



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CHALLENGING A GREAT POWER: IRAN'S GRAY ZONE OPERATIONS IN THE MIDDLE EAST

by

Shawn M. Bunting

June 2023

Thesis Advisor:
Second Reader:

Afshon P. Ostovar
Ryan Gingeras

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2023	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE CHALLENGING A GREAT POWER: IRAN'S GRAY ZONE OPERATIONS IN THE MIDDLE EAST			5. FUNDING NUMBERS	
6. AUTHOR(S) Shawn M. Bunting				
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) How effective have Iran's gray zone operations been at advancing its strategic objectives in the Middle East? This thesis analyzed both lethal and nonlethal gray zone operations, including Iranian proxy attacks, drone attacks, weapons testing, missile strikes, maritime attacks, cyber warfare, information operations, and economic coercion. The research found that, between 2017–2022, Iranian gray zone operations effectively advanced Iran's strategic objectives. However, the thesis concludes that Iranian gray zone operations were often ad hoc and a response to unfolding political and military events, rather than proactive in nature. Despite Iran's extensive gray zone operations, the United States and Israel remained the most powerful forces in the Middle East and Iran was unable to become the dominant power in the region.				
14. SUBJECT TERMS gray zone, Iran, asymmetric warfare, proxy forces, ballistic missile, cruise missile, improvised explosive device, IED, unmanned surface vessel, USV, unmanned aerial vehicle, UAV, drones, cyber warfare, information operations, economic coercion, U.S. Navy, U.S. Marine Corps, maximum pressure, Islamic Revolutionary Guards Corps, IRGC, Houthi, Lebanese Hezbollah, Shia Militia			15. NUMBER OF PAGES 103	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**CHALLENGING A GREAT POWER:
IRAN'S GRAY ZONE OPERATIONS IN THE MIDDLE EAST**

Shawn M. Bunting
Major, United States Marine Corps
BS, United States Naval Academy, 2011

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(MIDDLE EAST, SOUTH ASIA, SUB-SAHARAN AFRICA)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2023**

Approved by: Afshon P. Ostovar
Advisor

Ryan Gingeras
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

How effective have Iran's gray zone operations been at advancing its strategic objectives in the Middle East? This thesis analyzed both lethal and nonlethal gray zone operations, including Iranian proxy attacks, drone attacks, weapons testing, missile strikes, maritime attacks, cyber warfare, information operations, and economic coercion. The research found that, between 2017–2022, Iranian gray zone operations effectively advanced Iran's strategic objectives. However, the thesis concludes that Iranian gray zone operations were often ad hoc and a response to unfolding political and military events, rather than proactive in nature. Despite Iran's extensive gray zone operations, the United States and Israel remained the most powerful forces in the Middle East and Iran was unable to become the dominant power in the region.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	MAJOR RESEARCH QUESTION.....	1
B.	SIGNIFICANCE OF THE RESEARCH QUESTION.....	2
C.	LITERATURE REVIEW	3
1.	Defining the Gray Zone.....	3
2.	Gray Zone Actors.....	6
3.	Gray Zone Operations.....	7
4.	Iran’s Strategic Objectives.....	9
5.	Iran’s Asymmetric Warfare Doctrine.....	10
D.	POTENTIAL EXPLANATIONS AND HYPOTHESES	12
E.	RESEARCH DESIGN	13
F.	THESIS OVERVIEW	13
II.	LETHAL PROXY GRAY ZONE OPERATIONS 2017–2022	15
A.	HOUTH OPERATIONS.....	15
B.	IRAQI AND SYRIAN SHIA MILITIA OPERATIONS.....	23
C.	CONCLUSION	32
III.	IRANIAN GRAY ZONE OPERATIONS 2017–2022	35
A.	LETHAL IRANIAN GRAY ZONE OPERATIONS.....	35
B.	NON-LETHAL GRAY ZONE OPERATIONS	45
1.	Cyber Warfare	45
2.	Information Operations.....	51
3.	Economic Coercion	54
4.	Conclusion	57
IV.	IMPACT OF GRAY ZONE OPERATIONS ON IRANIAN STRATEGIC OBJECTIVES	59
A.	REGIME SURVIVAL	59
B.	DETER AGGRESSION	60
C.	PROJECT POWER.....	61
D.	PROTECT THE HOMELAND.....	62
E.	CONCLUSION	63
V.	CONCLUSION	65

A.	SUMMARY OF RESEARCH	65
B.	IMPLICATIONS OF IRANIAN GRAY ZONE OPERATIONS.....	67
1.	Implications for U.S. Counter-Iran Campaigns in the Middle East.....	67
2.	Implications for the U.S. Navy and Marine Corps	68
C.	RECOMMENDATIONS FOR FURTHER RESEARCH	70
	LIST OF REFERENCES.....	71
	INITIAL DISTRIBUTION LIST	89

LIST OF ACRONYMS AND ABBREVIATIONS

AAH	Asa'ib Ahl al-Haq
APT	advanced persistent threat
ASBM	anti-ship ballistic missile
CENTCOM	Central Command
CISA	Cybersecurity and Infrastructure Security Agency
C-RAM	counter-rocket, artillery, mortar
CSIS	Center for Strategic and International Studies
DDoS	distributed denial-of-service
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
FTO	Foreign Terrorist Organization
IC	intelligence community
ICBM	intercontinental ballistic missile
IED	improvised explosive device
IO	information operations
IPO	initial public offering
IRGC	Islamic Revolutionary Guards Corps
IRGCAF	Islamic Revolutionary Guards Corps Aerospace Force
IRGCN	Islamic Revolutionary Guards Corps Navy
IRGC-QF	Islamic Revolutionary Guards Corps Quds Force
IRIB	Islamic Republic of Iran Broadcasting
ISIS	Islamic State of Iraq and Syria
IUVM	International Union of Virtual Media
JCPOA	Joint Comprehensive Plan of Action
KH	Kata'ib Hezbollah
LH	Lebanese Hezbollah

LRBM	long-range ballistic missiles
MEU	Marine Expeditionary Unit
MoI	Ministry of Intelligence
MOOTW	military operations other than war
MRBM	medium-range ballistic missile
MSS	Mission Support Site
NATO	North Atlantic Treaty Organization
NEO	non-combatant evacuation operation
NSI	National Security Innovations
SAM	surface-to-air missile
SLV	satellite launch vehicle
SOCOM	Special Operations Command
SRBM	short-range ballistic missile
THAAD	Terminal High Altitude Area Defense
U.A.E.	United Arab Emirates
U.N.	United Nations
U.S.	United States
UAV	unmanned aerial vehicle
USAGM	United States Agency for Global Media
USV	unmanned surface vessels

ACKNOWLEDGMENTS

I cannot thank my wife, daughter, and family enough for the support and encouragement they provided during this long process. As time passes and the ideas of this thesis become obsolete, their love will endure.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Since 1979, the Islamic Republic of Iran has viewed the United States (U.S.) as its main adversary and source of the Middle East's problems—the United States is the “Great Satan.”¹ The United States and Iran have had a poisoned relationship since Iran's seizure of the U.S. embassy in Tehran and the United States' failed hostage rescue attempt.² Due to this animosity, the United States and Iran have been adversaries in the Middle East ever since. On multiple occasions the United States and Iran have fought each other from attacks on each other's warships to killing troops on the ground.³ Although the United States and Iran have never fought a conventional war, they continue to counter each other in the Middle East. This thesis seeks to further understand this conflict's development since 2017 and Iran's strategic position in the region.

A. MAJOR RESEARCH QUESTION

Iran conducts gray zone operations, operations in the space between peace and open war, to counter the United States and its allies while still avoiding direct conflict. The United States must understand how Iran conducts gray zone operations and its underlying strategy in order to properly counter Iran in the gray zone. This thesis seeks to determine how Iran conducts gray zone operations in the Middle East and analyze their effectiveness at obtaining Iran's strategic objectives since 2017. The research seeks to answer: How effective have been Iran's gray zone operations at advancing its strategic objectives in the Middle East?

¹ Gawdat Bahgat and Anoushiravan Ehteshami, *Defending Iran: From Revolutionary Guards to Ballistic Missiles* (Cambridge, United Kingdom ; New York, NY: Cambridge University Press, 2021), 1.

² Lawrence Freedman, *A Choice of Enemies America Confronts the Middle East* (Public Affairs, 2009), 82–83.

³ David Crist, *The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran* (New York: Penguin Press, 2012), 277–99, 512–37.

B. SIGNIFICANCE OF THE RESEARCH QUESTION

Deterring Iranian aggression and protecting U.S. allies in the Middle East remains a strategic priority for President Joseph Biden and the U.S. government.⁴ The U.S. Intelligence Community (IC) also identifies Iran as a major threat to U.S. interests and assesses Iran will continue to try to erode U.S. influence in the Middle East.⁵ The IC specifically identifies Iran's gray zone operations, such as unconventional warfare, cyberattacks, and proxy forces, as a threat to U.S. interests in the Middle East for the foreseeable future.⁶ The Department of Defense (DOD) also identifies Iran as a persistent threat and gray zone actor in the 2022 National Defense Strategy.⁷ U.S. Central Command (CENTCOM), identifies countering Iran as its first priority and as the "greatest single day-to-day threat to regional security."⁸ This thesis seeks to support the IC and DOD's understanding of the Iranian threat and strategic intentions in the Middle East.

Since 2017, the United States has taken a more aggressive stance against Iran and in 2018 instituted a "maximum pressure campaign," which triggered a significant Iranian response.⁹ Iran sought to respond to U.S. aggression, as well as to U.S. allies, with operations primarily below the threshold of war. The intensity and scope of these gray zone operations have not been seen since Iran's proxy war against U.S. troops in Iraq between 2003–2011.¹⁰ The recent unrest and protests in Iran since September 2022 has also increased the risk of Iranian attacks in order to distract domestic attention and counter

⁴ Joseph Biden, *2022 National Security Strategy* (Washington, DC: The White House, 2022), 11, 18, 42.

⁵ Office of the Director of National Intelligence, "2022 Annual Threat Assessment of the U.S. Intelligence Community" (ODNI), 14–15, accessed June 16, 2022, <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community>.

⁶ Office of the Director of National Intelligence, 14.

⁷ Lloyd Austin, *2022 National Defense Strategy* (Washington, DC: Department of Defense, 2022), 2, 5–6.

⁸ Kenneth F. McKenzie, "CENTCOM Posture Statement," CENTCOM, March 15, 2022, <https://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/>.

⁹ Mohammed Nuruzzaman, "President Trump's 'Maximum Pressure' Campaign and Iran's Endgame," *Strategic Analysis* 44, no. 6 (November 1, 2020): 570–71, <https://doi.org/10.1080/09700161.2020.1841099>.

¹⁰ Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of Its Asymmetric Way of War," *Prism* 9, no. 2 (2021): 86, <https://www.jstor.org/stable/27008977?pq-origsite=summon>.

perceived U.S. interference with Iran’s internal affairs.¹¹ The Iranian regime and security apparatus have directly blamed U.S. intelligence and its allies of inciting violence and sponsoring the recent October 2022 attack on the Shah Cheragh shrine.¹² These recent developments present additional importance for understanding how Iran responds with gray zone operations. By analyzing Iran’s gray zone operations over the last six years and how they have supported Iran’s strategic goals, this thesis will also complement the existing body of gray zone literature and fill the current gap in Iranian gray zone analysis.

C. LITERATURE REVIEW

The objective of this literature review is to understand three things—the nature of gray zone operations, Iran’s strategic goals, and where the two intersect. Because of the nature of the topic, it has not been given much attention in academia. Therefore, the sources under review are mixed, drawn from scholarly books, journal articles, think-tank publications, unclassified U.S. intelligence products, and journalistic reporting. Upon review, the literature can be divided into two main themes, gray zone operations and Iranian grand strategy. Within the gray zone literature emerge three subthemes; definitions or characterizations of the gray zone, gray zone actors, and gray zone operations. Similarly, the Iranian grand strategy literature is divided into two subthemes, Iranian strategic objectives and asymmetric warfare. The gray zone literature and Iran’s grand strategy eventually intersect at Iran’s asymmetric warfare doctrine.

1. Defining the Gray Zone

It is important to discuss the definitional gray zone literature because the definition of the gray zone has evolved since 2015. Furthermore, the DOD’s understanding of gray zone operations also evolved and thus affects how the thesis will analyze gray zone operations. The sudden appearance of gray zone literature in 2015 was likely the result of

¹¹ Dion Nissenbaum, “WSJ News Exclusive | Saudi Arabia, U.S. on High Alert After Warning of Imminent Iranian Attack,” WSJ, accessed December 9, 2022, <https://www.wsj.com/articles/saudi-arabia-u-s-on-high-alert-after-warning-of-imminent-iranian-attack-11667319274>.

¹² Kitaneh Fitzpatrick et al., “Iran Crisis Update, October 28,” Critical Threats, October 28, 2022, <https://www.criticalthreats.org/analysis/iran-crisis-update-october-28>.

the 2014 Russian annexation of Crimea and the Chinese construction of islands in the South China Sea. In particular, it was the testimony of General Joseph L. Votel, commander of Special Operations Command (SOCOM), to the House Armed Services Committee regarding the emergence of these “gray zone approach [es]” that restarts the DOD’s concern for the gray zone.¹³ SOCOM became the progenitor of the initial understanding of the gray zone with its 2015 white paper, “The Gray Zone.” This paper first defined the “gray zone challenges” as the “competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality.”¹⁴ This white paper is a foundational document for the gray zone literature and is often cited by other publications when defining the gray zone. Michael J. Mazarr, a key gray zone thinker from the RAND Corporation, published his analysis of “gray zone strategies” in 2015, which also became a foundational document for subsequent gray zone publications, definitions, and this literature review.¹⁵ The RAND Corp, Center for Strategic and International Studies (CSIS) and the National Security Innovations (NSI) Team also provide definitions for the gray zone which are frequently cited and used by other journal articles.¹⁶ The NSI Team’s definition and discussion was developed specifically for the DOD’s 2016 *Strategic Multi-Layer Assessment Gray Zone Conflicts, Challenges, and Opportunities: A Multi-Agency Deep Dive Assessment*. Despite the increased usage of the gray zone concept by U.S. policy makers and the DOD since 2015, there is still no doctrinal DOD definition for gray zone. For this thesis, RAND’s 2019 definition is used:

¹³ “Statement of General Joseph L. Votel, U.S. Army Commander United States Special Operations Command Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities” (Washington, DC, March 18, 2015).

¹⁴ Philip Kapusta, *The Gray Zone* (MacDill AFB, FL: U.S. Special Operations Command, 2015), 1, <https://info.publicintelligence.net/USSOCOM-GrayZones.pdf>.

¹⁵ Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Advancing Strategic Thought Series (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2015), 1–9, 55–79.

¹⁶ Lyle J. Morris et al., “Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War” (RAND Corporation, June 27, 2019), 8, https://www.rand.org/pubs/research_reports/RR2942.html; Kathleen H. Hicks, John Schaus, and Michael Matлага, *Zone Defense: Countering Competition in the Space between War and Peace* (Washington, DC: Center for Strategic and International Studies, 2018), 2, <https://www.csis.org/features/zone-defense>; George Popp and Sarah Canna, *The Characterization and Conditions of the Gray Zone* (Boston, MA: NSI Team, 2016), 2, https://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViT-Ta-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf.

The gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events.¹⁷

Based on the evolution of the literature this definition best meets the current DOD understanding of the gray zone. As mentioned earlier, Michael Mazarr, who wrote prolifically on the gray zone, was involved in this definition and has continued to use it in more recent gray zone publications for the U.S. Army.¹⁸ This definition is also consistent with how this thesis views the gray zone as a struggle between state actors, which will be discussed later.

The literature, also when discussing gray zone definitions, inconsistently uses other terms such as irregular warfare, unconventional warfare, asymmetric warfare, special warfare, military operations other than war (MOOTW), short-of-war strategies, and hybrid warfare to describe or use as synonyms for the gray zone.¹⁹ Eventually, RAND has sought to distinguish the gray zone from a type of warfare, but as an “analytical concept” where these types of warfare can be used.²⁰ The changing definitions and inconsistent use of terms led to criticisms of the gray zone concept as confusing and even unnecessary.²¹ The critical literature of the gray zone concept consistently points out that these short-of-war

¹⁷ Morris et al., “Gaining Competitive Advantage in the Gray Zone,” 8.

¹⁸ Michael J. Mazarr et al., “What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression” (RAND Corporation, April 19, 2021), 1, https://www.rand.org/pubs/research_reports/RR3142.html.

¹⁹ Mazarr, *Mastering the Gray Zone*, 2; Joseph L. Votel et al., “Unconventional Warfare in the Gray Zone,” *Joint Force Quarterly*, no. 80 (2016): 102–8; Kapusta, *The Gray Zone*, 1; Ronald O’Rourke, *Renewed Great Power Competition: Implications for Defense—Issues for Congress*, R43838 (Washington, DC: Congressional Research Service), 25, accessed July 20, 2022, <https://crsreports.congress.gov/product/details?prodcode=R43838>.

²⁰ Mazarr et al., “What Deters and Why,” 1–10.

²¹ Adam Elkus, “50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense,” *War on the Rocks*, December 15, 2015, <https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/>; Donald Stoker and Craig Whiteside, “Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking,” *Naval War College Review* 73, no. 1 (2020): 14–15, <http://www.jstor.org/stable/26868211>; Megan Price, “Taming the ‘Grey Zone,’” *RealClear Defense*, December 9, 2021, https://www.realcleardefense.com/articles/2021/12/09/taming_the_grey_zone_807104.html.

actions are not historically new and do not need new terminology.²² The harshest critics, professors from the U.S. Naval War College, argued the gray zone concept may lead policy makers to commit an act of war despite thinking they are “fighting in the gray zone.”²³ Despite this criticism, the NSI Team does acknowledge that gray zone actions are not a new phenomenon and that, “the gray zone cannot mean everything if it is to mean anything.”²⁴ The definitional gray zone literature demonstrates that when answering the thesis’ research question it is important to be aware of potential sources confusing or incorrectly characterizing actions as gray zone.

2. Gray Zone Actors

In the same way the gray zone definition evolved over time, the understanding of who conducts gray zone operations has also evolved. The initial gray zone literature, including the SOCOM White Paper, considered gray zone actors as both states and non-state actors.²⁵ The debate on whether to include non-state actors, such as the Islamic State of Iraq and Syria (ISIS), was best captured in the NSI Team’s *The Characterization and Conditions of the Gray Zone*, and became foundational for this thesis’ understanding of who is a gray zone actor.²⁶ However, a more substantial body of literature understands gray zone actors as states, in particular, revisionist states who seek to change the status quo.²⁷ Once again, Mazarr best characterizes gray zone actors as states that are

²² Elkus, “50 Shades of Gray”; Stoker and Whiteside, “Blurred Lines,” 20–25.

²³ Stoker and Whiteside, “Blurred Lines,” 26.

²⁴ Popp and Canna, *The Characterization and Conditions of the Gray Zone*, 6–8.

²⁵ Kapusta, *The Gray Zone*, 2; Ilan Goldenberg et al., *Countering Iran in the Gray Zone* (Washington, DC: Center for New American Security, 2020), 2; James J. Wirtz, “Life in the ‘Gray Zone’: Observations for Contemporary Strategists,” *Defense & Security Analysis* 33, no. 2 (April 3, 2017): 106, <https://doi.org/10.1080/14751798.2017.1310702>.

²⁶ Popp and Canna, *The Characterization and Conditions of the Gray Zone*, 5–7.

²⁷ Morris et al., “Gaining Competitive Advantage in the Gray Zone,” 4, 8, 35; Mazarr, *Mastering the Gray Zone*, act 11; Eisenstadt, “Iran’s Gray Zone Strategy,” 77; Javier Jordan, “International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict,” *Journal of Strategic Security* 14, no. 1 (2020): 1–3, <https://www.jstor.org/stable/26999974>.

“dissatisfied powers” that want to shift the international distributions of power without going to war.²⁸

Javier Jordan’s journal article, “International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict,” was also important to understand the distinction between the non-state actors, such as terrorist groups or proxy forces, engaging in armed conflict with a state and two states competing in the gray zone.²⁹ This article was especially relevant since it used an Iran-Houthi example to illustrate the point that Saudi Arabia and Iran are the gray zone actors while the Houthis are a proxy in armed conflict with Saudi Arabia.³⁰ Jordan distinguishes the two by calling the Saudi-Iranian conflict a “gray zone dyad” and the Saudi-Houthi conflict an “armed conflict dyad.”³¹

Nearly all the literature identifies three major states as gray zone actors: Russia, China, and Iran. All three are characterized by Mazarr as revisionist powers who seek to change the current distribution of power or international system without direct conflict.³² All three operate within the gray zone because of their weaker relative power between themselves and the United States and its allies.³³ After reviewing the literature, this thesis will only consider gray zone competition as between states. The non-state actors are used by states *within* gray zone competition, but not themselves in a gray zone competition with a state.

