. RR-2959-AF. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2959.html.
- Public-Private Analytic Exchange Program. *Cyber Resilience and Response*. Washington, DC: Office of the Director of National Intelligence, 2018. https://www.dni.gov/files/PE/Documents/2018_Cyber-Resilience.pdf.
- Quester, George H. *The Continuing Problem of International Politics*. New York: The Dryden Press, 1974.
- . *Offense and Defense in the International System*. International Relations Series. Edited by Richard Rosecrance. New York: John Wiley and Sons, 1977.
- Rao, G. A., and S. P. Mahulikar. "Integrated Review of Stealth Technology and Its Role in Airpower." *The Aeronautical Journal* 106, no. 1066 (2002): 629–41. <https://doi.org/10.1017/S0001924000011702>.
- Reagan, Ronald. *National Security Strategy of the United States*. Washington, DC: The White House, 1987. <https://history.defense.gov/Historical-Sources/National-Security-Strategy/>.

- Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013.
- Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37. <https://doi.org/10.1080/01402390.2014.977382>.
- Ritchie, Hannah, and Max Roser, "Urbanization," *OurWorldInData.org* (web page), ed. Oxford Martin Programme on Global Development, Updated November 2019, accessed 4 March 2020, <https://ourworldindata.org/urbanization>.
- Ritter, Gerhard. *The Schlieffen Plan: Critique of a Myth*. Translated by Andrew Wilson and Eva Wilson. Auckland, NZ: Eschenburg Press, 2018. e-Book. <http://www.pp-publishing.com/>.
- Roger, Stern. "The Iranian Petroleum Crisis and United States National Security." *Proceedings of the National Academy of Sciences* 104, no. 1 (2007): 377–82. <https://doi.org/10.1073/pnas.0603903104>.
- Rogers, Everett M. *Diffusion of Innovations*. Fifth ed. New York: Free Press, 2003.
- Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800–160 Volume 2. Gaithersburg, MD: National Institute of Standards and Technology, 2019. <https://doi.org/10.6028/NIST.SP.800-160v2>.
- Russell, Alison Lawlor. *Cyber Blockades*. Washington, DC: Georgetown University Press, 2014.
- Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34, no. 1 (2013): 40–63. <https://doi.org/10.1080/13523260.2013.771031>.
- Samuel, Lawrence R. *The American Way of Life: A Cultural History*. Fairleigh Dickinson Series in American History and Culture. Edited by Kalman Goldstein. Teaneck, NJ: Fairleigh Dickinson University Press, 2017.
- Sarkees, Meredith Reid, and Frank Wayman. "Resort to War: 1816–2007." In *Correlates of War*. Washington, DC: CQ Press, 2010. <http://www.correlatesofwar.org/datasets/COW-war>.
- Schelling, Thomas C. *The Strategy of Conflict*. 1980 Paperback ed. Cambridge, MA: Harvard University Press, 1960.
- Schelling, Thomas C., and Morton H. Halperin. *Strategy and Arms Control*. New York: The Twentieth Century Fund, 1961.

- Sechrist, Michael. *Cyberspace in Deep Water: Protecting Undersea Communications Cables By Creating an International Public-Private Partnership*. Cambridge, MA: Harvard University Belfer Center for Science and International Affairs, 2010. <https://www.belfercenter.org/publication/cyberspace-deep-water-protecting-undersea-communications-cables-creating-international>.
- Sharp, Jeremy M. *U.S. Foreign Aid to Israel*. RL33222. Washington, DC: Congressional Research Service, 2019. <https://fas.org/sgp/crs/mideast/RL33222.pdf>.
- Shirer, William L. *The Rise and Fall of the Third Reich: A History of Nazi Germany*. New York: Simon & Schuster, 1960.
- Singer, Peter W., and Emerson T. Brooking. *Like War: The Weaponization of Social Media*. Boston, MA: Houghton Mifflin, 2018.
- Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.
- Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment.” *International Security* 41, no. 3 (2016): 72–109. https://doi.org/10.1162/ISEC_a_00267.
- Smith, William, and Eugene Lawrence. *The History of Rome: From Early Times to the Establishment of the Empire*. Luton, UK: Andrews UK Limited, 2010.
- Snow, Jennifer J. “Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies.” Graduate Thesis, Naval Postgraduate School, 2015.
- Snyder, Glenn H. *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961. doi:10.1515/9781400877164.
- Snyder, Jack L. *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914*. Cornell Studies in Security Affairs. Edited by Robert J. Art, Robert Jervis and Stephen M. Walt. Ithaca, NY: Cornell University Press, 1989.
- . *Myths of Empire: Domestic Politics and International Ambition*. Cornell Studies in Security Affairs. Edited by Robert J. Art, Robert Jervis and Stephen M. Walt. Ithaca, NY: Cornell University Press, 1991.
- Snyder, Jack L., and Keir A. Lieber. “Defensive Realism and the ‘New’ History of World War I.” *International Security* 33, no. 1 (2008): 174–94.
- Stanik, Joseph T. “Welcome to El Dorado Canyon.” *Proceedings* 122 (1996): 57–64.
- Stefik, Mark, and Barbara Stefik. *Breakthrough: Stories and Strategies of Radical Innovation*. Cambridge, MA: MIT Press, 2004.