3. Gray Zone Operations

The literature does not provide a specific list of what constitutes a gray zone operation or activity. Jordan understands a gray zone operation as any coercive action from one state against another that reduces the relative power of the targeted state using means

²⁸ Mazarr, *Mastering the Gray Zone*, 11, 28.

²⁹ Jordan, “International Competition Below the Threshold of War,” 2–3.

³⁰ Jordan, 2.

³¹ Jordan, 19.

³² Mazarr, *Mastering the Gray Zone*, 3–11.

³³ Mazarr, 57; Votel et al., “Unconventional Warfare in the Gray Zone,” 102.

below the threshold of war.³⁴ Specifically, the literature mentions the gray zone actions would not trigger a North Atlantic Treaty Organization (NATO) Article 5 response or United Nations (U.N.) Security Council Resolution.³⁵ The literature consistently uses terms such as ambiguity, salami-slicing, gradualism, and *fait accompli* to describe gray zone operations.³⁶ Gray zone operations can occur in all domains—land, sea, air, information, cyber, and space.³⁷ James Wirtz’s analysis of gray zone activities produced an important observation, “all short-of-war strategies are enabled by the victim’s desire to avoid engaging in hostilities and to not directly take actions that would contribute to this ‘strategic’ defeat (i.e., failure of deterrence).”³⁸ This understanding is important because it will help to determine if a gray zone operation is effective. A gray zone operation must be directed at a victim that is executing a deterrent strategy and views war as a strategic defeat.³⁹ The literature identifies political warfare, proxy warfare, information warfare, economic coercion, cyber warfare, military maneuvers and combinations of each as potential gray zone activities to change the status quo below the threshold of war.⁴⁰ The literature also typically calls the combination of these operations a gray zone campaign.⁴¹ Without a doubt the literature demonstrates gray zone operations can involve a variety of

³⁴ Jordan, “International Competition Below the Threshold of War,” 9.

³⁵ Antulio Echevarria, “How Should We Think about ‘Gray-Zone’ Wars?,” *Infinity Journal* 5, no. 1 (2015): 16, <https://www.militarystrategymagazine.com/article/how-should-we-think-about-gray-zone-wars/>; Votel et al., “Unconventional Warfare in the Gray Zone,” 102.

³⁶ Mazarr, *Mastering the Gray Zone*, 2, 28, 36–37.; Wirtz, “Life in the ‘Gray Zone,’” 106–8; Jordan, “International Competition Below the Threshold of War,” 13–14; O’Rourke, *Renewed Great Power Competition*, 25; Morris et al., “Gaining Competitive Advantage in the Gray Zone,” 9–12; Mazarr et al., “What Deters and Why,” 10; Kapusta, *The Gray Zone*, act 2; Eisenstadt, “Iran’s Gray Zone Strategy,” 78.

³⁷ Eisenstadt, “Iran’s Gray Zone Strategy,” 81.

³⁸ Wirtz, “Life in the ‘Gray Zone,’” 107.

³⁹ Wirtz, 107.

⁴⁰ Goldenberg et al., *Countering Iran in the Gray Zone*, 2; Wirtz, “Life in the ‘Gray Zone,’” 106; Jordan, “International Competition Below the Threshold of War,” 9–13; Melissa G. Dalton, “How Iran’s Hybrid-War Tactics Help and Hurt It,” *Bulletin of the Atomic Scientists* 73, no. 5 (September 3, 2017): 312, <https://doi.org/10.1080/00963402.2017.1362904>; Votel et al., “Unconventional Warfare in the Gray Zone,” act 102; Michael Matlaga, “Case Study: Israel’s Competition with Iran: 1991–2015,” Center for Strategic and International Studies, August 13, 2019, 78, <https://www.csis.org/analysis/case-study-israels-competition-iran-1991-2015>; Popp and Canna, *The Characterization and Conditions of the Gray Zone*, 11; Morris et al., “Gaining Competitive Advantage in the Gray Zone,” xi–xii; Hicks, Schaus, and Matlaga, *Zone Defense: Countering Competition in the Space between War and Peace*, 2.

⁴¹ Mazarr et al., “What Deters and Why,” ix; Mazarr, *Mastering the Gray Zone*, 40, 60.

military and non-military actions in any domain as long as they fall below the threshold of war and seek to coerce an opponent.

4. Iran's Strategic Objectives

The current literature demonstrates Iran's strategic objectives are driven largely by its post-1979 revolutionary ideology—independence from U.S. and foreign influence, anti-monarchical, and Shia Islamist beliefs.⁴² Afshon Ostovar's journal articles and book *Vanguard of the Imam*, are foundational parts of this thesis' understanding of the drivers of Iran's strategic objectives. In particular, *Vanguard of the Imam* details how the current regime was founded and details its key ideology—an Islamic republic ruled by a guardian Shia jurist.⁴³ However, along with this revolutionary ideology Iran's strategic objectives are also driven by pragmatism, self-reliance, and regime interests.⁴⁴ Even with its revolutionary and Shia foundations, the literature describes Iran's decision-making since 1979 as sometimes closer to realpolitik than sectarian.⁴⁵

The literature then describes how these drivers helped form Iran's strategic objectives and behavior. Gawdat Bahgat and Anoushiravan Ehteshami's book *Defending Iran*, provides a clear analysis of Iran's strategic objectives and military capabilities, including sections on gray zone competition, drones, ballistic missiles, cyber, and proxy forces.⁴⁶ Bahgat and Ehteshami detail Iran's first strategic objective—regime survival.⁴⁷ The survival of Iran's unique theocratic system of government is paramount, and viewed by the Iranian regime as necessary not just for Shia Islam, but for the Muslim world.⁴⁸

⁴² Afshon Ostovar, "The Grand Strategy of Militant Clients: Iran's Way of War," *Security Studies* 28, no. 1 (2019): 10, <https://doi.org/10.1080/09636412.2018.1508862>; Ariane M. Tabatabai, *No Conquest, No Defeat: Iran's National Security Strategy* (New York: Oxford University Press, 2020), 298.

⁴³ Afshon Ostovar, *Vanguard of the Imam: Religion, Politics, and Iran's Revolutionary Guards* (New York, NY: Oxford University Press, 2016), 38.

⁴⁴ Bahgat and Ehteshami, *Defending Iran*, 222; Tabatabai, *No Conquest, No Defeat*, 299–300.

⁴⁵ Afshon Ostovar, "Sectarianism and Iranian Foreign Policy," in *Beyond Sunni and Shia*, by Afshon Ostovar (Oxford University Press, 2018), 88, <https://doi.org/10.1093/oso/9780190876050.003.0005>.

⁴⁶ Bahgat and Ehteshami, *Defending Iran*, 1–45, 111–35, 197, 218.

⁴⁷ Bahgat and Ehteshami, 2, 11, 218.

⁴⁸ Bahgat and Ehteshami, 11.

Iran's second objective is to deter aggression from its adversaries—the United States, Saudi Arabia, the United Arab Emirates, and Israel.⁴⁹ This also includes establishing a strategic balance of power against the United States with ties to great powers such as Russia and China.⁵⁰ The literature consistently demonstrates Iran is a revisionist power with its third strategic objective to project power and reassert its leadership in the region.⁵¹ Iran perceives itself as the natural leader in the Middle East, which was denied by meddling foreign powers, such as the British, Russians, and Americans.⁵² This objective in particular will be key in determining the effectiveness of Iran's gray zone strategy since the gray zone is a means for changing the status quo.⁵³ Finally, Iran's fourth main objective is to protect the homeland and its key allies—the Assad regime, Lebanese Hezbollah, Hamas, Iran-backed Iraqi Shia militias, and the Houthis.⁵⁴ Iran views itself in a troubled region, plagued by failed states, hostile terrorist groups, and foreign powers; thus protecting the homeland includes securing its borders, territorial integrity, and sovereignty.⁵⁵

5. Iran's Asymmetric Warfare Doctrine

The final theme within the Iranian grand strategy literature is its asymmetric warfare doctrine. Iran's asymmetric warfare doctrine emphasizes avoiding its adversaries' conventional military advantages while exploiting their weaknesses.⁵⁶ This means Iran prioritizes capabilities such as ballistic missiles, drones, fast attack boats, cyber warfare, and proxy groups.⁵⁷ In addition to *Defending Iran*, the Defense Intelligence Agency's (DIA's) *Iran Military Power* was a key publication for understanding Iran's overall

⁴⁹ Bahgat and Ehteshami, 11–12.

⁵⁰ Bahgat and Ehteshami, 228.

⁵¹ Bahgat and Ehteshami, 218, 220; Eisenstadt, "Iran's Gray Zone Strategy," 78.

⁵² Bahgat and Ehteshami, *Defending Iran*, 220.

⁵³ Eisenstadt, "Iran's Gray Zone Strategy," 77–78.

⁵⁴ Bahgat and Ehteshami, *Defending Iran*, 218; Ostovar, *Vanguard of the Imam*, 205, 217, 219, 223.

⁵⁵ Tabatabai, *No Conquest, No Defeat*, 300.

⁵⁶ Bahgat and Ehteshami, *Defending Iran*, 6–7.

⁵⁷ Bahgat and Ehteshami, 13, 141, 219.

military doctrine and how asymmetric warfare fits into its core military capabilities.⁵⁸ In addition, *Iran Military Power*, has an extensive source list which helped to determine other key authors in the Iranian strategic literature. The literature shows that Iran has used asymmetric warfare to deter its adversaries as well as project power in the Middle East.⁵⁹ For example, Iran's proxies or militant clients, provide Iran with not only offensive capabilities, but the ability to influence regional governments and counter U.S influence.⁶⁰ Although, Iran's allies and proxies are also linked to its objective to project power and influence, they represent a central part of its asymmetric and "forward defense" strategy.⁶¹ Nearly every major report and book on Iran's asymmetric warfare doctrine also mention cyber warfare's role within that doctrine. The most useful publication in understanding Iran's cyber threat and its role in Iran's asymmetric warfare doctrine was the Carnegie Endowment's "Iran's Cyber Threat: Espionage, Sabotage, and Revenge."⁶² As a major pillar of Iran's asymmetric warfare doctrine, Iran has invested significant resources in developing its cyber capabilities since the early 2000s.⁶³ Just as armed proxy groups are a key asymmetric capability for retaliation and deniability, cyber proxies form a major part of Iran's cyber warfare.⁶⁴ Finally, when deterrence fails, the Iranians see asymmetric warfare as their best chance to retaliate, impose high costs, and then reestablish deterrence.⁶⁵

The literature also clearly shows Iran's asymmetric capabilities and warfare doctrine allow it to advance its strategic goals and engage adversaries short of armed

⁵⁸ Robert Ashley, *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance* (Washington, DC: Defense Intelligence Agency, 2019), 22–36.

⁵⁹ Ostovar, *Vanguard of the Imam*, 206; Bahgat and Ehteshami, *Defending Iran*, 232; Ashley, *Iran Military Power*, 22–23.

⁶⁰ Ostovar, "The Grand Strategy of Militant Clients," 7, 11.

⁶¹ Bahgat and Ehteshami, *Defending Iran*, 198, 213.

⁶² Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge" (Carnegie Endowment for International Peace, 2018), 1–3, <http://www.jstor.org/stable/resrep26913>.

⁶³ Bahgat and Ehteshami, *Defending Iran*, 141.

⁶⁴ Catherine A Theohary, *Iranian Offensive Cyberattack Capabilities* (Washington, DC: Congressional Research Service, 2020), 1, <https://crsreports.congress.gov/product/pdf/IF/IF11406/2>.

⁶⁵ Bahgat and Ehteshami, *Defending Iran*, 12; Ashley, *Iran Military Power*, 22.

conflict.⁶⁶ Michael Eisenstadt's, "Iran's Gray Zone Strategy: Cornerstone of its Asymmetric Way of War" was an important article for understanding how Iran's "way of war" is linked to its gray zone operations.⁶⁷ Eisenstadt describes Iran's asymmetric deterrence capabilities as the "linchpin" for Iran's gray zone strategy.⁶⁸ The asymmetric capabilities make war with Iran very costly and thus provide Iran the freedom of action to operate in the gray zone.⁶⁹ The literature shows Iran is a sophisticated gray zone actor which uses a variety of gray zone operations, courtesy of its asymmetric capabilities.⁷⁰ Without a doubt, the literature shows Iran's gray zone operations nest within its asymmetric warfare doctrine, and more broadly its grand strategy.

D. POTENTIAL EXPLANATIONS AND HYPOTHESES

There are three potential hypotheses for the effectiveness of Iran's gray zone operations in advancing its strategic objectives. The first hypothesis is Iranian gray zone operations succeeded in advancing Iran's strategic objectives. More specifically, gray zone operations have enabled Iran to project power in the Middle East and counter the United States and its allies. Evidence of this hypothesis would include Iranian gray zone operations reducing the United States or its allies' ability to act in the Middle East. Furthermore, Iranian gray zone operations would be shown to increase Iran's influence in the region. The second hypothesis is Iran's gray zone operations failed to advance its strategic goals. Evidence of this hypothesis would show that despite the presence of an Iranian gray zone campaign, Iran has no more or less influence in the Middle East. The third and final hypothesis, is Iranian gray zone operations have a negative impact on Iran's strategic objectives. Evidence would include a gray zone operation leading to Iran's influence

⁶⁶ Ashley, *Iran Military Power*, 23; Eisenstadt, "Iran's Gray Zone Strategy," 77.

⁶⁷ Eisenstadt, "Iran's Gray Zone Strategy," 77–83.

⁶⁸ Eisenstadt, 81.

⁶⁹ Eisenstadt, 81.

⁷⁰ Goldenberg et al., *Countering Iran in the Gray Zone*, 2–3; Eisenstadt, "Iran's Gray Zone Strategy," 84–85; Ashley, *Iran Military Power*, 22–23; Dalton, "How Iran's Hybrid-War Tactics Help and Hurt It," 312–14.

decreasing, threatening the survival of the regime, or increasing the United States' or its allies' ability to act in the Middle East.

E. RESEARCH DESIGN

The research design uses a qualitative approach and consists of a literature review, a regional analysis of Iranian gray zone operations, an assessment of their impact on Iran's strategic objectives, conclusion and recommendations for future research. Using the types of gray zone operations identified in the literature review, this thesis will analyze Western and regional news articles, unclassified intelligence reports, journal articles, published interviews, and books to determine what gray zone operations Iran conducted since 2017. This includes discovering the use of Iranian proxy forces, cyber warfare, economic coercion, military operations, and weapons testing as gray zone operations to target the power of the United States and its allies in the Middle East. Once each type of gray zone operation or campaign is identified, the thesis will then assess if the four strategic objectives identified in the literature review were advanced since 2017.

F. THESIS OVERVIEW

The first chapter introduces Iranian gray zone operations, describe their significance to U.S. policy makers, and review the literature. The second chapter analyzes the lethal proxy gray zone operations against the United States and its Middle Eastern allies since 2017. These proxy forces include the Houthis and Iranian-backed Shia militia in Iraq and Syria. The third chapter analyzes direct Iranian lethal gray zone operations and non-lethal gray zone operations against the United States and its Middle Eastern allies since 2017. Non-lethal gray zone operations include Iranian cyber warfare, economic coercion, and information operations. The fourth chapter assesses the gray zone operations' impact on advancing Iran's four strategic goals as identified in the literature review. The fifth chapter summarizes the research findings, provides implications for U.S. policy makers, the U.S. Navy and Marine Corps, and recommendations for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LETHAL PROXY GRAY ZONE OPERATIONS 2017–2022

Gray zone operations conducted by Iran’s proxy forces are the most public and prolific of Iran’s lethal gray zone operations. The Islamic Revolutionary Guards Corps Quds Force (IRGC-QF), is the arm of the IRGC responsible for funding, training, and equipping Iran’s many proxy forces including the Houthis or *Ansar Allah*, Lebanese Hezbollah (LH), Iraqi and Syrian militias.⁷¹ This chapter analyzes the lethal gray zone operations of the IRGC-QF in conjunction with the Houthi, and Iran-backed Shia militias in Iraq and Syria. These groups were the most important of Iran’s proxy forces for lethal gray zone operations from 2017–2022. The current Yemen Civil War is beyond the scope of this thesis and is not analyzed as a part of Iran’s lethal gray zone operations. Only Houthi attacks outside of Yemen are analyzed to determine their effect on Iran’s strategic goals. Although, LH is Iran’s most important and oldest proxy their role was primarily to support the Assad regime in Syria and to act as a trainer and facilitator for Syrian and Iraqi Shia militias—which is already well studied.⁷² In addition, LH did not conduct significant lethal gray zone operations against the United States and its allies during this time and so are not featured in this analysis. The following chapter goes through each year from 2017–2022 of lethal gray zone operations conducted by the Houthis and Iraqi and Syrian Shia militias.

A. HOUTHI OPERATIONS

According to CENTCOM’s 2022 Posture Statement, the Houthis are the, “least restrained and most destabilizing of all of Iran’s affiliates in the region.”⁷³ The Houthis are a key ally of Iran and form an integral part of the “Axis of Resistance” in the last 10 years.⁷⁴ After the 2015 Saudi intervention in the Yemen Civil War, the Houthis became deeply intertwined with Iran’s gray zone operations and began receiving critical Iranian weapon

⁷¹ Ostovar, *Vanguard of the Imam*, 5–6.

⁷² Ostovar, 114–15, 214–17.

⁷³ Mckenzie, “CENTCOM Posture Statement.”

⁷⁴ Katherine Zimmerman, *Yemen’s Houthis and the Expansion of Iran’s Axis of Resistance* (Washington, DC: American Enterprise Institute for Public Policy Research, 2022), 4.

and technical knowledge transfers.⁷⁵ Iranian ballistic missiles, cruise missiles, unmanned aerial vehicles (UAVs), and unmanned surface vessels (USVs) are some of the key weapons provided to the Houthis for lethal gray zone operations.⁷⁶ In addition, the Houthis provide Iran with a crucial geographic foothold in the Arabian Peninsula, which allows them to target Saudi Arabia and the United Arab Emirates while threatening key Red Sea shipping lanes.⁷⁷ The Houthis also have provided Iran with a live-fire testing ground for Iran's drones and missiles, which has enabled Iran to innovate and develop new tactics.⁷⁸ During this period, lethal gray zone operations via the Houthis have provided significant leverage to Iran against the Saudis and Emiratis.

In 2017, the Houthis began the year with three USVs striking a Saudi frigate in the Red Sea, killing at least two sailors on board.⁷⁹ Originally, this attack was viewed as a suicide attack, but were actually remote controlled 33 ft patrol boats laden with explosives likely supplied by Iran.⁸⁰ Also in January 2017, the Houthis launched their new missiles acquired from Iran at the Saudi-Emirati military base on Zuqar Island in the Red Sea killing at least 80 soldiers.⁸¹ Then in June 2017, the Houthis launched Iranian anti-ship missiles at a United Arab Emirates (U.A.E.) naval vessel in the Bab al-Mandeb Strait.⁸² The remainder of the attacks outside of Yemen were primarily directed at Saudi

⁷⁵ Seth G Jones et al., *The Iranian and Houthi War against Saudi Arabia* (Washington, DC: Center for Strategic and International Studies, 2021), 1–3.

⁷⁶ Jeremy Sharp, *Yemen: Civil War and Regional Intervention* (Washington, DC: Congressional Research Service, 2021), 8–10; Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 2; Zimmerman, *Yemen's Houthis and the Expansion of Iran's Axis of Resistance*, 2022, 1.

⁷⁷ Afshon Ostovar, "Deterring Iran: Strategic Behavior and the Maritime Domain," Technical (Monterey, California: Naval Postgraduate School, October 2022), 14; Sharp, *Yemen: Civil War and Regional Intervention*, 10.

⁷⁸ Zimmerman, *Yemen's Houthis and the Expansion of Iran's Axis of Resistance*, 2022, 1.

⁷⁹ H. I. Sutton, "Disguised Explosive Boat May Be New Threat To Tankers Off Yemen," *Forbes*, March 4, 2020, sec. Aerospace & Defense, <https://www.forbes.com/sites/hisutton/2020/03/04/new-disguised-explosive-boat-may-threaten-tankers-off-yemen/>.

⁸⁰ Christopher P. Cavas, "New Houthi Weapon Emerges: A Drone Boat," *Defense News*, February 19, 2017, sec. IDEX, <https://www.defensenews.com/digital-show-dailies/idex/2017/02/19/new-houthi-weapon-emerges-a-drone-boat/>.

⁸¹ Ian Williams and Shaan Shaikh, *The Missile War in Yemen* (Washington, DC: Center for Strategic and International Studies, 2020), 5.

⁸² Williams and Shaikh, 6.

targets using ballistic missiles. The Saudi capital, Riyadh, became a recurring target by short-range ballistic missiles (SRBMs) starting in May 2017.⁸³ However, the July 2017 attack on Saudi Aramco refinery at Yanbu, marked the first reported use of the Burkan 2-H medium-range ballistic missile (MRBM).⁸⁴ The use of the Burkan 2-H is important in this time period because it marks the escalation in sophistication and lethality of Iran's gray zone attacks in Saudi Arabia—particularly because of its range and difficulty of interception by Saudi Patriot missiles.⁸⁵ The Burkan 2-H was used again in attacks in November and December with targets such as the King Khalid International Airport and King Salman's Palace in Riyadh.⁸⁶ The debris recovered from these missiles showed Iranian markings and gave definitive proof of Iran's involvement in escalating gray zone operations against Saudi Arabia, which they continued to deny.⁸⁷ Throughout 2017, Iran used the Houthis to conduct significant attacks against the Saudis and Emiratis while providing the deniability necessary to keep the conflict below the threshold of direct war with Saudi Arabia and its ally, the United States.

Again in 2018, the Houthis increased the complexity of their attacks against Saudi Arabia and the United Arab Emirates by using drones and missiles concurrently.⁸⁸ The Houthis, were used to counter the Trump Administration's "maximum pressure campaign," and respond to the United States' withdrawal from the Joint Comprehensive Plan of Action (JCPOA).⁸⁹ The Houthis employed MRBMs and Iranian designed drones in January, March, April and June against Saudi Ministry of Defense targets and Saudi petroleum

⁸³ Williams and Shaikh, 5.

⁸⁴ Williams and Shaikh, 12.

⁸⁵ Williams and Shaikh, 22.

⁸⁶ John Chapman, ed., *Iran's Networks of Influence in the Middle East* (London, United Kingdom: International Institute for Strategic Studies, 2019), 28.

⁸⁷ Chase Winter, "US Lt. Gen: Yemen's Missiles Have 'Iranian Markings,'" DW News, November 10, 2017, <https://www.dw.com/en/us-air-force-missiles-fired-at-saudi-arabia-from-yemen-have-iranian-markings/a-41333618>.

⁸⁸ Williams and Shaikh, *The Missile War in Yemen*, 6.

⁸⁹ Eisenstadt, "Iran's Gray Zone Strategy," 83, 87–88.

facilities in Jizan, Najran, Khamis Mushait, and most significantly in the capital Riyadh.⁹⁰ Although many missiles were intercepted by Saudi Patriot batteries, at least one person was killed with many others injured due to debris.⁹¹ In July 2018, the Houthis, with help from the IRGC, attacked two Saudi tankers in the Red Sea.⁹² Although the damage was minor, it caused the Saudis to temporarily suspend its oil shipments through the Bab al-Mandeb for ten days—affecting the 500,000-700,000 barrels of oil that are transported through the strait per day.⁹³ Drone attacks continued throughout the year against Saudi Aramco facilities, but more significantly the Houthis used long-range drones against Abu Dhabi International Airport and Dubai International Airport in August and September, respectively.⁹⁴ Although, U.A.E. officials denied these attacks the Houthis later presented videos of the drones striking a truck within one of the terminals—showing the embarrassing nature of Houthi attacks to the Emirati government.⁹⁵ Once again, the IRGC successfully employed the Houthis to strike deeper and disrupt Saudi Arabia and the United Arab Emirates.

Iran's lethal gray zone operations via its Houthi proxies were the most significant in 2019. In April and May, drone attacks began hitting Saudi oil infrastructure, wounding civilians, and damaging oil pumping stations.⁹⁶ May 2019 also saw several SRBMs intercepted over Jeddah and Taif with no reported damage.⁹⁷ In June, the Houthis shot down a U.S. MQ-9 drone with direct help from the IRGC-QF on the ground in Yemen.⁹⁸

⁹⁰ "Iran Missile Milestones: 1985–2022," Iran Watch, June 29, 2022, <https://www.iranwatch.org/our-publications/weapon-program-background-report/iran-missile-milestones-1985-2022>.

⁹¹ "Iran Missile Milestones: 1985–2022."

⁹² Chapman, *Iran's Networks of Influence in the Middle East*, 173.

⁹³ Rania El Gamal, "Saudi Arabia Halts Oil Exports in Red Sea Lane after Houthi Attacks," Reuters, July 25, 2018, <https://www.reuters.com/article/us-yemen-security-idUSKBN1KF0XN>; Williams and Shaikh, *The Missile War in Yemen*, 7.

⁹⁴ Williams and Shaikh, *The Missile War in Yemen*, 8.

⁹⁵ Williams and Shaikh, 8.

⁹⁶ "Timeline: Houthis' Drone and Missile Attacks on Saudi Targets," Al Jazeera, September 14, 2019, <https://www.aljazeera.com/news/2019/9/14/timeline-houthis-drone-and-missile-attacks-on-saudi-targets>.

⁹⁷ "Timeline: Houthis' Drone and Missile Attacks on Saudi Targets."

⁹⁸ "U.S. Blames Iran for Helping Houthi Rebels Shoot down Drone in Yemen," Reuters, June 16, 2019, <https://www.reuters.com/article/us-mideast-attacks-usa-drone-idUSKCN1TH0LA>.

Despite Saudi Patriot batteries intercepting many attacks, cruise missiles successfully hit a power station in Jizan and water desalination plant in Shuqaiq city.⁹⁹ In June and July, the Saudi Abha Airport was hit several times by missiles and drones with at least ten civilians killed and dozens of civilians wounded, including children.¹⁰⁰ August was the most significant month of 2019 due to the escalation in attacks and the introduction of long-range ballistic missiles (LRBMs). The first Burkan-3 missile was fired at a Saudi military site in Dammam, a record 1200 km from Houthi held territory.¹⁰¹ Then in August the Houthis started using drone wave attacks on Saudi airports, airbases, and petroleum facilities with up to ten drones employed at a time.¹⁰² Lastly, ten Badr-1 SRBMs were fired at Jizan airport killing and wounding several civilians.¹⁰³ Although, the Houthis claimed responsibility for the September 2019 complex drone and missile attack on the Saudi Aramco facilities in Abqaiq and Khurais, it was likely the IRGC and so this attack will be discussed in another section.¹⁰⁴ However, this does demonstrate how Iran uses the Houthis to sow confusion and provide it deniability for attacks. The Houthi attacks in 2019 were significant in both their quantity, complexity, and increasing range.

For 2020, Houthi attacks were significantly less than the previous year and the lowest since 2016 due in part to the COVID-19 pandemic and the ceasefire put in place in April to help halt its spread.¹⁰⁵ There were some SRBM, cruise missile, and drone attacks before the ceasefire in March, and then again in June and November when the ceasefire temporarily expired. These attacks, once again, included a wide variety of targets such as

⁹⁹ “Timeline: Houthis’ Drone and Missile Attacks on Saudi Targets.”

¹⁰⁰ “Timeline: Houthis’ Drone and Missile Attacks on Saudi Targets”; “Yemen’s Houthis Attack Saudi’s Abha Airport, Injuring Civilians,” Al Jazeera, July 2, 2019, <https://www.aljazeera.com/news/2019/7/2/yemens-houthis-attack-saudis-abha-airport-injuring-civilians>.

¹⁰¹ Williams and Shaikh, *The Missile War in Yemen*, 44.

¹⁰² “Timeline: Houthis’ Drone and Missile Attacks on Saudi Targets.”

¹⁰³ “Timeline: Houthis’ Drone and Missile Attacks on Saudi Targets.”

¹⁰⁴ Zimmerman, *Yemen’s Houthis and the Expansion of Iran’s Axis of Resistance*, 2022, 2.

¹⁰⁵ Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 10; Ben Hubbard and Saeed Al-Batati, “Saudi Arabia Declares Cease-Fire in Yemen, Citing Fears of Coronavirus,” *The New York Times*, April 8, 2020, sec. World, <https://www.nytimes.com/2020/04/08/world/middleeast/saudi-yemen-ceasefire-coronavirus.html>.

the Saudi MoD in Riyadh, Abha airport, and petroleum facilities in Jeddah and Jizan.¹⁰⁶ However, the interesting development of 2020 was the emerging Houthi tactic of using USVs to target Saudi tankers.¹⁰⁷ Although a USV attack occurred in 2017, the attacks in 2020 were done by larger skiffs, have greater ranges, and can easily be disguised as fishing boats.¹⁰⁸ For example, the attack on the Saudi tanker in March 2020 was 90 miles from the Yemen coast, the longest range attack yet.¹⁰⁹ In November a Houthi USV damaged a Saudi Aramco fueling terminal and tanker in Shuqaiq.¹¹⁰ Lastly in December, a USV struck a Saudi Aramco tanker off the coast of Jeddah, causing significant damage to the vessel and temporarily shutting down the Jeddah port—the most important shipping point for Saudi Arabia.¹¹¹ Although 2020, was a comparatively quiet year for drone and missile attacks, Iran and the Houthis continued to inflict damage to Saudi Arabia on land and at sea.

In 2021, the Houthis conducted 325 cross-border attacks against Saudi Arabia and the United Arab Emirates.¹¹² Compared to the previous year, these attacks had significant impacts against Saudi petroleum infrastructure, airports, military installations and deeply unnerved the Emiratis after high profile attacks against U.A.E bases.¹¹³ The Houthis also continued to lay naval mines in the Red Sea, and launch USVs at Saudi tankers.¹¹⁴ These

¹⁰⁶ Mohammed Benmansour, “Yemen’s Houthis Reach Saudi Capital with Missiles for First Time since COVID Ceasefire,” Reuters, June 23, 2020, <https://www.reuters.com/article/us-yemen-security-saudi-idUSKBN23U0KA>; “Detail of Ansar Allah Missile and Drone Attacks on Saudi Arabia,” Islamic World News, June 23, 2020, <https://english.iswnews.com/13906/detail-of-ansar-allah-missile-and-drone-attacks-on-saudi-arabia/>; “Open-Source Analysis of Iran’s Missile and UAV Capabilities and Proliferation,” International Institute for Strategic Studies, April 2021, <https://www.iiss.org/blogs/research-paper/2021/04/iran-missiles-uavs-proliferation>.

¹⁰⁷ Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 11.

¹⁰⁸ Sutton, “Disguised Explosive Boat May Be New Threat To Tankers Off Yemen.”

¹⁰⁹ Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 11.

¹¹⁰ “Country Reports on Terrorism 2020: Saudi Arabia,” United States Department of State, accessed January 17, 2023, <https://www.state.gov/reports/country-reports-on-terrorism-2020/saudi-arabia/>.

¹¹¹ “‘External Source’ Causes Oil Tanker Blast off Saudi Arabia,” AP News, accessed January 15, 2023, <https://apnews.com/article/dubai-saudi-arabia-united-arab-emirates-jeddah-yemen-5493fe28dab563c4a457a325b20e3c62>.

¹¹² McKenzie, “CENTCOM Posture Statement.”

¹¹³ Zimmerman, *Yemen’s Houthis and the Expansion of Iran’s Axis of Resistance*, 2022, 1.

¹¹⁴ Zimmerman, 10.

USVs were launched as far north as Yanbu, 900 km from Yemeni waters, where the crucial East-West oil pipeline ends for exporting.¹¹⁵ In March, the Houthis conducted a complex attack of drones and missiles against the Saudi Aramco facility in Jizan.¹¹⁶ These types of attacks would continue through September and November against Saudi cities using dozens of drones and missiles, damaging oil facilities and residential areas.¹¹⁷ Also in November, the Houthis stormed the former U.S. embassy in Sanaa, although no U.S. personnel were present, the Houthis did detain the local Yemeni staff of the U.S. embassy.¹¹⁸ In December, many Houthi missiles were intercepted, particularly over Riyadh, but an attack on Jizan managed to kill three civilians and wounding six others.¹¹⁹ The year 2021 showed that despite Western sanctions and a world-wide pandemic, Iran could continue to project power across the Arabian Peninsula. In 2021, Iran successfully provided training and advanced conventional weapons and used the Houthis to conduct almost daily attacks on Saudi Arabia.¹²⁰

January 2022 began with the Houthis hijacking an Emirati flagged ship in the Red Sea and refused to release the vessel despite a statement from the U.N. Security Council demanding its release.¹²¹ The Houthis then launched three major drone and missile attacks on the United Arab Emirates in January. The most complex attack occurred on January 17, using drones, SRBMs, and cruise missiles, the Houthis hit the Abu Dhabi International airport and targeted Al Dhafra Air Base and Dubai.¹²² Although U.A.E. and U.S. THAAD missile defense batteries intercepted the ballistic missiles, the Houthi drones caused

¹¹⁵ “Saudi Arabia Says ‘Booby-Trapped’ Boat Destroyed off Yanbu Port,” Al Jazeera, April 27, 2021, <https://www.aljazeera.com/news/2021/4/27/saudi-arabia-says-it-foiled-boat-attack-off-yanbu-port>.

¹¹⁶ Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 1.

¹¹⁷ Jones et al., 1.

¹¹⁸ Mckenzie, “CENTCOM Posture Statement.”

¹¹⁹ “Saudi Arabia: Houthi Attack Kills 2 in Jizan,” DW News, December 25, 2021, <https://www.dw.com/en/saudi-arabia-houthi-attack-kills-2-in-jizan/a-60254504>; Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 1.

¹²⁰ Mckenzie, “CENTCOM Posture Statement.”

¹²¹ “Yemen’s Houthis Reject UN Call to Free UAE-Flagged Ship,” Al Jazeera, January 16, 2022, <https://www.aljazeera.com/news/2022/1/16/houthis-reject-un-call-to-free-uae-flagged-ship>.

¹²² Jeremy M. Sharp and Carla E Humud, *Attacks Against the United Arab Emirates: Issues for Congress* (Washington, DC: Congressional Research Service, 2022), 2.

substantial damage when it ignited fuel stockpiles at the Abu Dhabi airport.¹²³ The attacks were significant not only due to the proximity of U.S. troops at Al Dhafra, but also the presence of Israel's President Isaac Herzog during the January 31 visit to Abu Dhabi.¹²⁴ These attacks were deeply upsetting to the Emiratis who called for the United States to place the Houthis back on the Foreign Terrorist Organizations (FTO) list.¹²⁵ On March 25, 2022, the Saudi Aramco oil storage facility in Jeddah was hit by several Houthi missiles, causing several large fires to storage tanks, all while threatening the Saudi Arabian Grand Prix held nearby.¹²⁶ In addition, many more Houthi drones and missiles were intercepted over Saudi Arabia likely targeting petroleum facilities in Jizan and Majran that same day.¹²⁷ In April 2022 there was truce between the Saudi coalition and the Houthis which relatively held for the remainder of the year—the first nationwide halt of fighting in the past six years.¹²⁸ For the Houthis, 2022 was a short yet productive year to strike at Saudi Arabia and the United Arab Emirates. Once again, Iran effectively used to the Houthis to threaten Saudi Arabia's and the United Arab Emirates' southern flank with relatively cheap drones and missiles.¹²⁹

¹²³ Sidharth Kaushal, "Lessons from the Houthi Missile Attacks on the UAE," Royal United Services Institute, February 3, 2022, <https://rusi.org/explore-our-research/publications/commentary/lessons-houthi-missile-attacks-uae>.

¹²⁴ Sharp and Humud, *Attacks Against the United Arab Emirates: Issues for Congress*, 2.

¹²⁵ Embassy of the United Arab Emirates, *Returning the Houthis to the U.S. Terrorist List* (Washington, DC: Embassy of the United Arab Emirates, 2022).

¹²⁶ Aziz El Yaakoubi and Maha El Dahan, "Saudi Aramco Petroleum Storage Site Hit by Houthi Attack, Fire Erupts," Reuters, March 26, 2022, <https://www.reuters.com/world/middle-east/saudi-air-defences-destroy-houthi-drones-state-tv-2022-03-25/>.

¹²⁷ Tawfiq Nasrallah, "Video: Saudi-Led Arab Coalition Intercepts Houthi Drones | Saudi – Gulf News," Gulf News, March 25, 2022, <https://gulfnews.com/world/gulf/saudi/video-saudi-led-arab-coalition-intercepts-houthi-drones-1.1648228385136>.

¹²⁸ "Yemen's Warring Sides Agree to Renew Existing Truce: UN," Al Jazeera, August 2, 2022, <https://www.aljazeera.com/news/2022/8/2/yemens-warring-sides-agree-to-renew-existing-truce-un>.

¹²⁹ Kaushal, "Lessons from the Houthi Missile Attacks on the UAE."

B. IRAQI AND SYRIAN SHIA MILITIA OPERATIONS

The IRGC-QF is directly behind the major operations of Iran-backed Shia militias in Iraq and Syria from 2017–2022.¹³⁰ The IRGC-QF, along with LH trainers, developed the most powerful militias in Iraq and Syria such as Kata'ib Hezbollah (KH) and Asa'ib Ahl al-Haq (AAH).¹³¹ The former leader of KH, even publicly thanked LH for training its fighters in Iran for battle in Iraq and Syria.¹³² The IRGC-QF and its proxies formed an Iranian dominated “land bridge” from Tehran to the Mediterranean by controlling key lines of communications from Iraq through Syria and then to Lebanon.¹³³ In 2017, these groups were primarily focused on defeating ISIS in both Iraq and Syria and so did not target the U.S.-led coalition.¹³⁴ This all changed in December 2017 when Iraq's Prime Minister, Haider al-Abadi, declared victory on the war against ISIS—the Iran-backed Shia militias could now target the United States.¹³⁵

The first half of 2018 was not defined by lethal operations, but of increasing hostile rhetoric between the United States and Iran—especially due to the start of the Trump Administration's “maximum pressure campaign” in May 2018.¹³⁶ Although, in February 2018, hundreds of pro-Syrian Regime forces and Russian paramilitary mercenaries attacked U.S. forces at Mission Support Site (MSS) Conoco in eastern Syria.¹³⁷ This intense battle will not be considered an Iranian gray zone action since it was likely Russian-

¹³⁰ Goldenberg et al., *Countering Iran in the Gray Zone*, 4.

¹³¹ “Mapping Militants Profiles: Kata'ib Hezbollah,” Stanford University, September 2020, <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/kataib-hezbollah>; “Mapping Militants Profiles: Asa'ib Ahl al-Haq,” Stanford University, July 2018, <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/asaib-ahl-al-haq>.

¹³² Garrett Nada and Mattisan Rowan, “Part 2: Pro-Iran Militias in Iraq,” Wilson Center, April 27, 2018, <https://www.wilsoncenter.org/article/part-2-pro-iran-militias-iraq>.

¹³³ Goldenberg et al., *Countering Iran in the Gray Zone*, 5.

¹³⁴ Sarhang Hamasaeed and Garrett Nada, “Iraq Timeline: Since the 2003 War,” United States Institute of Peace, May 29, 2020, <https://www.usip.org/iraq-timeline-2003-war>.

¹³⁵ Hamasaeed and Nada.

¹³⁶ Eisenstadt, “Iran's Gray Zone Strategy,” 87–88.

¹³⁷ Thomas Gibbons-Neff, “How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria,” New York Times (Online) (New York, United States: New York Times Company, May 24, 2018), <https://www.proquest.com/docview/2043078446/abstract/6F29F96A83D84254PQ/1>.

led and most of the forces were from the Russian Wagner Group despite denials from the Kremlin.¹³⁸ However, September 2018 saw the first Katyusha rocket attacks, supplied by Iran, fired on the U.S. consulate in Basra, Iraq.¹³⁹ The U.S. Embassy in Baghdad was also hit by rocket and mortar attacks in the same week, in coordination with the IRGC-QF and other Shia militias.¹⁴⁰ Due to the danger of further attacks from Iraqi Shia militias, U.S. Secretary of State Mike Pompeo ordered the evacuation of U.S. personnel from the consulate in Basra.¹⁴¹ With just a few attacks in 2018, the IRGC-QF and Shia militias perceived the United States as risk averse, which then encourage the large increase of attacks in 2019.

The beginning of 2019 was quiet and saw no major lethal gray zone operations in Iraq or Syria. Then in May 2019, Iraqi Shia militias in southern Iraq launched drone attacks for the first time against Saudi Arabia at oil pumping stations in al-Daudmi.¹⁴² The drone attack caused only caused minor damage, but made Saudi Aramco temporarily shut down its East-West pipeline.¹⁴³ The Saudis had limited missile and drone defenses oriented toward southern Iraq and so it provided Iran another vector to strike at Saudi Arabia.¹⁴⁴ Iraqi Shia militias' rocket attacks against U.S. targets also resumed in May 2019. First, the Green Zone, where the U.S. embassy is located, was targeted by rockets and caused the U.S. State Department to evacuate nonessential personnel from the Baghdad embassy and consulate in Erbil.¹⁴⁵ Further rocket attacks occurred against Camp Taji, where a U.S.-

¹³⁸ Gibbons-Neff.

¹³⁹ Hamasaeed and Nada, "Iraq Timeline."

¹⁴⁰ "U.S. Closes Consulate in Southern Iraq, Blames Iran," The Iran Primer, September 10, 2018, <https://iranprimer.usip.org/blog/2018/oct/03/us-closes-consulate-southern-iraq-blames-iran>.