- Stein, Janice Gross. "Rational Deterrence against 'Irrational' Adversaries? No Common Knowledge." In *Complex Deterrence: Strategy in the Global Age*, edited by Thazha V. Paul, Patrick M. Morgan and James J. Wirtz, 58–82. Chicago, IL: University of Chicago Press, 2009.
- . "The Wrong Strategy in the Right Place: The United States in the Gulf." *International Security* 13, no. 3 (1989): 142–67. <https://doi.org/10.2307/2538739>.
- Stephens, Alan. "The Air War in Korea, 1950–1953." Chap. 4 In *A History of Air Warfare*, edited by John Andreas Olsen, 85–106. Washington, DC: Potomac Books, 2010.
- Stimson George, W., D. Griffiths Hugh, J. Baker Chris, and Dave Adamy. *Stimson's Introduction to Airborne Radar*. Third ed. Edison, NJ: SciTech Publishing, 2014.
- Stuckenberg, David, R. James Woolsey, and Douglas DeMaio. *Electromagnetic Defense Task Force 2.0*. Edited by Donna Budjenska. LeMay Papers. Maxwell AFB, AL: Air University Press, 2019. <https://www.airuniversity.af.edu/AUPress/LeMay-Papers/>.
- Sullivan, Walter. "Reds Proclaim a Republic In China; Chou Is Premier." *New York Times*, 2 October 1949, 1. <https://www.nytimes.com/1949/10/02/archives/reds-proclaim-a-republic-in-china-chou-is-premier-chinese-republic.html>.
- Tang, Shiping. "Offence-Defence Theory: Towards a Definitive Understanding." *Chinese Journal of International Politics* 3, no. 2 (2010): 213–60. <https://doi.org/10.1093/cjip/poq004>.
- . "The Security Dilemma: A Conceptual Analysis." *Security Studies* 18, no. 3 (2009): 587–623. <https://doi.org/10.1080/09636410903133050>.
- Taylor, A.J.P. *The Origins of the Second World War*. New York: Antheneum, 1962.
- The Joint Chiefs of Staff. *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3105.01: Joint Risk Analysis*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2019. <https://www.jcs.mil/Library/CJCS-Manuals/>.
- Thompson, Robert. *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam*. Studies in International Security. New York: Frederick A. Praeger, 1966.
- Thompson, Wayne. "Operations over North Vietnam, 1965–1973." Chap. 5 In *A History of Air Warfare*, edited by John Andreas Olsen, 107–26. Washington, DC: Potomac Books, 2010.