¹⁴¹ "U.S. Closes Consulate in Southern Iraq, Blames Iran."

¹⁴² Isabel Coles and Dion Nissenbaum, "U.S.: Saudi Pipeline Attacks Originated From Iraq," *Wall Street Journal*, June 28, 2019, sec. World, <https://www.wsj.com/articles/u-s-saudi-pipeline-attacks-originated-from-iraq-11561741133>.

¹⁴³ Coles and Nissenbaum.

¹⁴⁴ Coles and Nissenbaum.

¹⁴⁵ Hamasaeed and Nada, "Iraq Timeline"; Laurel Wamsley, "State Department Orders Nonessential U.S. Government Employees Out Of Iraq," National Public Radio, May 15, 2019, <https://www.npr.org/2019/05/15/723466550/state-department-orders-non-emergency-u-s-government-employees-out-of-iraq>.

coalition training facility was located.¹⁴⁶ This attack was likely in response to U.S. efforts in northern Iraq to negotiate the removal of non-local militias—meaning the Iran-backed Shia militias would lose influence in the area.¹⁴⁷ These types of attacks continued in June 2019, with more rocket and mortar attacks on U.S. training facilities at Camp Taji, a U.S. facility near Mosul, and Balad Air Base.¹⁴⁸ It was speculated the rocket attack on U.S. owned oil facilities in Basra was meant to hamper U.S. energy initiatives in Iraq and interfere with a proposed Exxon Mobil deal in June 2019.¹⁴⁹ The pattern continued in September, October, and November with rocket and mortar attacks on the Green Zone, Balad Air Base, Mosul and Camp Taji with one American wounded.¹⁵⁰ December 2019, had the most rocket attacks for the year and became deadliest month for the United States. KH was instrumental in leading the December 27 rocket attack on a U.S. base in Kirkuk that killed three U.S. servicemembers and one contractor.¹⁵¹ This prompted a swift U.S. response with strikes against KH facilities in Iraq and Syria killing at least 20 KH fighters.¹⁵² A few days later KH, along with other Shia militias, would organize a siege on the U.S. Embassy in Baghdad in response to the U.S. strikes on KH facilities in Iraq and Syria.¹⁵³ The U.S. Embassy compound was broken into and the reception area was set on fire until Iraqi security forces stopped further escalation.¹⁵⁴ Key leaders from Iraqi Shia

¹⁴⁶ Michael Knights, “Iran-Backed Militias Test the Credibility of Iraq’s Prime Minister,” The Washington Institute, accessed January 24, 2023, <https://www.washingtoninstitute.org/policy-analysis/iran-backed-militias-test-credibility-iraqs-prime-minister>.

¹⁴⁷ Knights.

¹⁴⁸ “Flashpoints: Iraq,” International Crisis Group, December 14, 2017, <https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/iraq>.

¹⁴⁹ Knights, “Iran-Backed Militias Test the Credibility of Iraq’s Prime Minister.”

¹⁵⁰ Behnam Taleblu, “Collecting and Analyzing Shiite Militia Attacks against the U.S. Presence in Iraq,” Foundation for Defense of Democracies Long War Journal, May 5, 2020, <https://www.longwarjournal.org/archives/2020/05/collecting-and-analyzing-shiite-militia-attacks-against-the-u-s-presence-in-iraq.php>; “Flashpoints: Iraq.”

¹⁵¹ Hamasaeed and Nada, “Iraq Timeline.”

¹⁵² Hamasaeed and Nada.

¹⁵³ Hamasaeed and Nada.

¹⁵⁴ “Protesters Attack U.S. Embassy in Baghdad after Airstrikes,” AP News, April 20, 2021, <https://apnews.com/article/us-news-ap-top-news-mark-esper-international-news-north-carolina-75228a8a607a44863b57021ac33264dc>.

militias, including KH and AAH, were present outside the U.S. Embassy during the protest and attack.¹⁵⁵ The December 2019 attacks would be catalyst for the very strong U.S. response to the IRGC-QF and KH in 2020.

On January 3, 2020, a U.S. drone strike killed Qasem Soleimani and Abu Mahdi al-Muhandis, the IRGC-QF and KH commanders, respectively.¹⁵⁶ The Iraqi Shia militias were an essential part of Iran's response, which began the next day with rockets and mortars hitting Balad Airbase and in the Green Zone.¹⁵⁷ In conjunction with Iran's January 8th ballistic missile strike against the U.S. forces in Iraq, Shia militias conducted mortar and rocket attacks against an American facility nearly every day—Camp Taji, Balad Air Base, and the Green Zone were the primary targets.¹⁵⁸ Despite the frequency of these attacks, only one American was injured in January.¹⁵⁹ Comparatively, February 2020 had relatively few attacks with only two days of rocket attacks on K-1 Air Base in Kirkuk and the Green Zone.¹⁶⁰ Unfortunately, attacks would surge in March 2020 which would become the deadliest month of the year. On March 11, KH would launch its largest rocket barrage yet with over 30 Katyusha rockets fired at Camp Taji, killing two U.S. and one British soldier and injuring 14 others.¹⁶¹ A few days later, KH would launch 25 more rockets at Camp Taji, injuring three more U.S. soldiers.¹⁶² Despite U.S. retaliatory strikes, rocket attacks would continue throughout the month, but mainly targeting the Green Zone.¹⁶³ In April 2020, KH issued a ceasefire on U.S. forces.¹⁶⁴ However, there were sporadic rocket attacks against U.S. energy facilities at Basra and U.S. facilities at the

¹⁵⁵ “Protesters Attack U.S. Embassy in Baghdad after Airstrikes.”

¹⁵⁶ Eisenstadt, “Iran’s Gray Zone Strategy,” 88.

¹⁵⁷ Taleblu, “Collecting and Analyzing Shiite Militia Attacks against the U.S. Presence in Iraq.”

¹⁵⁸ Taleblu.

¹⁵⁹ Taleblu.

¹⁶⁰ Taleblu.

¹⁶¹ Hamasaeed and Nada, “Iraq Timeline.”

¹⁶² Hamasaeed and Nada.

¹⁶³ Taleblu, “Collecting and Analyzing Shiite Militia Attacks against the U.S. Presence in Iraq.”

¹⁶⁴ “Flashpoints: Iraq.”

Baghdad International Airport and Green Zone in April and May 2020. KH and AAH would ramp up rocket attacks on U.S. facilities in Baghdad and Camp Taji in June 2020.¹⁶⁵ It is no accident the increased attacks occurred during and after the Strategic Dialogue between the U.S. and Iraqi governments in June. This meeting was in part to determine the status of remaining U.S. forces.¹⁶⁶ July 2020, would be another month of weekly rocket attacks against U.S. facilities in the Green Zone, Baghdad International Airport, Camp Taji, and Besmaya military base.¹⁶⁷ According to CENTCOM, these attacks were attributed to Iran's proxies and likely due to the U.S. forces remaining in Iraq at the request of the Iraqi government.¹⁶⁸

The Iraqi Shia militias would shift tactics in August 2020, and begin targeting logistics convoys destined for U.S.-coalition facilities with roadside bombs or improvised explosive devices (IEDs).¹⁶⁹ Rocket attacks would also continue against the Green Zone, Camp Taji, Baghdad International Airport, in addition to the roadside IEDs.¹⁷⁰ Throughout September and early October 2020, Iraqi Shia militias conducted weekly roadside bomb attacks against U.S.-led coalition convoys, but with no U.S. casualties.¹⁷¹ Rocket attacks, mainly small barrages, against U.S. facilities at Erbil International Airport, Baghdad International Airport, and the Green Zone were also weekly occurrences during this time.¹⁷² However, on October 10, the Coordinating Body of Iraqi Resistance, an array of Shia militias which include KH and AAH, ordered a truce toward American forces and persuaded its factions to “stop the bombing operations until the end of the American

¹⁶⁵ “Flashpoints: Iraq.”

¹⁶⁶ “Flashpoints: Iraq.”

¹⁶⁷ “Flashpoints: Iraq.”

¹⁶⁸ Carla Babb, “VOA Exclusive: CENTCOM Chief Says U.S. Can Do Job in Iraq with Fewer Forces,” VOA, July 15, 2020, https://www.voanews.com/a/middle-east_voa-exclusive-centcom-chief-says-us-can-do-job-iraq-fewer-forces/6192870.html.

¹⁶⁹ “Iraq: IED Attack Hits Logistical Convoy in Taji August 11,” Crisis24, August 11, 2020, <https://crisis24.garda.com/alerts/2020/08/iraq-ied-attack-hits-logistical-convoy-in-taji-august-11>.

¹⁷⁰ “Flashpoints: Iraq.”

¹⁷¹ “Flashpoints: Iraq.”

¹⁷² “Flashpoints: Iraq.”

election.”¹⁷³ The KH spokesman specifically said the cessation of hostilities was only for two months to allow the U.S. forces to withdraw from Iraq and attacks would resume if they did not.¹⁷⁴ With the exception of one rocket attack near the U.S. Embassy in November 2020, the truce would hold until mid-December.¹⁷⁵ As the one-year anniversary of Soleimani’s death approached, roadside IEDs resumed hitting U.S.-led coalition convoys and large rocket attacks were launched with some salvos containing as many as 20 rockets.¹⁷⁶ Overall, 2020 saw a major increase in lethal gray zone attacks by Iraqi Shia militias and was the most effective way for Iran to kill or injure U.S. personnel while avoiding direct conflict.

In 2021, the lethal gray zone attacks in Iraq began to include Iranian-made drones, as well expand to U.S. bases in eastern Syria. From 2017–2020 there was no significant reporting of major attacks by Iran-backed Shia militia on U.S. bases in Syrian-opposition held territory, likely due to the IRGC-QF prioritizing counter-ISIS missions. This would change in 2021 as Iran supplied more sophisticated drones to its proxies in Iraq.¹⁷⁷ By 2021, Iran had supplied KH with significant drone capabilities which they used to target the Yamamah Palace in Riyadh for the first time in January.¹⁷⁸ This attack demonstrated for the first time the capability for KH to strike targets at least 950 km away.¹⁷⁹ Rocket attacks also continued in January and February 2021 against Baghdad International Airport, Erbil and Balad Air Base, which injured six Americans, including a U.S. servicemember.¹⁸⁰ In March and April rocket attacks on Al Asad, Balad, and Erbil,

¹⁷³ “Iran-Backed Militias Offer Truce for U.S. Pullout from Iraq,” AP News, April 26, 2021, <https://apnews.com/article/iran-us-news-baghdad-middle-east-iraq-f12d77bec74acefc7c4883eb30d832eb>.

¹⁷⁴ “Iran-Backed Militias Offer Truce for U.S. Pullout from Iraq.”

¹⁷⁵ “Rockets Hit near U.S. Embassy in Iraq as Tensions Flare,” France 24 News, December 20, 2020, <https://www.france24.com/en/live-news/20201220-rockets-hit-near-us-embassy-in-iraq-as-tensions-flare>.

¹⁷⁶ “Rockets Hit near U.S. Embassy in Iraq as Tensions Flare”; “Flashpoints: Iraq.”

¹⁷⁷ Michael Knights and Crispin Smith, “Kataib Hezbollah Leads Drone Warfare Inside Iraq,” The Washington Institute, May 14, 2021, <https://www.washingtoninstitute.org/policy-analysis/kataib-hezbollah-leads-drone-warfare-inside-iraq>.

¹⁷⁸ Knights and Smith.

¹⁷⁹ Knights and Smith.

¹⁸⁰ “Flashpoints: Iraq.”

continued to increase, particularly in the once protected areas of the Kurdistan Region of Iraq.¹⁸¹ Most significantly, the April 2021 drone attack on Erbil International Airport was the first major drone attack against U.S. forces in Kurdistan, which caused a large fire and damaged a building.¹⁸² In May and June, rockets hit Baghdad International Airport, Balad, and Al Asad Air Base.¹⁸³ June 2021, also saw the largest rocket attacks on U.S. bases in eastern Syria.¹⁸⁴ In particular, the June 28 rocket attack used 34 large caliber rockets on MSS Green Village near Deir al-Zour.¹⁸⁵ Once again, Iranian-made drone attacks would have the greatest effect and damaged buildings in Al Asad, Erbil, and Baghdad International Airport.¹⁸⁶ In July 2021, weekly rocket and drone attacks would continue across Iraq and eastern Syria against U.S. forces.¹⁸⁷ The July attacks in eastern Syria would increase in their geographic scope to include U.S. bases near al-Shadadi, al-Omar oilfields, and Conoco oilfields.¹⁸⁸ Iranian-made rocket and drone attacks in Iraq and eastern Syria would peak in August, but no significant damage or injuries were reportedly done to U.S.

¹⁸¹ Katherine Lawlor and Nicholas Carl, “Iran File: Iranian Proxies Increase Attacks on U.S. Forces to Catalyze a U.S. Withdrawal from Iraq,” Critical Threats, July 9, 2021, <https://www.criticalthreats.org/briefs/iran-file/iranian-proxies-increase-attacks-on-us-forces-to-catalyze-a-us-withdrawal-from-iraq>; “DOD Statement on Rocket Attack at Al Asad by Pentagon Press Secretary John F. Kirby,” U.S. Department of Defense, accessed January 25, 2023, <https://www.defense.gov/News/Releases/Release/Article/2522600/dod-statement-on-rocket-attack-at-al-asad-by-pentagon-press-secretary-john-f-ki/><https://www.defense.gov/News/Releases/Release/Article/2522600/dod-statement-on-rocket-attack-at-al-asad-by-pentagon-press-secretary-john-f-ki/>; “Flashpoints: Iraq.”

¹⁸² “US Commander Says More Work Needed to Counter Small Drones,” AP News, May 22, 2021, <https://apnews.com/article/donald-trump-middle-east-government-and-politics-e39fb650c283cc6e3962752e1d9e339b>.

¹⁸³ “Flashpoints: Iraq.”

¹⁸⁴ Crispin Smith and Hamdi Malik, “The Muqawama Are Focusing Attack Claims on U.S. Bases in Syria,” The Washington Institute, accessed January 26, 2023, <https://www.washingtoninstitute.org/policy-analysis/muqawama-are-focusing-attack-claims-us-bases-syria>.

¹⁸⁵ Lawlor and Carl, “Iran File.”

¹⁸⁶ “Flashpoints: Iraq.”

¹⁸⁷ “Flashpoints: Iraq”; “Flashpoints: Middle Euphrates River Valley, Syria,” International Crisis Group, December 14, 2017, <https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/middle-euphrates-river-valley>.

¹⁸⁸ Lawlor and Carl, “Iran File”; Smith and Malik, “The Muqawama Are Focusing Attack Claims on U.S. Bases in Syria.”

forces.¹⁸⁹ September 2021, only saw a few drone attacks in Iraq and eastern Syria with the most prominent one on September 11 in Erbil.¹⁹⁰ The prominent Iraqi Shia militia media outlet, Sabereen News, claimed the attack was because, “we just wanted to remind the Americans of the Sep. 11 attacks in our own way.”¹⁹¹ October 2021 saw a few rocket attacks on the Green Zone in Iraq, but one large combined drone and rocket attack on the U.S. base in at-Tanf, Syria.¹⁹² Rocket attacks in Iraq would ramp up again in late November and December in advance of the declared end of the U.S. combat mission in Iraq on December 31, 2021.¹⁹³ However, in only one attack was damage reported to vehicles in the Green Zone.¹⁹⁴ Overall, Iran used its Syrian and Iraqi proxies aggressively throughout 2021 to pressure the Biden Administration to withdrawal troops from Iraq. As the attacks peaked against U.S. forces in August, Iran began shifting its use of proxies to Turkish and Kurdish targets in northern Iraq, which explains the decrease in attacks against the U.S. forces toward the end of 2021.¹⁹⁵

The attacks against U.S. forces began almost immediately in January 2022, after the December 31, 2021 Shia militias’ ultimatum for the United States to withdraw forces from Iraq went by without any U.S. withdrawal.¹⁹⁶ Primarily KH and AAH with other Shia militias launched weekly rocket, mortar, and drone attacks on Baghdad International

¹⁸⁹ Eric Feely, “Militias Pivot Away from U.S. Targets, Toward Kurdistan and Turkish Bases,” The Washington Institute, October 17, 2022, <https://www.washingtoninstitute.org/policy-analysis/militias-pivot-away-us-targets-toward-kurdistan-and-turkish-bases>; Michael Knights, Crispin Smith, and Hamdi Malik, “Iran’s Proxies in Iraq Undertake the World’s Only Terrorist Attack Commemorating 9/11,” The Washington Institute, accessed January 26, 2023, <https://www.washingtoninstitute.org/policy-analysis/irans-proxies-iraq-undertake-worlds-only-terrorist-attack-commemorating-911>.

¹⁹⁰ Knights, Smith, and Malik, “Iran’s Proxies in Iraq Undertake the World’s Only Terrorist Attack Commemorating 9/11.”

¹⁹¹ Knights, Smith, and Malik.

¹⁹² “Flashpoints: Iraq”; Crispin Smith, “Militia Propaganda Around the Attack on Al-Tanf,” The Washington Institute, October 22, 2021, <https://www.washingtoninstitute.org/policy-analysis/militia-propaganda-around-attack-al-tanf>.

¹⁹³ Feely, “Militias Pivot Away from U.S. Targets, Toward Kurdistan and Turkish Bases.”

¹⁹⁴ “Flashpoints: Iraq.”

¹⁹⁵ Feely, “Militias Pivot Away from U.S. Targets, Toward Kurdistan and Turkish Bases.”

¹⁹⁶ Michael Knights and Crispin Smith, “Making Sense of Militia Attacks in Iraq and Syria in Early 2022,” The Washington Institute, January 6, 2022, <https://www.washingtoninstitute.org/policy-analysis/making-sense-militia-attacks-iraq-and-syria-early-2022>.

Airport, Al Asad, Balad, the Green Zone, and U.S. bases in eastern Syria.¹⁹⁷ Despite the intensity of the attacks only a few casualties were reported after a rocket attack on the U.S. embassy in Baghdad.¹⁹⁸ February 2022 was quiet within Iraq and Syria, but KH still launched three drones against the United Arab Emirates, a first for Iraqi Shia militias.¹⁹⁹ This drone attack was coordinated with other drone and missile attacks launched by the Houthis during the same period.²⁰⁰ March through July 2022, was also relatively quiet with sporadic rocket and drone attacks on U.S. facilities at Balad, al-Asad, and Erbil Airbases.²⁰¹ This lull in attacks can be attributed to renewed nuclear negotiations between Iran and the Biden Administration.²⁰² August and September 2022 saw renewed drone, rocket, and mortar strikes against the U.S. base in at-Tanf, MSS Conoco, and MSS Green Village, while only rocket attacks on Bagdad International Airport.²⁰³ At least three U.S. servicemembers were injured in the August eastern Syria attacks.²⁰⁴ Importantly, the drones from the August at-Tanf attack were launched from the same KH compound that also likely launched the attacks against Saudi Arabia and the United Arab Emirates.²⁰⁵ October through December 2022 were the quietest months of the year with minimal rocket

¹⁹⁷ “Flashpoints: Iraq”; Knights and Smith, “Making Sense of Militia Attacks in Iraq and Syria in Early 2022.”

¹⁹⁸ “Flashpoints: Iraq.”

¹⁹⁹ Seth J. Frantzman, “Five Times Iran Used Iraqi Militias to Conduct Drone Attacks – Analysis,” *The Jerusalem Post*, February 4, 2022, <https://www.jpost.com/middle-east/iran-news/article-695541>.

²⁰⁰ Sharp and Humud, *Attacks Against the United Arab Emirates: Issues for Congress*, 1–2.

²⁰¹ “Flashpoints: Iraq.”

²⁰² Cameron Abadi, “Iran’s Revolutionary Year,” *Foreign Policy* (blog), December 25, 2022, <https://foreignpolicy.com/2022/12/25/iran-protest-revolution-2022-raisi-irgc/>.

²⁰³ “Flashpoints: Middle Euphrates River Valley, Syria.”

²⁰⁴ “CENTCOM Forces Respond to Attempted Coordinated Rocket Attacks at Conoco, Green Village Ba,” U.S. Central Command, accessed October 20, 2022, <https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/3138816/centcom-forces-respond-to-attempted-coordinated-rocket-attacks-at-conoco-green/https%3A%2F%2Fwww.centcom.mil%2FMEDIA%2FPRESS-RELEASES%2FPress-Release-View%2FArticle%2F3138816%2Fcentcom-forces-respond-to-attempted-coordinated-rocket-attacks-at-conoco-green%2F>.

²⁰⁵ Michael Knights, “Kataib Hezbollah’s Role in the August 15 al-Tanf Attack,” The Washington Institute, August 25, 2022, <https://www.washingtoninstitute.org/policy-analysis/kataib-hezbollahs-role-august-15-al-tanf-attack>.

attacks on U.S. bases in eastern Syria and only one rocket attack on the Green Zone.²⁰⁶ This lull also corresponded to the major “Women, Life, Freedom” protest movement across Iran, which began in September after the death of 22-year-old Mahsa Amini at the hands of the Iranian regime’s morality police.²⁰⁷ Although, 2022 lethal proxy operations were not as prolific in as in previous years, they demonstrated an increasing geographic scope and capability. The decrease in attacks were not due to Iran losing capability to project power, but rather due to ongoing political events.

C. CONCLUSION

For the Houthis and Iran-backed Shia militias in Iraq and Syria, the proliferation of sophisticated Iranian weapons dramatically increased the lethality, complexity, and geographic scope of lethal gray zone operations. From 2017–2022, Iran, through its proxies, was able to target its adversaries’ critical economic infrastructure, military bases, embassies, government buildings, and key shipping lanes, while avoiding direct conflict. By 2022, there was no place in the Arabian Peninsula, Levant, Red Sea, and Persian Gulf where the U.S. and its allies could not be targeted by Iran’s proxies. Whether it is long-range drones with demonstrated ranges of 950 km, LRBMs with ranges of 1200 km, or USVs with ranges over 300 km, Iran can project power throughout the Middle East.²⁰⁸ After 2017, Iran-backed Shia militia also effectively employed hundreds of simpler weapons such as rockets, mortars, and roadside IEDs to attack and kill U.S. troops, contractors, and its allies in Iraq and Syria.

By analyzing the attacks month by month, it becomes clear the attacks often ebbed and flowed due to political considerations within Yemen, Iraq, Syria, and Iran. Iran was clearly using its proxies to respond to political and military events as they occurred—in an ad hoc approach. Although many of the attacks were reactionary, there were instances

²⁰⁶ “Flashpoints: Middle Euphrates River Valley, Syria”; “Flashpoints: Iraq.”

²⁰⁷ Abadi, “Iran’s Revolutionary Year.”

²⁰⁸ Knights and Smith, “Kataib Hezbollah Leads Drone Warfare Inside Iraq”; Williams and Shaikh, *The Missile War in Yemen*, 44; Tamir Eshel, “Houthi’s New Naval Weapons Extend Their Reach 200 Nm into the Gulf of Aden,” *Defense Update*: (blog), September 26, 2022, https://defense-update.com/20220926_houthis-naval-weapons.html.

where Iran did have a defined campaign to pressure the Saudis, Emirates, or American governments to make political decisions, such as evacuating embassies or agreeing to ceasefires. However, Iran did not cause the Saudi-led coalition to leave Yemen or the United States to withdraw from Syria and Iraq using lethal gray zone operations. It is also important to mention that although many of Iran's gray zone responses were ad hoc and evolved with events, they had the strategic foresight to train and equip their proxies to give them the ability to respond. Finally, an analysis of attacks also shows that the IRGC-QF has the capability to coordinate attacks between the Houthis and Iraqi Shia militias—demonstrated by the 2022 attacks on the United Arab Emirates. This type of coordination means that Iran can conduct multi-axis and multi-domain lethal gray zone operations. Clearly, from 2017–2022 Iran was able to use proxy attacks below the threshold of war to project power and improve its strategic position in the Middle East.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IRANIAN GRAY ZONE OPERATIONS 2017–2022

This chapter analyzes the lethal and non-lethal gray zone operations directly conducted by Iranian actors and not its proxies. Iran’s IRGC and regular military, called the *Artesh*, both conducted lethal gray zone operations, but the IRGC remained the primary actor for Iran.²⁰⁹ Not only is the IRGC responsible for proxy forces, but it is also responsible for Iran’s missile forces and testing.²¹⁰ The first part of the chapter analyzes Iran’s lethal gray zone operations which consisted of offensive weapons testing and maritime, drone, and missile attacks. This section goes through each attack and weapons test by year from 2017–2022. These lethal operations remained below the threshold of war but sought to use violence or intimidation to coerce the United States and its allies. The second part of the chapter analyzes Iran’s significant non-lethal gray zone operations including cyber warfare, information operations, and economic coercion. It is important to remember these gray zone operations were conducted concurrently and in concert with the gray zone operations from the previous chapter.

A. LETHAL IRANIAN GRAY ZONE OPERATIONS

In 2017 Iran conducted no significant gray zone attacks against the United States or its allies, which corresponds with Iran’s focus on defeating ISIS in Iraq and Syria as previously discussed. However, Iran did significant weapons testing throughout the year. In January, February, and March Iran conducted new ballistic and cruise missile tests, with the most conducted during the “Defenders of Velayat Skies” annual exercise.²¹¹ According to U.S. defense officials, the new Khorramshar MRBM reportedly had a 1000 km range and greater payload than in previous MRBMs.²¹² The most significant of these tests was the Hormuz-2 anti-ship ballistic missile (ASBM) in March 2017, which reportedly struck

²⁰⁹ Ashley, *Iran Military Power*, 25.

²¹⁰ Ashley, 27.

²¹¹ “Iran Missile Milestones: 1985–2022.”

²¹² “Iran Missile Milestones: 1985–2022.”

floating targets over 300 km away.²¹³ These tests occurred concurrently with several unsafe IRGC Navy (IRGCN) interactions with U.S. Navy in the Persian Gulf.²¹⁴ The beginning of 2017 also saw increasing hostile rhetoric and new sanctions placed on Iran's ballistic missile program by the Trump Administration.²¹⁵ The rest of 2017 saw less tests with a Simorgh satellite launch vehicle (SLV), Iran's most advanced satellite carrying rocket, and another Khorramshar missile test in September with a reported range increase to 2000 km.²¹⁶ It is no coincidence the September Khorramshar test occurred nine days after the U.S. Treasury placed additional sanctions on entities and individuals associated with the IRGC's ballistic missile program.²¹⁷ The Khorramshar test is also important because in November 2017, the IRGC deputy commander, Hossein Salami, threatened to break Iran's self-imposed 2000 km range on LRBMs, "if Europe turns into a threat."²¹⁸ This threat corresponds with pressure from the Trump Administration on European powers to cancel the JCPOA.²¹⁹ Missile tests in 2017 were a central part of Iran's gray zone operations, especially, when trying to coerce the United States and Europe to remain within JCPOA.

In 2018, with exception of one MRBM test in January, Iran did not directly conduct any gray zone operations before May.²²⁰ During early 2018, Iran was trying to prevent the collapse of JCPOA which may explain the lack of lethal gray zone operations conducted by the IRGC.²²¹ The only known attack in 2018 was conducted by the IRGC-QF when 32

²¹³ "Iran Says Ballistic Missile Capable of Hitting Ships Tested Successfully," CBS News, March 9, 2017, <https://www.cbsnews.com/news/iran-ballistic-missile-capable-hitting-ships-test-launch/>.

²¹⁴ "Iran Says Ballistic Missile Capable of Hitting Ships Tested Successfully."

²¹⁵ "Iran Says Ballistic Missile Capable of Hitting Ships Tested Successfully."

²¹⁶ "Timeline of Military and Security Events," The Iran Primer, August 10, 2021, <https://iranprimer.usip.org/resource/timeline-military-and-security-events>.

²¹⁷ "Timeline of Military and Security Events."

²¹⁸ "Tehran-U.S. Iran Trigger List," International Crisis Group, December 14, 2017, <https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/tehran>.

²¹⁹ "Tehran-U.S. Iran Trigger List."

²²⁰ Michael Bachner, "Israel Accuses Iran of Testing 2 Missiles This Year, Violating UNSC Resolution," The Times of Israel, May 24, 2018, <https://www.timesofisrael.com/israel-accuses-iran-of-testing-2-missiles-this-year-violating-uns-c-resolution/>.

²²¹ "Tehran-U.S. Iran Trigger List."

rockets were fired at Israeli positions in the Golan Heights from Syria in May.²²² Eventually Iran would resume missile tests with SRBM tests during a naval exercise in the Strait of Hormuz in August 2018.²²³ Although Iran would not test again until December 2018, the MRBM test would start a significant period of missile testing beginning in 2019.²²⁴ The start of IRGC missile testing in December corresponds with the USS John C. Stennis entering the Persian Gulf after a long absence of U.S. aircraft carriers in the critical waterway.²²⁵ Although Iran's lethal gray zone operations in 2018 were not significant, they corresponded to the growing tensions with the Trump Administration and would accelerate the next year.

Iranian lethal gray zone operations were the most numerous in 2019 and ranged from missile tests to maritime attacks. In January and February Iran failed to launch two SLVs; however, the United States viewed the rockets for Iran's satellite launches as cover for Iran's intercontinental ballistic missile (ICBM) program.²²⁶ Although, it is debated whether these space launches are for military use, it is categorized as a lethal weapons test because the U.S. government views it as linked to Iran's ICBM program, the SLV uses a rocket engine previously used in ballistic missiles, and could be augmented for military purposes.²²⁷ February 2019 was also significant for missile testing because Iran tested several new capabilities. Iran tested a surface-to-surface cruise missile based off the nuclear capable Soviet Kh-55, which has a range up to 1200 km.²²⁸ Most significantly, Iran tested

²²² Judah Ari Gross, "Air Force Chief: Iranians Fired 32 Rockets at Golan on May 10," *The Times of Israel*, May 22, 2018, <https://www.timesofisrael.com/air-force-chief-iranians-fired-32-rockets-at-golan-on-may-10/>.

²²³ "Iran Missile Milestones: 1985–2022."

²²⁴ "Tehran-U.S. Iran Trigger List."

²²⁵ "Iran Says It Made Successful Submarine Missile Launch in Gulf War Games," *Reuters*, February 24, 2019, <https://www.reuters.com/article/us-iran-gulf-wargames-idUSKCN1QD06S>.

²²⁶ Geoff Brumfiel, "Iran Is Preparing A Launch. But Is It For A Space Rocket Or A Missile?," *National Public Radio*, January 14, 2019, <https://www.npr.org/2019/01/14/684467347/iran-is-preparing-a-launch-but-is-it-for-a-space-rocket-or-a-missile>; Geoff Brumfiel, "Satellite Imagery Suggests 2nd Iranian Space Launch Has Failed," *National Public Radio*, February 6, 2019, <https://www.npr.org/2019/02/06/692071812/satellite-imagery-suggests-second-iranian-space-launch-has-failed>.

²²⁷ Brumfiel, "Iran Is Preparing A Launch. But Is It For A Space Rocket Or A Missile?"

²²⁸ "Iran Missile Milestones: 1985–2022."

its first submarine-launched cruise missile during the Velayat 97 exercise.²²⁹ Submarine-launched cruise missiles give Iran not only a greater maritime attack capability, but gives Iran another method of attack where determining attribution is difficult. In May 2019 Iran began direct attacks on oil tankers as a response to the United States ending waivers on Iran oil sanctions, designating the IRGC as a foreign terrorist organization (FTO) in April 2019, the U.S. Navy announcing the deployment of the USS Abraham Lincoln Carrier Strike Group, and the deployment of the U.S. Air Force bomber task force to the Middle East in early May of 2019.²³⁰ On May 12, 2019 four tankers, two Saudi, one Emirati, and one Norwegian flagged, were significantly damaged likely by Iranian limpet mines.²³¹ Although Iran denied involvement in the attack, Rear Admiral Michael Gilday, director of the Joint Staff, confirmed the limpet mine attack and the IRGC's involvement.²³² In June 2019, the IRGC attacked two more tankers, one Japanese and one Norwegian, in the Gulf of Oman as they were traveling from the United Arab Emirates.²³³ The U.S. Navy, using a surveillance drone, was able to film an IRGC patrol boat trying to remove an unexploded limpet mine from the Kokura Courageous, the damaged Japanese tanker.²³⁴ During this incident, Iran also unsuccessfully tried to prevent the surveillance of IRGC patrol boats near the damaged vessels by shooting at the U.S. drone.²³⁵ As tensions and rhetoric between Iran and the Trump Administration escalated in June, an Iranian surface-to-air missile (SAM) shot down a U.S. RQ-4 Global Hawk operating in international airspace over the Strait of Hormuz.²³⁶ Iran claimed the drone was violating its airspace, which the

²²⁹ "Iran Missile Milestones: 1985–2022."

²³⁰ "Timeline of Military and Security Events"; "Tehran-U.S. Iran Trigger List."

²³¹ Ostovar, "Deterring Iran: Strategic Behavior and the Maritime Domain," 17–18.

²³² "Timeline of Military and Security Events."

²³³ "Factbox: Latest on Tanker Attacks South of Strait of Hormuz," Reuters, June 13, 2019, <https://www.reuters.com/article/us-mideast-tankers-facts/latest-on-suspected-attacks-on-tankers-in-gulf-of-oman-idUSKCN1TE142>.

²³⁴ Ostovar, "Deterring Iran: Strategic Behavior and the Maritime Domain," 18.

²³⁵ "U.S. Blames Iran for Helping Houthi Rebels Shoot Down Drone in Yemen," Reuters, June 16, 2019, <https://www.reuters.com/article/us-mideast-attacks-usa-drone/us-blames-iran-for-helping-houthi-rebels-shoot-down-drone-in-yemen-idUSKCN1TH0LA>.

²³⁶ "Timeline of Military and Security Events."

United States denied.²³⁷ In July 2019, Iran would test fire another MRBM with a reported range of 1100 km.²³⁸ Also in July, an Iranian drone harassed a U.S. warship several times and was shot down because it threatened the safety of the vessel.²³⁹ Maritime gray zone attacks in 2019 would cease after the summer.

September 2019 marked a major escalation in Iran's gray zone operations and the most significant direct attack on Saudi Arabia. On September 14, 2019 the IRGC launched cruise missiles and drones at Saudi oil facilities in Abqaiq and Khurais.²⁴⁰ At least 18 one-way drones were launched at Abqaiq and seven cruise missiles struck Khurais causing significant damage and taking oil offline for weeks.²⁴¹ Abqaiq is one of the most important oil facilities in the world and the largest in Saudi Arabia, while the Khurais facility is over the largest oil field in Saudi Arabia.²⁴² The attack suspended the production of 5.7 million barrels of oil a day—six percent of the global supply.²⁴³ The attack temporarily halved Saudi oil production and caused significant embarrassment to the Saudi government.²⁴⁴ Iran denied involvement in the attack and used their Houthi proxies to take credit, but the attack had clearly originated from Iran.²⁴⁵ The attack demonstrated that Iran could strike Saudi Arabia's most important economic infrastructure, coordinate a sophisticated and complex attack, and most importantly, that Saudi Arabia and the United States would not retaliate in kind. These gray zone attacks on economic infrastructure can also be considered economic coercion and is discussed in a later section. While a significant escalation of attacks occurred using Iran's proxies in Iraq, Iran did not conduct any further lethal gray

²³⁷ "Timeline of Military and Security Events."

²³⁸ "Iran Missile Milestones: 1985–2022."

²³⁹ "Tehran-U.S. Iran Trigger List."

²⁴⁰ "Timeline of Military and Security Events."

²⁴¹ Ostovar, "Deterring Iran: Strategic Behavior and the Maritime Domain," 20–21.

²⁴² "Timeline of Military and Security Events."

²⁴³ "Timeline of Military and Security Events."

²⁴⁴ Katherine Zimmerman, "Yemen's Houthis and the Expansion of Iran's Axis of Resistance," Critical Threats, March 14, 2022, 2, <https://www.criticalthreats.org/analysis/yemens-houthis-and-the-expansion-of-irans-axis-of-resistance>.

²⁴⁵ Ostovar, "Deterring Iran: Strategic Behavior and the Maritime Domain," 21.

zone operations in 2019. Iran's lethal gray zone operations in 2019 were significant in both their damage and scope, but also because despite the presence of U.S. carrier strike groups, strategic bombers, and more troops, the United States and its allies had no effective response or ways to counter Iran's gray zone operations.

Tensions between Iran and the United States reached a pinnacle in January 2020 after the U.S. strike on IRGC-QF commander Qasem Soleimani as discussed earlier. In response to his death on January 3, Iran launched 16 ballistic missiles into Iraq against U.S. forces in Al Asad and Erbil.²⁴⁶ Although there was no loss of life, this was the largest ballistic missile strike against U.S. troops in history.²⁴⁷ It was later revealed that at least 109 U.S. servicemembers suffered brain damage due to the attack.²⁴⁸ It could be argued that the attack was attributable, unambiguous, and significant enough to be classified as above the threshold of armed conflict, and thus might not be considered a gray zone attack. However, after considerable deliberation, the ballistic missile attack is categorized as a gray zone attack, albeit at the very limit of gray zone operations. It is categorized as a gray zone attack because the targets were limited in size compared to more significant U.S. bases in Bahrain, the United Arab Emirates, and Qatar which could have been targeted if Iran did not want to remain below the threshold of war. In addition, the attack was accompanied by non-escalatory language from the Iranian Foreign Minister, Javad Zarif, who invoked Article 51 of the U.N. Charter and insisted that Iran did not want war.²⁴⁹ Due to the heightened tensions, Iran conducted no more direct gray zone attacks in 2020.

In April 2020, 11 IRGCN fast attack craft did harass and conduct dangerous approaches to six U.S. vessels in international waters of the Persian Gulf.²⁵⁰ Although this is not a new tactic for the IRGCN and occurs frequently, due to the large number of vessels

²⁴⁶ "Tehran-U.S. Iran Trigger List."

²⁴⁷ Michael Kaplan and Catherine Herridge, "Army to Award Purple Hearts to 50 Soldiers Injured in Iran Missile Attack Following CBS News Investigation," CBS News, December 20, 2021, <https://www.cbsnews.com/news/purple-heart-iran-missile-attack-50-soldiers/>.

²⁴⁸ "Timeline of Military and Security Events."

²⁴⁹ "Tehran-U.S. Iran Trigger List."

²⁵⁰ "Tehran-U.S. Iran Trigger List."

involved and at such heightened time it should be considered a coercive act and categorized as a gray zone operation. Also in April 2020, the IRGC launched a Nour-1 “multipurpose satellite,” which was viewed by the United States and Israel as a facade for another missile test.²⁵¹ In July 2020, the IRGCN and IRGC Aerospace Force (IRGCAF) conducted a wargame which simulated attacks against a mock U.S. aircraft carrier near the Strait of Hormuz.²⁵² This was likely a response to the Nimitz Carrier Strike Group arriving in the Middle East in June 2020.²⁵³ The last direct Iranian gray zone operation of 2020 occurred when naval, army, and air force elements of the *Artesh* conducted cruise missile and drone tests during the Zolfaghar-99 military exercise.²⁵⁴ After August 2020, there was a massive spike in daily COVID-19 cases, peaking in December 2020, which may explain the significant reduction in gray zone operations during this time.²⁵⁵

The Iranians started 2021 with several lethal gray zone operations to test and pressure the newly inaugurated Biden Administration. In January 2021, the IRGC test fired ballistic missiles and drones during a large-scale military exercise.²⁵⁶ During the exercise the Iranians tested a LRBM with a range of 1800 km and claimed it was designed for the “enemy’s warships.”²⁵⁷ The IRGC also unveiled a newly constructed underground missile base on the southern coast of Iran to store IRGCN strategic missiles.²⁵⁸ February saw an especially large increase in weapons testing and military drills as a part of an effort to pressure the new Biden Administration to resume JCPOA talks.²⁵⁹ This includes the firing

²⁵¹ “Tehran-U.S. Iran Trigger List.”

²⁵² “Timeline of Military and Security Events.”

²⁵³ Megan Eckstein, “Nimitz Carrier Strike Group to Return Home from Middle East Deployment,” USNI News, December 31, 2020, <https://news.usni.org/2020/12/31/nimitz-carrier-strike-group-to-return-home-from-middle-east-deployment>.

²⁵⁴ “Timeline of Military and Security Events.”

²⁵⁵ “Iran Struggles with COVID-19 in 2020,” The Iran Primer, December 16, 2020, <https://iranprimer.usip.org/blog/2020/dec/16/iran-struggles-covid-19-2020>.

²⁵⁶ “Tehran-U.S. Iran Trigger List.”

²⁵⁷ “Tehran-U.S. Iran Trigger List.”

²⁵⁸ “Tehran-U.S. Iran Trigger List.”