- Thucydides. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. Translated by Richard Crawley. Edited by Robert B. Strassler. New York: Free Press, 1996.
- Trager, Robert, and Dessislava P. Zagorcheva. “Deterring Terrorism: It Can Be Done.” *International Security* 30, no. 3 (2005): 87–123.
<https://doi.org/10.1162/016228805775969564>.
- Trump, Donald. *National Security Strategy of the United States*. Washington, DC: The White House, 2017. <http://nssarchive.us/>.
- Turbiville, Graham H., Jr. *Logistic Support and Insurgency: Guerrilla Sustainment and Applied Lessons of Soviet Insurgent Warfare*. JSOU Report 05–4. Hurlburt Field, FL: Joint Special Operations University, 2005.
<https://www.hsdl.org/?abstract&did=476313>.
- U.S. Air Force. *Air Force Doctrine Annex 3–0: Operations and Planning*. Maxwell AFB, AL: Lemay Center for Doctrine, 2016. <https://www.doctrine.af.mil/>.
- . *Air Force Doctrine Annex 3–01: Counterair Operations*. Maxwell AFB, AL: Lemay Center for Doctrine, 2019. <https://www.doctrine.af.mil/>.
- . *Air Force Doctrine Annex 3–51: Electromagnetic Warfare and Electromagnetic Spectrum Operations*. Maxwell AFB, AL: Lemay Center for Doctrine, 2019.
<https://www.doctrine.af.mil/>.
- . *Air Force Doctrine Annex 3–70: Strategic Attack*. Maxwell AFB, AL: Lemay Center for Doctrine, 2017. <https://www.doctrine.af.mil/>.
- . *Air Force Doctrine Volume I: Basic Doctrine*. Maxwell AFB, AL: Lemay Center for Doctrine, 2014. <https://www.doctrine.af.mil/>.
- . *Electronic Warfare Fundamentals*. Nellis AFB, NV: Air Warfare Center, 2000.
- . *Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*. Washington, DC: U.S. Air Force Headquarters, 2019.
<https://www.af.mil/Portals/1/documents/2019%20SAF%20story%20attachments/Air%20Force%20Science%20and%20Technology%20Strategy.pdf>.
- U.S. Army. *Field Manual 3–24: Counterinsurgency*. Washington, DC: Department of the Army Headquarters, 2006. <https://www.hsdl.org/?abstract&did=468442>.
- U.S. Cyber Command, “U.S. Cyber Command History,” 2019, accessed 21 August 2019, <https://www.cybercom.mil/About/History/>.

- U.S. Department of Defense. *DOD Dictionary of Military and Associated Terms*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2019. <https://www.jcs.mil/Doctrine/DOD-Terminology-Program/>.
- . *Joint Concept for Operating in the Information Environment (JCOIE)*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2018. <https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>.
- . *Joint Operating Concept: Irregular Warfare: Countering Irregular Threats, Version 2.0*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2010. <https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>.
- . *Joint Publication 1: Doctrine for the Armed Forces of the United States, Incorporating Change 1, 12 July 2017*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2013. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 2-03: Geospatial Intelligence in Joint Operations*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-0: Joint Operations, Incorporating Change 1, 22 October 2018*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-01: Countering Air and Missile Threats*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-05: Special Operations*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2014. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-12: Cyberspace Operations*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2018. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-13: Joint Operations, Incorporating Change 1, 20 November 2014*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2012. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-24: Counterinsurgency*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2018. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- . *Joint Publication 3-30: Joint Air Operations*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2019. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.

- . *Joint Publication 5-0: Joint Planning*. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2017. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/>.
- U.S. Government Accountability Office. *Electronic Warfare: DOD Should Select Most Cost-Effective Infrared Countermeasure System*. Washington, DC: U.S. Government Accountability Office, 1998. <https://www.gao.gov/archive/1998/ns98002.pdf>.
- . *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*. GAO-06-672. Washington, DC: U.S. Government Accountability Office, 2006. <https://www.gao.gov/assets/260/250483.pdf>.
- . *Special Operations Forces: Opportunities Exist to Improve Transparency of Funding and Assess Potential to Lessen Some Deployments*. GAO-15-571. Washington, DC: U.S. Government Accountability Office, 2015. <https://www.gao.gov/assets/680/671920.pdf>.
- U.S. Marine Corps. *Small Wars Manual (Reprint of 1940 Edition)*. Washington, DC: Department of the Navy, 1940.
- Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press, 2018.
- van Creveld, Martin. *Technology and War: From 2000 B.C. to the Present*. Revised and Expanded ed. New York: The Free Press, 1991.
- Van Evera, Stephen. *Causes of War: Power and the Roots of Conflict*. Cornell Studies in Security Affairs. Edited by Robert J. Art, Robert Jervis and Stephen M. Walt. Ithaca, NY: Cornell University Press, 1999.
- . “The Cult of the Offensive and the Origins of the First World War.” *International Security* 9, no. 1 (1984): 58–107. <https://doi.org/10.2307/2538636>.
- . “Offense, Defense, and the Causes of War.” *International Security* 22, no. 4 (1998): 5–43. <https://doi.org/10.1162/isec.22.4.5>.
- Vick, Alan J., Richard M. Moore, Bruce R. Pirnie, and John Stillion. *Aerospace Operations Against Elusive Ground Targets* MR-1398-AF. Santa Monica, CA: RAND Corporation, 2001. https://www.rand.org/pubs/monograph_reports/MR1398.html.
- von der Heydte, Friedrich August Freiherr. *Modern Irregular Warfare in Defense Policy and as a Military Phenomenon*. Translated by George Gregory. First English ed. New York: New Benjamin Franklin House, 1986.