²⁵⁹ “Iran’s Army Test Fires Short-Range ‘smart’ Missile,” AP News, February 14, 2021, <https://apnews.com/article/tehran-iran-ad9f0bbe47a54853188c2252b54c199b>.

of a new “smart” short-range missile and testing another SLV, which the State Department believed to incorporate technology identical and interchangeable with ballistic missiles.²⁶⁰ February 2021 also saw the beginning of a renewed maritime gray zone campaign, but this time against ships associated with Israeli companies. Iran’s maritime gray zone attacks were a response to the Israeli attacks on Iranian ships bringing fuel and weapons to Syria in 2019.²⁶¹ The Israeli owned Helios Ray, a cargo ship, was the first Israeli ship damaged in 2021 by two limpet mines placed on the outside of its hull in the Gulf of Oman—Iran denied involvement, despite the Israeli government blaming Iran.²⁶² As more discussions between the United States and Iran about returning to the JCPOA grew, Iran continued attacking Israeli container ships in March and April of 2021.²⁶³ The Israeli-owned Lori was struck by an IRGC missile in the Arabian Sea in late March.²⁶⁴ In April 2021 the Hyperion Ray was hit by an IRGC missile or one-way drone off the coast of Fujairah, which was likely a response to the alleged Israeli sabotage of the Iranian nuclear enrichment facility in Natanz two days earlier.²⁶⁵ May and June 2021 remained quiet, but Iran resumed attacks on Israeli-owned ships in July with a missile or drone strike against the CSAV Tyndall off the Emirati coast.²⁶⁶ Then again in late July, the M/T Mercer Street was struck on two consecutive days by delta-wing one-way attack drones causing significant damaged and killing the ship’s master and security officer.²⁶⁷ Parts recovered by an explosive ordnance disposal team from the USS Ronald Reagan were analyzed and

²⁶⁰ “Iran’s Army Test Fires Short-Range ‘smart’ Missile”; “Tehran-U.S. Iran Trigger List.”

²⁶¹ “Israel-Iran Conflict at Sea,” The Iran Primer, April 14, 2021, <https://iranprimer.usip.org/blog/2021/apr/14/israel-iran-conflict-sea>.

²⁶² “Netanyahu Blames Iran for Blast on Israeli-Owned Ship in Gulf of Oman,” BBC News, March 1, 2021, <https://www.bbc.com/news/world-middle-east-56237295>.

²⁶³ “Timeline of Military and Security Events.”

²⁶⁴ “Tehran-U.S. Iran Trigger List.”

²⁶⁵ “Timeline of Military and Security Events.”

²⁶⁶ Reuters, “Israeli Officials Say Cargo Ship Possibly Attacked En Route to UAE- Israeli Media,” Reuters, July 3, 2021, <https://www.reuters.com/world/middle-east/israeli-officials-say-cargo-ship-possibly-attacked-en-route-uae-israeli-n12-news-2021-07-03/>.

²⁶⁷ U.S. Central Command, “Iranian UAV Attack Against MOTOR TANKER MERCER STREET” (MacDill AFB, FL: U.S. Central Command, August 6, 2021), <https://www.centcom.mil/Portals/6/PressReleases/MERCERSTREETATTACK06AUG2%20final.pdf>.

determined to be of Iranian origin.²⁶⁸ Iran conducted no additional direct attacks for the remainder of the year as negotiations between Iran and the Biden Administration progressed, and as the United States withdrew from Afghanistan.²⁶⁹ As U.S.-Iranian talks stalled and JCPOA negotiations entered their eighth round in December 2021, Iran began significant weapons testing again.²⁷⁰ The IRGCN test fired 16 ballistic and cruise missiles as well as drones during a military exercise in late December 2021.²⁷¹ Iran finished 2021 with an additional launch of “space cargoes” via its SLV, which the United States expressed concern that the tests were a cover for additional ballistic missile testing.²⁷² Iran’s lethal gray zone operations in 2021 should be viewed from two angles, one as trying to bring the new Biden Administration to the JCPOA negotiating table and the second as a response to the Israeli campaign targeting Iranian shipping.²⁷³

The first eight months of 2022 were relatively quiet compared to 2021 and Iran mainly conducted weapons testing. In February 2022, the IRGC unveiled a new ballistic missile, the Kheibar Shekan, which has a range of 1450 km and was claimed to be more maneuverable.²⁷⁴ The IRGC did launch 12 ballistic missiles at a suspected Israeli Mossad facility in Erbil, likely in response to an Israeli airstrike on IRGC-QF forces in Damascus, but no casualties were reported despite the IRGC claiming otherwise.²⁷⁵ The LRBM attack, launched from Iran, also landed near U.S. facilities, but none were damaged.²⁷⁶ In

²⁶⁸ U.S. Central Command.

²⁶⁹ “Tehran-U.S. Iran Trigger List.”

²⁷⁰ “Tehran-U.S. Iran Trigger List.”

²⁷¹ “Iran Missile Milestones: 1985–2022”; “Tehran-U.S. Iran Trigger List.”

²⁷² “Tehran-U.S. Iran Trigger List.”

²⁷³ “Israel-Iran Conflict at Sea.”

²⁷⁴ Jeremy Binnie, “Iran Unveils Kheibar Shekan Ballistic Missile,” *Janes*, February 10, 2022, <https://www.janes.com/defence-news/news-detail/iran-unveils-kheibar-shekan-ballistic-missile>.

²⁷⁵ “Iranian Guards Claim Ballistic Missile Attacks in Erbil,” *Al Jazeera*, March 13, 2022, <https://www.aljazeera.com/news/2022/3/13/missiles-hit-iraqs-kurdish-capital-no-casualties-officials>; “IRGC Warns Israel after Missile Strike on Mossad Bases in Erbil,” *PressTV* (PressTV, March 13, 2022), <https://www.presstv.ir/Detail/2022/03/13/678473/Iran-IRGC-Missile-Attack-Israel-Erbil>.

²⁷⁶ “Iran Claims Responsibility for Missile Strike near U.S. Consulate in Iraq,” *The Guardian*, March 13, 2022, sec. World news, <https://www.theguardian.com/world/2022/mar/13/iran-claims-responsibility-missile-strike-erbil-iraq-us-consulate>.

May the IRGC unveiled its first drone-launched cruise missile, the Heidar-1 and 2, with a range of 200 km—the Heidar-2 uses the same type of engine found on Houthi missiles.²⁷⁷ There would be no more Iranian lethal gray zone operations until August when the IRGCN tried to capture a U.S. Navy USV Saildrone in the Persian Gulf.²⁷⁸ This is included as a lethal gray zone operation because both sides involved warships and the U.S. Navy had to threaten force to get the IRGCN to release the surveillance USV.²⁷⁹ The *Artesh* navy would try a few days later in September 2022, to capture two more Saildrones with a frigate—U.S. Navy destroyers intercepted the Iranians and forced them to release the drones.²⁸⁰ September 2022, also saw a massive attack on Erbil with 73 ballistic missiles and dozens of drones hitting U.S.-backed Kurdish groups in which one U.S. citizen died.²⁸¹ The attack on the Kurdish groups threatened the United States enough for an F-15 to shoot down a drone operating near U.S. forces.²⁸² Iran would continue attacking Kurdish groups for 14 consecutive days, but is not categorized as gray zone operations because they did not involve U.S.-backed forces and were likely a response to growing protests in the Kurdish region of Iran.²⁸³ The last lethal gray zone operation of 2022 was the IRGC launching another SLV, which the U.S. said used ballistic missile technology.²⁸⁴ As discussed earlier, the Iranian regime was overwhelmed by protests due to the death of Mahsa Amini, which may explain the lack of significant lethal gray zone operations during the end of 2022.

²⁷⁷ “Iran Missile Milestones: 1985–2022.”

²⁷⁸ Caitlin M. Kenney, “Iranian Navy Tries To Steal U.S. Unmanned Vessel At Sea,” *Defense One*, August 30, 2022, <https://www.defenseone.com/threats/2022/08/iranian-navy-tries-steal-us-unmanned-vessel-sea/376513/>.

²⁷⁹ Kenney.

²⁸⁰ Mallory Shelbourne, “Iran Temporarily Captures Two U.S. Saildrones in Red Sea,” *USNI News*, September 2, 2022, <https://news.usni.org/2022/09/02/iran-temporarily-captures-two-u-s-saildrones-in-red-sea>.

²⁸¹ “Iran Attacks Kurdish Groups in Iraq,” *The Iran Primer*, September 29, 2022, <https://iranprimer.usip.org/blog/2022/sep/29/iran-attacks-kurdish-groups-iraq>; Vedant Patel, “Department Press Briefing – September 29, 2022,” United States Department of State, September 29, 2022, <https://www.state.gov/briefings/departments-press-briefing-september-29-2022/>.

²⁸² “Iran Attacks Kurdish Groups in Iraq.”

²⁸³ “Iran Attacks Kurdish Groups in Iraq.”

²⁸⁴ “Tehran-U.S. Iran Trigger List.”

B. NON-LETHAL GRAY ZONE OPERATIONS

1. Cyber Warfare

Cyber warfare allows Iran to respond to threats while avoiding a conventional war with stronger adversaries.²⁸⁵ As a major pillar of Iran’s asymmetric warfare doctrine, Iran has invested significant resources in developing its cyber capabilities since the early 2000s.²⁸⁶ The IRGC and Ministry of Intelligence (MoI) are the main government actors executing Iran’s cyber gray zone operations.²⁸⁷ The IRGC sponsors or performs the majority of Iran’s offensive cyberattacks both internally and externally.²⁸⁸ The IRGC is also the most important sponsor of Iran’s cyber proxy groups, independent contractors, and volunteer cyber actors.²⁸⁹ Just as armed proxy groups are a key asymmetric capability for retaliation and deniability, cyber proxies form a major part of Iran’s cyber warfare.²⁹⁰ Although most cyber proxies are not technically sophisticated, many of Iran’s most successful cyberattacks were conducted by proxies, such as the Iranian Cyber Army and Shamoon Group.²⁹¹ In addition, the Mabna Institute is an Iran-based company established by the IRGC to conduct cyberespionage against foreign scientific and research institutions.²⁹² Furthermore, within the IRGC there is a volunteer paramilitary organization called the *Basij*—the Basij has its own cyber force controlled under the Basij Cyber Council.²⁹³ The Basij’s “cyber army” typically executes low-level hacking and unsophisticated attacks.²⁹⁴

²⁸⁵ Bahgat and Ehteshami, *Defending Iran*, 137.

²⁸⁶ Bahgat and Ehteshami, 141.

²⁸⁷ Anderson and Sadjadpour, “Iran’s Cyber Threat,” 5.

²⁸⁸ Anderson and Sadjadpour, 17.

²⁸⁹ Anderson and Sadjadpour, 17.

²⁹⁰ Theohary, *Iranian Offensive Cyberattack Capabilities*, 1.

²⁹¹ Marie Baezner, “Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions,” application/pdf (ETH Zurich, May 2019), 11, <https://doi.org/10.3929/ETHZ-B-000344841>.

²⁹² Fabio Rugge, *Confronting an “Axis of Cyber”?* (IT: Ledizioni, 2018), 129–30, <https://doi.org/10.14672/67058655>.

²⁹³ Theohary, *Iranian Offensive Cyberattack Capabilities*, 1.

²⁹⁴ “The Iranian Cyber Threat Structure,” United Against Nuclear Iran, September 2022, <https://www.unitedagainstinucleariran.com/iranian-cyber-threat-structure>.

Iran's cyber warfare is mainly devoted to espionage and sabotage.²⁹⁵ Iranian advanced persistent threats (APTs) regularly use spear phishing, distributed denial-of-service (DDoS attacks), personally identifiable information theft, and destructive malware for espionage and sabotage.²⁹⁶ Compared to Russian or Chinese hackers, Iranian hackers typically seek to do as much damage as possible vice developing technical information or mapping networks for future use.²⁹⁷ Cyberespionage remains the primary reason for Iran's cyberattacks, including government, military, and scientific institutions.²⁹⁸ For example, the Iranian APT MuddyWater, has targeted telecommunications, defense, and oil and gas companies in support of the MoI's global cyberespionage campaign.²⁹⁹ Cyber sabotage is Iran's primary means of retaliation against United States and its allies.³⁰⁰ Iranian cyber sabotage operations are most prevalent after the United States, Israel, or Saudi Arabia have conducted operations against Iran.³⁰¹

From 2017–2022, Iran used cyber warfare in concert with its lethal gray zone operations to respond to the United States and its allies as it has in the past. In January 2017, the Shamoon 2 virus, an updated version of the Shamoon malware that paralyzed Saudi Aramco in 2012, was used to attack the Saudi labor ministry as well as several Saudi petrochemical companies.³⁰² Although the full extent of the damage is unknown, only network disruptions were reported and nothing like the damage of the original Shamoon

²⁹⁵ Anderson and Sadjadpour, "Iran's Cyber Threat," 6.

²⁹⁶ "Iran Cyber Threat Overview and Advisories," Cyber and Infrastructure Security Agency, accessed June 14, 2022, <https://www.cisa.gov/uscrt/iran>.

²⁹⁷ Patrick Diotte, "The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online," *Canadian Military Journal* 20, no. 4 (2020): 37–38.

²⁹⁸ Anderson and Sadjadpour, "Iran's Cyber Threat," 7, 30.

²⁹⁹ "Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks," U.S. Cyber Command, February 24, 2022, <https://www.cybercom.mil/Media/News/Article/2945592/iranian-government-sponsored-actors-conduct-cyber-operations-against-global-gov/>.

³⁰⁰ Anderson and Sadjadpour, "Iran's Cyber Threat," 6.

³⁰¹ Anderson and Sadjadpour, 7.

³⁰² "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces," Reuters, January 23, 2017, <https://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR>.

virus was experienced.³⁰³ In August 2017, another cyber-attack was launched against Aramco with the intent to target safety control systems and potentially cause an explosion.³⁰⁴ At the time of the cyber-attack, Saudi Arabia was preparing for the initial public offering (IPO) of Aramco, and the attack was likely meant to cause the IPO significant loss.³⁰⁵ In 2018, several U.S. hospitals, municipalities, and public institutions suffered several SamSam Ransomware attacks causing over \$30 million in losses due to an Iranian hacking group.³⁰⁶ The largest of these ransomware attacks was against the City of Atlanta where the city government's computer systems were essentially shutdown for days and affected six million people.³⁰⁷ In March 2018, the FBI revealed a massive hacking campaign by the Mabna Institute, where 31 terabytes of documents were stolen from 8,000 professors across 144 U.S.-based universities and 176 foreign universities.³⁰⁸ Although the Mabna Institute's campaign began as earlier as 2013, it went until at least December 2017 and was able to obtain massive amounts of academic data and intellectual property.³⁰⁹ Then in 2018, after the Trump Administration withdrew from JCPOA in May, Iranian cyberattacks increased significantly against the United States.³¹⁰ In particular, the MoI sponsored group MuddyWater, began its widespread campaign against government

³⁰³ "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces."

³⁰⁴ Elias Groll, "Cyberattack Targets Safety System at Saudi Aramco," *Foreign Policy*, December 21, 2017, <https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/>.

³⁰⁵ Groll.

³⁰⁶ Office of Public Affairs, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over \$30 Million in Losses," U.S. Department of Justice, November 28, 2018, <https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public>.

³⁰⁷ Alan Blinder and Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder," *CNBC*, March 28, 2018, <https://www.cnbc.com/2018/03/28/a-cyberattack-hobbles-atlanta-and-security-experts-shudder.html>.

³⁰⁸ Office of Public Affairs, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," U.S. Department of Justice, March 23, 2018, <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>.

³⁰⁹ Office of Public Affairs.

³¹⁰ "The Invisible U.S.-Iran Cyber War," *The Iran Primer*, October 25, 2019, <https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war>.

and private sector organizations in 2018 as a response to increasing tensions with the United States.³¹¹

Throughout 2019, FireEye, a cyber security firm, revealed further Iranian cyberattacks across the Middle East against telecoms, internet service providers, and governments.³¹² Microsoft also reported in 2019, that over 200 companies had been targeted by Iran over the past two years resulting in \$100 million in lost productivity.³¹³ The U.S. Department of Homeland Security (DHS) said that Iran’s malicious cyber activity had increased against U.S. government and private industry in 2019.³¹⁴ The most notable Iranian attack in 2019 was when an Iranian hacker group tried to breach accounts associated with the upcoming 2020 U.S. presidential election.³¹⁵ Then in 2020 the scope and intensity of cyberattacks increased significantly after the death of IRGC-QF commander, Qasem Soleimani.³¹⁶ In April 2020, Iran hacked Israel’s water authority systems to increase the chlorine levels in the water and cause pump malfunctions.³¹⁷ Also in April 2020, Iran attempted phishing attacks against U.S. drugmaker Gilead Sciences, which was working on treatments for COVID-19.³¹⁸ Throughout the summer of 2020, Iranian APT35, also known as Charming Kitten, had several high-profile hacking attempts including phishing attacks against the Trump reelection campaign.³¹⁹ Iranian APT35 also breached Google

³¹¹ “Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks.”

³¹² Lily Hay Newman, “A Worldwide Hacking Spree Uses DNS Trickery to Nab Data,” *Wired*, accessed March 28, 2023, <https://www.wired.com/story/iran-dns-hijacking/>.

³¹³ Robert McMillan, “Iranian Hackers Have Hit Hundreds of Companies in Past Two Years,” *The Wall Street Journal*, accessed March 28, 2023, <https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036>.

³¹⁴ “The Invisible U.S.-Iran Cyber War.”

³¹⁵ “The Invisible U.S.-Iran Cyber War.”

³¹⁶ “Heightened Awareness for Iranian Cyber Activity,” Cyber and Infrastructure Security Agency, January 25, 2022, <https://www.cisa.gov/news-events/alerts/2020/12/03/heightened-awareness-iranian-cyber-activity>.

³¹⁷ “Israel-Iran Cyber War, Gas Station Attack,” *The Iran Primer*, November 2, 2021, <https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack>.

³¹⁸ Jack Stubbs and Christopher Bing, “Exclusive: Iran-Linked Hackers Recently Targeted Coronavirus Drugmaker Gilead – Sources,” *Reuters*, May 8, 2020, <https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV>.

³¹⁹ “The Invisible U.S.-Iran Cyber War.”

accounts of U.S. Navy officials and targeted State Department officials’ personal Google accounts.³²⁰ Once again, MuddyWater was able to target several Israeli organizations with malware and ransomware in September 2020.³²¹ Another Iranian hacking group was able to use phishing to hack into the accounts of the Munich Security Conference and Saudi Think20 causing the compromise of the accounts of several former ambassadors and senior policy experts.³²² Lastly in 2020, an Iranian cyber group was able to target several U.S. state election websites and obtain “non-public voter data.”³²³ Overall, Iranian APTs were so active in 2020 the Cybersecurity and Infrastructure Security Agency (CISA) had to issue several advisories on Iran’s cyber-attacks.³²⁴

In 2021, the first prominent Iranian cyber-attack was again from Charming Kitten, where two dozen senior medical researchers specializing in oncology, neurology, and genetics in the United States and Israel experienced several phishing attempts in March.³²⁵ In July 2021, Iranian hackers, using Facebook, targeted over 200 people associated with the U.S. and U.K. military and defense industries.³²⁶ The Facebook campaign was also a part of a larger IRGC linked cyberespionage campaign.³²⁷ Also in July, documents leaked to Sky News show an IRGC cyber unit, Intelligence Team 13, planned to hack water filtration systems, fuel systems, maritime communications, and other critical infrastructure

³²⁰ Thomas Brewster, “Big Leak Reveals Iran Targeting U.S. Military With Super Speedy Google Account Hacks,” *Forbes*, June 16, 2020, sec. Cybersecurity, <https://www.forbes.com/sites/thomasbrewster/2020/07/16/big-leak-reveals-iran-targeting-us-military-with-super-speedy-google-account-hacks/>.

³²¹ “Israel-Iran Cyber War, Gas Station Attack.”

³²² “The Invisible U.S.-Iran Cyber War.”

³²³ “The Invisible U.S.-Iran Cyber War.”

³²⁴ “The Invisible U.S.-Iran Cyber War.”

³²⁵ Joshua Miller, “BadBlood: TA453 Targets U.S. & Israel in Credential Phishing | Proofpoint US,” Proofpoint, March 30, 2021, <https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential>.

³²⁶ Musadiq Bidar, “Facebook Says Iranian Hackers Targeted U.S. Military Personnel,” CBS News, July 15, 2021, <https://www.cbsnews.com/news/facebook-iran-hackers-us-military-defense-contractors-fake-accounts/>.

³²⁷ Bidar.

associated with the United States, France, and Germany.³²⁸ In October and November 2021, Microsoft revealed that Iranian APTs were able to hack into U.S. and Israeli maritime companies as well as gain access to U.S. critical infrastructure.³²⁹ There were less high profile hacking incidents in 2022, but Iranian APTs continued cyberattacks against the Microsoft Exchange in attempt to gain access to U.S. critical infrastructure.³³⁰ The IRGC also published hacked Israeli port footage and personal information of Israeli port workers as a response to an Israeli cyberattack against an Iranian port earlier in 2022.³³¹ At the end of 2022, CISA released that Iranian APTs had throughout 2022, compromised Federal Civilian Executive Branch organizations and harvested credentials and account information.³³² Cyber warfare was a key component of Iran's overall gray zone operations from 2017–2022 and was consistently used when lethal means were not viable. It is difficult to fully account for all of Iran's cyberattacks during this time, but it is safe to say Iranian APTs conducted sophisticated cyber campaigns which undermined the United States and its allies in the Middle East.

³²⁸ Deborah Haynes, "Iran's Secret Cyber Files on How Cargo Ships and Petrol Stations Could Be Attacked," Sky News, accessed March 28, 2023, <https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871>.

³²⁹ Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security, "Iran-Linked DEV-0343 Targeting Defense, GIS, and Maritime Sectors," *Microsoft Security Blog* (blog), October 11, 2021, <https://www.microsoft.com/en-us/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/>; "Iran Cyber Threat Overview and Advisories."

³³⁰ "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations," Cyber and Infrastructure Security Agency, September 14, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-257a>.

³³¹ "Israel-Iran Cyber War, Gas Station Attack"; "Iranian Hackers Publish CCTV Footage, Workers' Details from Haifa, Ashdod Ports," The Times of Israel, February 23, 2022, <https://www.timesofisrael.com/iranian-hackers-publish-cctv-footage-workers-details-from-haifa-ashdod-ports/>.

³³² "Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester," Cyber and Infrastructure Security Agency, November 25, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a>.

2. Information Operations

The Iranian regime views itself in an information war against its Sunni neighbors, Western colonialism, and Israel.³³³ Iran views information operations (IO) as a vital gray zone tool to push the regime's narrative, counter its enemies' messaging, and undermine U.S. influence.³³⁴ Iran uses a variety of methods from digital media to public diplomacy for IO, with social media as its greatest IO vector.³³⁵ The most important actor in Iran's IO campaigns is the Islamic Republic of Iran Broadcasting (IRIB), Iran's propaganda agency.³³⁶ To demonstrate IO's significance to the Iranian regime, Iran spends 50 times more, as a proportion of government spending, than the U.S. equivalent, the U.S. Agency for Global Media (USAGM).³³⁷ The IRIB is responsible for many of the major foreign broadcasting initiatives including, PressTV, Al Alam, Hispan TV, and Pars Today.³³⁸ The IRIB, along with the IRGC, operate radio channels and TV stations with significant web presences as well.³³⁹ There are also seemingly independent news websites that repackage Iranian state media messaging, such as the International Union of Virtual Media (IUVM), which are actually Iranian controlled.³⁴⁰ Pars Today and other IRIB broadcasters will sometimes even cite IUVM as source material for its news to launder the regime's message.³⁴¹ Most significantly, Iran's social media presence is massive—Facebook alone identified 766 regime-linked pages followed by 5.4 million users.³⁴² While the Iranian

³³³ Emerson T Brooking and Suzanne Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century* (Washington, DC: Atlantic Council, 2020), 2.

³³⁴ Eisenstadt, "Iran's Gray Zone Strategy," 85, 88.

³³⁵ Itay Haiminis, "Iran's Information Warfare," in *The Cognitive Campaign: Strategic and Intelligence Perspectives*, ed. Yossi Kuperwasser and David Siman-Tov (Tel Aviv University: Institute for National Security Studies, 2019), 136.

³³⁶ Brooking and Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, 8.

³³⁷ Brooking and Kianpour, 8.

³³⁸ Brooking and Kianpour, 14.

³³⁹ Brooking and Kianpour, 14.

³⁴⁰ Brooking and Kianpour, 15–16.

³⁴¹ Brooking and Kianpour, 16.

³⁴² Brooking and Kianpour, 15.

people are forbidden from Twitter, Supreme Leader Khamenei has an active Twitter account and regularly uses it in concert with IO campaigns.³⁴³ Iran's uses social media and fake websites as a guerrilla broadcasting apparatus that cannot easily be stopped by the United States or its allies.³⁴⁴

Due to the scope and scale of Iran's information operations from 2017–2022, this thesis cannot conduct a yearly analysis of the entirety of Iran's IO campaigns. Information operations are also not necessarily concrete and easily discernible such as with the lethal gray zone attacks, which is why only the major IO campaigns are discussed. The most significant IO campaign was against the Trump Administration's withdrawal from JCPOA and its "maximum pressure campaign."³⁴⁵ Throughout the period, Iran paired formal public diplomacy and strategic communications with coordinated weapons testing, military exercises, and incremental violations of the JCPOA limitations.³⁴⁶ Influential pro-Iranian figures in the United States such as Seyed Hossein Mousavian and Trita Parsi, attacked the Trump Administration and echoed the Iranian regime's narrative.³⁴⁷ Immediately following the Trump Administration's withdrawal from JCPOA there was a massive spike in Iranian Twitter activity against the Trump Administration.³⁴⁸ In Iraq, as the fight against ISIS came to a close, Iran was able to position itself as the protector of the Iraqi Shia population and limit American influence with an extensive IO campaign.³⁴⁹ As tensions in Iraq continued to rise along with lethal gray zone attacks, senior Trump Administration officials' social media accounts were flooded with anti-American comments and Iranian flags—the most prominent was Secretary of State Pompeo Instagram's account.³⁵⁰ In 2020, following the death of General Soleimani, Iranian-linked Facebook and Instagram

³⁴³ Brooking and Kianpour, 5.

³⁴⁴ Brooking and Kianpour, 5.

³⁴⁵ Eisenstadt, "Iran's Gray Zone Strategy," 83.

³⁴⁶ Haiminis, "Iran's Information Warfare," 139–40; Eisenstadt, "Iran's Gray Zone Strategy," 88.

³⁴⁷ Haiminis, "Iran's Information Warfare," 140.

³⁴⁸ Brooking and Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, 19–20.

³⁴⁹ Brooking and Kianpour, 141.

³⁵⁰ Brooking and Kianpour, 20.

accounts flooded the White House account and Trump family accounts with anti-American images and memes.³⁵¹ Regionally oriented Facebook pages were also flooded with anti-American messaging after Soleimani's death.³⁵² The JCPOA IO campaign continued even once the Biden Administration came to office, where Iran claimed it will return to JCPOA negotiations in return for immediate sanctions relief.³⁵³

During 2019–2021 there was also a significant Iranian IO campaign to exacerbate race relations, discredit the 2020 presidential election, and cause political turmoil in United States. For example, Iranian agents created BLMNews.com, a fake news website, which intermingled a variety of stories about racial injustice with those against U.S. sanctions and even promoted Hezbollah's humanitarian work.³⁵⁴ Furthermore, Twitter had to suspend 238 accounts linked to Iran for trying to disrupt and influence the 2020 U.S. presidential election.³⁵⁵ Iran flooded social media sites throughout 2021 to discredit U.S. democracy and circulate anti-U.S. messaging.³⁵⁶ During this time period Iran consistently used bots and fake social media accounts to divide and agitate the target U.S. audience.

Throughout the time period, Iran also conducted major IO campaigns against U.S. allies Saudi Arabia and Israel. Iran created fake news websites, such as the Arabic-website alawatanews.com, to spread false information about and discredit Saudi Crown Prince Mohammed bin Salman.³⁵⁷ Iran also created the fake Hebrew-language website Tel Aviv Times designed to target Israeli public opinion and spread Hezbollah propaganda.³⁵⁸

³⁵¹ Brooking and Kianpour, 17.

³⁵² Brooking and Kianpour, 17.

³⁵³ Office of the Director of National Intelligence, *2023 Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2023), 18.

³⁵⁴ Brooking and Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, 20.

³⁵⁵ "Tehran-U.S. Iran Trigger List."

³⁵⁶ John Weaver, *The U.S. Cybersecurity and Intelligence Analysis Challenges* (York, PA: Palgrave Macmillan, 2022), 68, 74.

³⁵⁷ Jack Stubbs and Tuqa Khalid, "Fake News Network vs. Bots: The Online War around Khashoggi Killing," Reuters, November 1, 2018, <https://www.reuters.com/article/us-saudi-khashoggi-disinformation-idUSKCN1N63QF>.

³⁵⁸ Sagi Cohen, "It's Not an Israeli Site, It's Iranian Propaganda," Ynet, September 6, 2018, <https://www.ynet.co.il/articles/0,7340,L-5342357,00.html>.

Iranian activists even infiltrated Israeli groups on WhatsApp and Telegram in order to promote protests against Prime Minister Netanyahu and stir divisions between Jews and Israeli Arabs.³⁵⁹ Iran also used social media to discredit Saudi Arabia and Israel, with some anti-Israel Twitter campaigns reaching over 100 million total views during the period.³⁶⁰ However, these IO campaigns were hampered in 2022 after the Mahsa Amini protests. Iran conducted major information operations to discredit and spread false information about the Amini mass protests.³⁶¹ Iran targeted not only Western audiences, but also the Persian diaspora using bots and fake accounts to counter the protesters' anti-regime narrative, particularly on Twitter.³⁶² Iran tried to blame the protests on the United States, Peshmerga, and other foreign actors.³⁶³ With the exception of Amini protest in 2022, Iran successfully conducted large-scale multi-domain information operations from 2017–2022.

3. Economic Coercion

Unlike other gray zone actors, such as Russia and China, Iran has limited options for economic coercion. Iran's heavily sanctioned and restricted economy cannot implement major economic sanctions or blockades to change the balance of power in the Middle East.³⁶⁴ For the most part, Iran imposes economic costs as a secondary effect to other gray zone operations. Attacking economic and military infrastructure and increasing the cost to protect them is the primary way Iran uses economic coercion. From 2017–2022, Saudi Arabia suffered the greatest economic costs to Iran's gray zone operations. For example,

³⁵⁹ Ofir Barel, "How Does Iran Wage Its Information Warfare Battle against Israel?," The Washington Institute, September 1, 2021, <https://www.washingtoninstitute.org/policy-analysis/how-does-iran-wage-its-information-warfare-battle-against-israel>.

³⁶⁰ Barel.

³⁶¹ Allan Hassaniyan, "How Longstanding Iranian Disinformation Tactics Target Protests," The Washington Institute, November 1, 2022, <https://www.washingtoninstitute.org/policy-analysis/how-longstanding-iranian-disinformation-tactics-target-protests>.

³⁶² Abbas Al Lawati and Nadeen Ebrahim, "The Battle of Narratives on Iran Is Being Fought on Social Media," CNN, October 5, 2022, <https://www.cnn.com/2022/10/05/middleeast/social-media-disinformation-mime-intl/index.html>.

³⁶³ Hassaniyan, "How Longstanding Iranian Disinformation Tactics Target Protests."

³⁶⁴ Philip Loft, "Iran's Influence in the Middle East," Research Briefing (London, United Kingdom: United Kingdom House of Commons, June 2, 2023), 20–22, <https://commonslibrary.parliament.uk/research-briefings/cbp-9504/>.

at the height of Houthi attacks, Saudi Arabia was spending billions per month to counter them.³⁶⁵ Saudi Arabia had to devote valuable military resources to protect its petroleum industry, spending \$1 million per Patriot missile to take down a Houthi drone that only costs a few hundred dollars.³⁶⁶ The Iranians and Houthis understood this impact and called their campaign against Saudi petroleum infrastructure “Operation Economic Deterrence.”³⁶⁷ Elsewhere, rocket attacks on U.S. owned oil facilities in Iraq were meant to hamper U.S. energy initiatives in Iraq and interfere with a proposed Exxon Mobil deal, another example of economic coercion.³⁶⁸ The missile and drone threat from these lethal gray zone operations also forced the Arab coalition and U.S. Navy to conduct resource-intensive interdiction operations and naval inspections along the Yemeni coast.³⁶⁹ Ultimately, the cost to the Saudi coalition brought them to the negotiating table and a ceasefire was implemented with the Houthis as discussed earlier.³⁷⁰ As Iran’s gray zone operations increased and tensions rose, the United States deployed more troops to Middle East further increasing the costs imposed by Iran.³⁷¹ Another example of a secondary cost imposed on the West was shipping insurance rates increased by ten-fold in 2019 after the Iranian attacks on shipping in the Strait of Hormuz.³⁷² Furthermore, Iran’s cyberattacks during this time also induced significant financial costs to the United States and its allies.³⁷³ As discussed earlier, millions of dollars were lost due to damage from

³⁶⁵ Williams and Shaikh, *The Missile War in Yemen*, 13.

³⁶⁶ Jones et al., *The Iranian and Houthi War against Saudi Arabia*, 11.

³⁶⁷ Williams and Shaikh, *The Missile War in Yemen*, 12.

³⁶⁸ Knights, “Iran-Backed Militias Test the Credibility of Iraq’s Prime Minister.”

³⁶⁹ Williams and Shaikh, *The Missile War in Yemen*, 13.

³⁷⁰ Martin Jay, “Saudi Arabia Looks for a Peace Deal in Yemen, but at What Price?,” *Inside Arabia* (blog), April 2, 2020, <https://insidearabia.com/saudi-arabia-looks-for-a-peace-deal-in-yemen-but-at-what-price/>.

³⁷¹ Barbara Starr, “Saudi Arabia Has Paid \$500M toward the Cost of U.S. Troops in Country,” CNN, January 16, 2020, <https://www.cnn.com/2020/01/16/politics/saudi-arabia-us-troops-payment/index.html>.

³⁷² Sam Meredith, “Insurance Rates Have ‘increased 10-Fold’ after Attacks in the Strait of Hormuz, Shipping CEO Says,” CNBC, July 9, 2019, <https://www.cnbc.com/2019/07/09/oil-insurance-rates-have-soared-since-tanker-attacks-near-iran.html>.

³⁷³ Sam Cohen, “Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests” 3, no. 1 (2019): 89–90.

cyberattacks, lost productivity, or paid to release files held by Iranian ransomware. Throughout this period, Iranian lethal and non-lethal gray zone operations were used as economic coercion on the United States and its allies.

Although most economic costs from gray zone operations were the result of secondary effects there were some instances of direct economic coercion. Iraq is the only U.S. ally that is the exception to Iran's economic influence, and it is estimated that 20 percent of the Iraqi economy is controlled by the IRGC.³⁷⁴ Iraq is very susceptible to Iran's economic coercion, especially in electricity since Iran supplies one-third of Iraq's electricity.³⁷⁵ When the Trump Administration began pressuring the Iraqi government to support sanctioning Iran, Iran withheld some electricity to Iraq in July 2018 and ensured the Iraqi government did not participate in the sanctions.³⁷⁶ The remaining acts of economic coercion occurred at sea during this time. First, in 2019 the IRGCN seized a British tanker, the *Stena Impero*, two weeks after British Royal Marines seized an Iranian tanker likely smuggling oil to Syria.³⁷⁷ The *Stena Impero* was released only after the British released the Iranian tanker, which eventually made it to Syria anyway.³⁷⁸ In 2021, the IRGCN seized a South Korean tanker because it had frozen \$7 billion in Iranian assets.³⁷⁹ The South Korean tanker would be released the same year without any apparent South Korean concessions.³⁸⁰ However, later in 2022 the South Koreans eventually unfroze Iran's assets.³⁸¹ South Korea also paid Iran's U.N. contributions with the frozen

³⁷⁴ "Flashpoints: Iraq."

³⁷⁵ "Flashpoints: Iraq."

³⁷⁶ Robert Bryce, "Iran's Power over Iraq Includes Electricity," *The Hill*, January 9, 2020, <https://thehill.com/opinion/energy-environment/477371-irans-power-over-iraq-includes-electricity/>.

³⁷⁷ "Stena Impero: Seized British Tanker Leaves Iran's Waters," BBC News, September 27, 2019, <https://www.bbc.com/news/world-middle-east-49849718>.

³⁷⁸ "Seized UK-Flagged Tanker Leaves Iranian Waters," Al Jazeera, September 27, 2019, <https://www.aljazeera.com/news/2019/9/27/seized-uk-flagged-tanker-stena-impero-leaves-iranian-port>.

³⁷⁹ "Tehran-U.S. Iran Trigger List."

³⁸⁰ Patrick Wintour and Patrick Wintour Diplomatic editor, "Iran Releases South Korean Tanker Seized in January," *The Guardian*, April 9, 2021, sec. World news, <https://www.theguardian.com/world/2021/apr/09/iran-releases-south-korean-tanker-seized-in-january-oil-revenue-us-sanctions>.

³⁸¹ "Tehran-U.S. Iran Trigger List."

assets in order for Iran to regain its U.N. voting right.³⁸² Most importantly, the U.S. Treasury had to approve a special license for the South Koreans to use the U.S. financial system to reimburse Iranian private investors in early 2022.³⁸³ Clearly, the Iranians were reimbursed for releasing the South Korean tanker. Finally, in response to the Greek Navy seizing an Iranian tanker, the IRGCN seized two Greek tankers in the Persian Gulf in 2022.³⁸⁴ Once again, the Iranians prevailed and Greece released the Iranian tanker and in exchange Iran released the Greek tankers later in 2022.³⁸⁵ Although the scale of Iran's direct economic coercion was relatively small, it worked every time and once again demonstrated the United States and its allies were unable to counter Iran's gray zone operations.

4. Conclusion

From 2017–2022 Iran successfully conducted lethal and non-lethal gray zone operations. As with Iran's lethal proxy operations, Iran's direct lethal operations were often in response to United States or its allies on an ad hoc basis. Despite, the presence of carrier strike groups, strategic bomber task forces, and large numbers of ground forces the United States did not prevent Iran from conducting significant gray zone attacks. The 2019–2021 attacks on shipping, the 2019 Abqaiq and Khurais oil facilities attack, and 2020 ballistic missile attack on Erbil and Al Asad all went without a credible response from the United States and its allies. Israel is the only exception and conducted its own tit-for-tat responses to Iranian operations. In addition, Iran demonstrated its ability to conduct complex multi-axis and multi-domain attacks against critical infrastructure and strategic waterways in the Middle East.

³⁸² "Tehran-U.S. Iran Trigger List."

³⁸³ Republic of Korea Ministry of Foreign Affairs, "Issuance of Specific License by U.S. Office of Foreign Assets Control (OFAC) related to Compensation in Investor State Dispute Settlement (ISDS) with Dayyani Family," ROK Ministry of Foreign Press Releases, January 12, 2022, https://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=321975&page=1; "Tehran-U.S. Iran Trigger List."

³⁸⁴ Ostovar, "Deterring Iran: Strategic Behavior and the Maritime Domain," 18–19.

³⁸⁵ Renee Maltezou and Jonathan Saul, "Iran Releases Two Greek Tankers Seized in May," Reuters, November 16, 2022, <https://www.reuters.com/world/greece-iran-agree-release-two-greek-tankers-seized-by-tehran-2022-11-16/>.

Furthermore, these lethal operations were often paired with cyberattacks, information operations, and economic coercion. Non-lethal gray zone operations were also successfully employed when lethal attacks were not a viable option or if tensions between the United States were too high. Iran was also able to use indirect economic coercion to impose significant costs on the United States and Saudi Arabia in particular. Iran's direct economic coercion, although small in scale, was also successful. Even during rising COVID-19 infections, JCPOA negotiations, or mass protests Iran was still able to conduct non-lethal gray zone operations. Despite the large scale of Iran's IO campaigns, it is difficult to assess, besides the number of views a website or social media post receives, whether any of Iran's IO campaigns actually changed opinions or caused political disruptions. It also difficult to assess, besides economic costs, whether Iran's cyberattacks influenced the United States, Saudi Arabia, or Israel to change policy or limit a particular response.

Overall, during this time Iran was able to project influence throughout the Middle East and even inside the United States. Furthermore, Iran's gray zone operations did not receive major consequences from the United States or its allies. The United States with all its military power and Saudi Arabia with all its oil riches did not stop Iranian attacks or influence. However, Iran did not cause the United States to leave the region or remove sanctions from the Iranian economy. Although Saudi Arabia agreed to a ceasefire and negotiations in Yemen, it did not recognize the Houthis or cease its support to its own Sunni proxies. Iran's gray zone operations from 2017–2022 showed it was a serious regional power, but also increased regional tensions and instability.

IV. IMPACT OF GRAY ZONE OPERATIONS ON IRANIAN STRATEGIC OBJECTIVES

As discussed in the opening chapter, Iran has four main strategic objectives: regime survival, deter aggression, project power, and protect the homeland. From 2017–2022, the survival of Iran’s unique theocratic system of government remained paramount, and was viewed by the Iranian regime as necessary not just for Shia Islam, but for the Muslim world.³⁸⁶ Iran’s second objective was to deter aggression from its adversaries—the United States, Israel, Saudi Arabia, and the United Arab Emirates.³⁸⁷ As a revisionist power, Iran’s third strategic objective was to project power and reassert its leadership in the region.³⁸⁸ Iran’s gray zone strategy was a means for changing the status quo in the Middle East and increasing Iran’s influence.³⁸⁹ Finally, Iran’s fourth main objective was to protect the homeland and its key allies—the Assad regime, Lebanese Hezbollah, Iran-backed Iraqi Shia militias, and the Houthis.³⁹⁰ Iran viewed protecting the homeland as securing its borders, maintaining territorial integrity, and ensuring its sovereignty.³⁹¹ This chapter assesses whether Iran’s gray zone operations advanced each of the four strategic objectives and then presents the general findings at the end.