- Waldman, Matt. "System Failure: The Underlying Causes of U.S. Policy-Making Errors in Afghanistan." *International Affairs* 89, no. 4 (2013): 825–43. <https://doi.org/10.1111/1468-2346.12047>.
- Walt, Stephen M. "Alliance Formation and the Balance of World Power." *International Security* 9, no. 4 (1985): 3–43. <https://doi.org/10.2307/2538540>.
- Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis*. 2001 ed. New York: Columbia University Press, 1959.
- . "The Origins of War in Neorealist Theory." *The Journal of Interdisciplinary History* 18, no. 4 (1988): 615–28. <https://doi.org/10.2307/204817>.
- . *Theory of International Politics*. Addison-Wesley Series in Political Science. First ed. Reading, MA: Addison-Wesley Publishing Company, 1979.
- Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. Fourth ed. New York: Basic Books, 2006.
- Warden, John A., III. *The Air Campaign: Planning for Combat*. Washington, DC: National Defense University Press, 1988.
- Warrick, Joby. *The Triple Agent*. New York: Vintage Books, 2012.
- Weigley, Russell F. *The American Way of War: A History of United States Military Strategy and Policy*. 1977 Paperback ed. Bloomington, IN: Indiana University Press, 1973.
- Weinberger, Caspar. "The Uses of Military Power." National Press Club Speech. Washington, DC: Office of Assistant Secretary of Defense, 1984.
- White, Jeffrey B. "Some Thoughts on Irregular Warfare: A Different Kind of Threat." *Studies in Intelligence* 39, no. 5 (1996), The Central Intelligence Agency's Center for the Study of Intelligence. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/>.
- Wilson, Greg. "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines." In *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, edited by Michael Freeman and Hy Rothstein, 27–32. Monterey, CA: Naval Postgraduate School, 2011. <https://calhoun.nps.edu/handle/10945/780>.
- Wirtz, James J. "The Cyber Pearl Harbor." In *Cyber Analogies*, edited by John Arquilla and Emily O. Goldman, 7–14. Monterey, CA: Naval Postgraduate School, 2014. <https://calhoun.nps.edu/handle/10945/40037>.

- Wohlforth, William C. "Realism." In *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal, 131–49. Oxford, UK: Oxford University Press, 2008.
<https://doi.org/10.1093/oxfordhb/9780199219322.003.0007>.
- Wohlstetter, Albert. "The Delicate Balance of Terror." *Foreign Affairs* 37, no. 2 (1958): 211–34. <https://doi.org/10.1080/00396335908440116>.
- Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.
- Woolf, Amy F. *Nonstrategic Nuclear Weapons*. RL32572. Washington, DC: Congressional Research Service, 2019.
<https://crsreports.congress.gov/product/pdf/rl/RL32572>.
- Wright, Quincy. *A Study of War*. Vol. 1, Chicago, IL: University of Chicago Press, 1942.
- Zasloff, J. J. *The Role of the Sanctuary in Insurgency: Communist China's Support to the Vietminh, 1946–1954*. RM-4618-PR. Santa Monica, CA: RAND Corporation, 1967.
https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM4618.pdf.
- Zimmermann, Klaus. "Roman Strategy and Aims in the Second Punic War." Chap. 16 In *A Companion to the Punic Wars*, edited by Dexter Hoyos, Blackwell Companions to the Ancient World, 280–98. Malden, MA: Wiley-Blackwell, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

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