A. REGIME SURVIVAL

The research demonstrates Iran’s gray zone operations from 2017–2022 positively impacted the Iranian regime’s survival. Iran’s unique theocratic regime did not succumb to the Trump Administration’s maximum pressure campaign and was able to respond to the campaign with a large-scale counter-pressure gray zone campaign. Iran’s regime was able to show strength by standing up to a great power, which helped it weather the economic

³⁸⁶ Bahgat and Ehteshami, *Defending Iran*, 11.

³⁸⁷ Bahgat and Ehteshami, 11–12.

³⁸⁸ Bahgat and Ehteshami, 218, 220; Eisenstadt, “Iran’s Gray Zone Strategy,” 78.

³⁸⁹ Eisenstadt, “Iran’s Gray Zone Strategy,” 77–78.

³⁹⁰ Bahgat and Ehteshami, *Defending Iran*, 218; Ostovar, *Vanguard of the Imam*, 205, 217, 219, 223.

³⁹¹ Tabatabai, *No Conquest, No Defeat*, 300.

and political storms of the time period. The Iranian regime avoided a catastrophic conventional war with the United States, did not submit to U.S. demands, and did not change its foreign or domestic policies despite significant U.S. coercive actions. In addition, the bulwark of the Iranian regime, the IRGC, benefitted the most from gray zone operations because it was the main actor who successfully countered the United States and its allies. Despite the IRGC receiving the U.S. FTO designation, gray zone operations gave the IRGC further legitimacy as the protector of the Iranian Revolution. Gray zone operations made the IRGC more capable of guarding the regime against foreign interference and attacking its adversaries. Furthermore, the Iranian regime's successful gray zone campaign and ability to counter the United States made it a more attractive ally for other revisionist powers, such as Russia and China. Iran's gray zone operations demonstrated it is a credible threat and a reliable partner for countering the United States. The Iranian regime's survival is bolstered because it has become an attractive partner to other great powers seeking to change the status quo. By 2022, the Iranian regime survived the onslaught from the United States and its allies in large part due to its successful gray zone operations.

B. DETER AGGRESSION

Iranian gray zone operations from 2017–2022 deterred major aggression by the United States and its allies. There was no major conflict or large attack within Iran during this time. Iranian deterrence is based on convincing the United States and its allies that Iran would inflict high costs on its enemies in a major conflict.³⁹² Iranian gray zone operations demonstrated this capability and showed Iran holds the entire region's critical infrastructure, government buildings, military bases, and strategic waterways at risk. Iranian gray zone operations validated Iran's asymmetric warfare doctrine and the importance of ballistic missiles as a deterrent. The United States and its allies had ample military capability in the region to attack Iran directly, but did not due in part to the capabilities demonstrated by Iran's proxies and the IRGC. For example, despite the largest ballistic missile strike against U.S. forces in history, the United States did not retaliate even

³⁹² Bahgat and Ehteshami, *Defending Iran*, 12.

though the ballistic missiles were launched from inside Iran. Iran's gray zone operations retaliated against any coercive action by the United States and its allies, while also deterring the United States from initiating a large-scale conflict.

However, there are important caveats to Iranian gray zone operations' impact on Iranian deterrence. First it is important to recall that a prerequisite for gray zone operations is that the victim must already be executing a deterrence strategy and view war as a strategic defeat.³⁹³ In Iran's case, the United States was already deterred from major conflict before 2017, which allowed Iran to conduct gray zone operations in the first place. Furthermore, the United States and its allies also had no issues striking Iranian proxies outside Iran and often did in response to a lethal proxy attack—even willing to kill General Soleimani in Iraq. Israel was also an exception and was not deterred by Iranian gray zone operations from conducting attacks on Iranian shipping or covert attacks within Iran. Yet, the Iranian gray zone operations demonstrated to the United States that further escalation would be even costlier and thus maintained the deterrence established before 2017.

C. PROJECT POWER

Iranian gray zone operations' greatest impact was on Iran's objective to project power and reassert its leadership in the Middle East. Iran's proxies across the region are now "facts on the ground" and form major centers of power in Lebanon, Syria, Iraq, and Yemen.³⁹⁴ Iranian gray zone operations allowed it to maintain control of its "land bridge" from Tehran to Lebanon and its position as the dominant power in Lebanon and Iraq.³⁹⁵ Iran can now threaten strategic waterways from the eastern Mediterranean to the Indian Ocean with ASCMs, USVs, drones, sea mines, and hijacking. Iranian gray zone operations during this time demonstrated Iran's capability to hold critical petroleum infrastructure, key government buildings, and military bases at risk. Iranian gray zone operations demonstrated Iran can coordinate attacks with different proxies and across thousands of

³⁹³ Wirtz, "Life in the 'Gray Zone.'"

³⁹⁴ Vali Nasr, "All Against All," *Foreign Affairs* (New York, United Kingdom: Council on Foreign Relations NY, February 2022), <https://www.proquest.com/docview/2616233383/abstract/7E5BA952B0C2492CPQ/1>.

³⁹⁵ Nasr.

miles. Furthermore, Iran's non-lethal gray zone operations, such as cyberattacks, projected Iranian power into the cities of the continental United States. As a result of Iran's gray zone operations there is no place in the Middle East that is not in the weapons engagement zone of an Iranian proxy or the IRGC.

Iran's gray zone operations also increased its influence in the region. Despite harsh economic sanctions and military threats from the world's most powerful military, Iran did not retreat from the Middle East, but expanded its proxies and ballistic missile program. Although the United States is still present in the region and maintained its alliances with Iran's enemies, the United States' influence in the Middle East is arguably reduced since 2017. As a result of Iran's gray zone campaign the Trump Administration's maximum pressure campaign failed and Saudi Arabia's military campaign in Yemen has ground to halt, with the Houthis controlling the capital Sanaa.³⁹⁶ Even the 2022 CENTCOM Posture Statement admits there is a perception of U.S. disengagement and faltering influence in the Middle East.³⁹⁷ Iran's gray zone operations reduced the United States' ability to act in the region and Iran now controls the strategic initiative.

D. PROTECT THE HOMELAND

Iranian gray zone operations from 2017–2022 had a mixed impact on Iran's objective to protect the homeland and its allies. Iranian gray zone campaigns during this period often increased tensions in the region and caused the United States and its allies to attack Iran's proxies. Gray zone operations frequently invited retaliation where Iran's borders and sovereignty were temporarily violated. Israel in particular, regularly conducted airstrikes against the IRGC-QF and Iranian proxies in Syria and Iraq. Within Iran, Israel conducted assassinations, industrial sabotage, and cyberattacks—often as response to Iran's gray zone operations.³⁹⁸ Many of the proxies in Syria and Iraq, such as KH and AAH, were targeted by the United States and killed as a result of conducting lethal gray zone attacks. However, the Houthis and Assad regime benefitted from the protection of

³⁹⁶ Nasr.

³⁹⁷ McKenzie, "CENTCOM Posture Statement."

³⁹⁸ Nasr, "All Against All."

Iran's gray zone operations. Iran's gray zone operations helped the Houthis and Assad regime maintain their power and counter threats by Sunni powers. Overall Iran's territorial integrity and sovereignty were maintained but not as a major result of Iran's gray zone operations.

E. CONCLUSION

This thesis finds that in general, Iranian gray zone operations from 2017–2022 effectively advanced Iran's strategic objectives. Iran's objective to project power and gain influence in the Middle East received the greatest positive impact from gray zone operations. Although economically weaker, Iran withstood a great power, coerced regional rivals, and decreased its adversaries' ability to act in the region. Due to Iran's gray zone operations Iran is more influential throughout the Middle East and maintains the strategic initiative. Furthermore, Iran's asymmetric warfare doctrine and deterrence strategy was validated by its gray zone operations. Iranian gray zone operations demonstrated that a direct conflict with Iran would come at a high cost and threaten the stability of the whole region—effectively deterring the United States and its allies.

Secondly, this thesis finds the majority of Iran's gray zone operations were ad hoc and not necessarily tied to a specific strategic objective. Iran's gray zone operations were typically in retaliation to the United States and its allies, such as increased sanctions, cyberattacks, airstrikes, or the presence of additional U.S. military forces. Iran did have the strategic foresight to develop its gray zone capabilities, such as proxies, to use when retaliation was required. In addition, there were some instances where Iran did have a defined campaign to pressure the Saudi, Emirati, or American governments to make political decisions, such as leaving the region, agreeing to ceasefires, or removing sanctions. Overall, it does not appear that Iran had developed preplanned gray zone campaigns where one gray zone operation set conditions for another operation until an ultimate political objective was achieved.

Lastly, this thesis finds that Iranian gray zone operations had limited success. They did not force the United States to withdraw from Iraq or Syria. Nor did gray zone operations end Saudi and Emirati support for counter-Houthi forces in Yemen. Gray zone operations

also did not force any concessions from the Israelis or limit their ability to act in the region. The United States remains in Iraq and Syria, Saudi Arabia still supports counter-Houthi forces, and Israel regularly targets Iran. Despite Iran's overall success with gray zone operations, the United States and Israel remain the most powerful forces in the Middle East and Iran is far from becoming the dominant regional power.

V. CONCLUSION

Deterring Iranian aggression and protecting U.S. allies in the Middle East remains a strategic priority for President Joseph Biden and the U.S. government.³⁹⁹ The U.S. IC also identifies Iran as a major threat to U.S. interests and assesses Iran will continue to try to erode U.S. influence in the Middle East.⁴⁰⁰ The IC specifically identifies Iran's gray zone operations, such as unconventional warfare, cyberattacks, and proxy forces, as a threat to U.S. interests in the Middle East for the foreseeable future.⁴⁰¹ The purpose of this thesis was to determine how Iran conducts gray zone operations in the Middle East and analyze their effectiveness at obtaining Iran's strategic objectives since 2017. This thesis sought to answer the following question: *How effective have been Iran's gray zone operations at advancing its strategic objectives in the Middle East?* The following chapter provides a summary of the research and findings, discusses the implications of Iranian gray zone operations, and provides recommendations for future research.

A. SUMMARY OF RESEARCH

In Chapter I, this thesis conducted a literature review of scholarly books, journal articles, think-tank publications, news articles, and unclassified intelligence reports to understand the nature of gray zone operations, Iran's strategic goals, and where the two intersect. The two major themes of the literature were gray zone operations and Iran's grand strategy. The gray zone operation literature had three subthemes—definitions or characteristics of the gray zone, gray zone actors, and types of gray zone operations. The Iran grand strategy literature had two subthemes—Iran's strategic objectives and asymmetric warfare. The literature provided the four main strategic objectives of Iran for the thesis and the main types Iranian gray zone operations to evaluate for effectiveness.

³⁹⁹ Biden, *2022 National Security Strategy*, 11, 18, 42.

⁴⁰⁰ Office of the Director of National Intelligence, "2022 Annual Threat Assessment," 14–15.

⁴⁰¹ Office of the Director of National Intelligence, 14.

Chapter II analyzed lethal gray zone operations conducted by the Houthis and Iranian-backed Syrian and Iraqi Shia militias from 2017–2022. The chapter first analyzes the Houthi attacks, which primarily targeted Saudi Arabia and the United Arab Emirates. The Houthis, due to training and weapons supplied by the IRGC and LH, caused significant damage to critical petroleum infrastructure, airports, government buildings, military bases, and shipping. The Houthis used USVs, ASCMs, drones, naval mines, and ballistic missiles to conduct complex multi-axis multidomain attacks against mainly Saudi and Emirati targets. The second part analyzes the attacks by Iranian-backed Shia militias in Iraq and Syria against the United States, Israel, Saudi Arabia, and United Arab Emirates. Although using less sophisticated weapons than the Houthis, such as rockets, drones, and IEDs, the Syrian and Iraqi militias caused the most deaths to the United States. The month-by-month analysis showed Iran’s proxy attacks were often ad hoc and a response to developing political or military events. Lethal proxy gray zone operations showed there was nowhere in the Middle East Iran could not project power and hold its adversaries at risk.

Chapter III analyzed lethal and non-lethal gray zone operations conducted directly by Iran. Iran’s lethal gray zone operations occurred concurrently and sometimes in concert with the lethal proxy attacks in the previous chapter. Iran conducted several high-profile weapons tests, complex multi-axis attacks against Saudi petroleum infrastructure, a ballistic missile attack on U.S. forces in Iraq, and attacks against commercial shipping. The second part of the chapter analyzed the major non-lethal gray zone operations of cyber warfare, information operations, and economic coercion. Iranian cyber warfare was able to project Iranian power beyond the Middle East to U.S. cities, cause millions of dollars in damage, and steal the sensitive information of Iran’s adversaries. Iranian information operations were significant and reached millions of viewers, but it is difficult to assess if any of the IO campaigns changed target audiences’ opinions or impacted political decisions. Lastly, the chapter discusses the enormous economic costs Iran imposed on the U.S. and its allies as well as the small instances of direct economic coercion.

Chapter IV assessed the impact of gray operations on each of the four Iranian strategic objectives identified in Chapter I—regime survival, deter aggression, project power, and protect the homeland. The thesis found that Iranian gray zone operations

positively impacted regime survival, deterring aggression, and projecting power. However, gray zone operations had a mixed impact on protecting the homeland. The thesis answered the research question and found that, overall, Iranian gray zone operations effectively advanced Iran's strategic objectives. Lastly, the thesis found Iranian gray zone operations had limited success. The United States and Israel remained the most powerful forces in the Middle East and Iran was unable to become the dominant power in the region.

B. IMPLICATIONS OF IRANIAN GRAY ZONE OPERATIONS

1. Implications for U.S. Counter-Iran Campaigns in the Middle East

For Iran, gray zone operations worked—the United States may not have left the Middle East or removed sanctions, but Iran successfully stood up to a great power and its regional partners and allies. Iran's success means U.S. policy makers can expect Iran will continue to use gray zone operations as its primary way to change the status quo in the Middle East. U.S. policy makers should also expect an extensive Iranian gray zone campaign if the United States initiates another campaign to coerce Iranian policy. The last six years of gray zone operations also shows that a renewed U.S. campaign to coerce Iran, like the maximum pressure campaign, will fail. A new maximum pressure campaign will fail against Iran because, in the gray zone, Iran has more and cheaper tools than the United States. Iran has demonstrated it is not coerced by severe economic sanctions, the presence of a carrier strike group, strategic bombers, or U.S. troops. In addition, U.S. allies are also unwilling to endure another Iranian gray zone campaign and are already seeking détente with Iran.⁴⁰² Furthermore, Iran's successful showdown with the United States has made it an even more attractive partner for Russia and China. The next time around, Iran may have another great power at its back if the United States tries to coerce Iranian policy.

Iran's lethal reach stretches from the eastern Mediterranean to the Indian Ocean and its non-lethal reach to inside the United States. Any attempt to coerce Iran must take this into account. The United States cannot rely on the safety of international borders to mass

⁴⁰² Peter Baker, "Chinese-Brokered Deal Upends Mideast Diplomacy and Challenges U.S.," *The New York Times*, March 11, 2023, sec. U.S., <https://www.nytimes.com/2023/03/11/us/politics/saudi-arabia-iran-china-biden.html>.

forces or build up capacity while preparing for a strike on Iran. Even if the U.S. military tried to implement a “distributed force” to mitigate against an Iranian ballistic missile strike, like the one in Iraq in January 2020, Iran has a large, distributed proxy force that can use other means to strike U.S. troops anywhere in the Middle East. This means the U.S. military would need significant air defense systems, such as the counter-rocket, artillery, mortar (C-RAM) systems and Patriot batteries, at even the smallest bases for adequate force protection. Iran’s gray zone capabilities also mean that a seemingly isolated incident in Iraq or Syria could result in a response by Iran thousands of miles away—along a key shipping lane or a cyberattack against an American city. Without a doubt, if the United States wants to counter Iranian influence or bring Iran to the negotiating table it will have to develop a different strategy.

2. Implications for the U.S. Navy and Marine Corps

Iranian gray zone operations demonstrated Iran’s proxies on the eastern Mediterranean and Red Sea have given Iran a “fleet-in-being” capability. A fleet-in-being is a strategy used by an inferior navy to deny a stronger navy command of the sea through harassment and evasion.⁴⁰³ The inferior navy avoids direct engagement with the stronger navy, while still actively providing strategic effects at sea, such as attacking trade.⁴⁰⁴ Fleet-in-being strategies have been successful in the past, such as the French Navy in the 18th century and the German High Seas Fleet in World War One (WWI).⁴⁰⁵ The difference is Iran’s proxies can use armed USVs, ASCMs, drones, naval mines, and fast attack craft instead of capital ships. Although LH was not involved in the level of maritime attacks that the IRGCN and Houthis were from 2017–2022, they have demonstrated similar

⁴⁰³ Geoffrey Till, *Seapower: A Guide For the Twenty-First Century*, 3rd ed (New York, NY: Routledge, 2013), 173.

⁴⁰⁴ Till, 173.

⁴⁰⁵ Wayne P. Hughes and Robert Girrier, *Fleet Tactics and Naval Operations*, Third edition, The U.S. Naval Institute Blue & Gold Professional Library (Annapolis, Maryland: Naval Institute Press, 2018), 237; Till, *Seapower*, 162.

capabilities.⁴⁰⁶ If a conflict with the United States were to arise, Iran could “activate” its eastern Mediterranean and Red Sea fleets-in-being. The past six years of Iran’s maritime gray zone operations show they can attack commercial shipping hundreds of kilometers from their ports and challenge major trade routes. Should Iran implement a fleet-in-being strategy it means the U.S. Navy would have to expend its limited resources protecting shipping from the eastern Mediterranean to the Indian Ocean. This is the other purpose of a fleet-in-being strategy—drain the superior navy’s resources.⁴⁰⁷ The U.S. Navy already faces high operational tempos, crew shortages, and maintenance issues, which a fleet-in-being strategy could further degrade.⁴⁰⁸ Iranian proxy fleets-in-being in the eastern Mediterranean and Red Sea would also constrain the U.S. Navy’s freedom to act in other areas just as the German fleet did to the British Navy in WWI.⁴⁰⁹ Although not a “fleet” in the traditional sense, LH and the Houthis could challenge U.S. sea control with a fleet-in-being strategy using its unconventional fleet of armed USVs, fast attack craft, naval mines, drones, and ASCMs. Lastly, a fleet-in-being strategy would complement Iran’s asymmetric warfare doctrine, which emphasizes avoiding their adversaries’ conventional military advantages while exploiting their weaknesses.⁴¹⁰

For the U.S. Marine Corps, Iranian gray zone operations demonstrated that its historic role in the region, as the primary force used for non-combatant evacuation operations (NEOs), is seriously threatened. The Marine Corps has on several occasions deployed to Lebanon for NEOs and peacekeeping missions. As recently as 2006, Marine Expeditionary Units (MEUs) relied on the U.S. Navy’s sea control to land on Lebanese

⁴⁰⁶ Joshua C. Waddell, “Rethink the MEU for Tomorrow’s Expeditionary Operations,” *U.S. Naval Institute* 146, no. 4 (April 1, 2020), <https://www.usni.org/magazines/proceedings/2020/april/rethink-meu-tomorrows-expeditionary-operations>; Seth J. Frantzman, “The Vast Iran-Hezbollah Drone Threat Is Escalating – Analysis,” *The Jerusalem Post*, July 4, 2022, <https://www.jpost.com/middle-east/article-711029>.

⁴⁰⁷ Hughes and Girrier, *Fleet Tactics and Naval Operations*, 231.

⁴⁰⁸ Max Hauptman, “Sailors across Navy Say They’re Undermanned, Overworked and Using ‘Band Aids’ to Get Underway,” *Task & Purpose*, February 19, 2022, <https://taskandpurpose.com/news/navy-sailors-overworked-undermanned-maintenance/>.

⁴⁰⁹ Till, *Seapower*, 175.

⁴¹⁰ Bahgat and Ehteshami, *Defending Iran*, 6–7.

beaches near the U.S. embassy and evacuate Americans.⁴¹¹ MEUs also have a history in Yemen, when the 24th MEU evacuated U.S. embassy personnel, special operation forces, and Yemen's President Hadi to ships in the Gulf of Aden.⁴¹² As recent maritime gray zone operations have shown, both LH and the Houthis could seriously hamper any MEU's ability to conduct NEOs. Even if Marines avoid armed USVs, naval mines, or ASCMs, once ashore, they could face complex multi-axis attacks such as those seen throughout 2017–2022. It is not implausible for regional tensions to rise and for another MEU to be sent to evacuate Americans. However, this time LH or the Houthis can strike amphibious ships, ship-to-shore connectors, landing areas, or even the embassies themselves—all demonstrated by Iran's recent gray zone operations.

C. RECOMMENDATIONS FOR FURTHER RESEARCH

This thesis did not cover how Iran's nuclear activities, which some consider a part of Iran's gray zone tool kit, were used to coerce the United States.⁴¹³ Further study on when and why Iran increased uranium enrichment or violated certain aspects of the JCPOA would benefit the gray zone research area. In addition, further research is needed on how Iran paired increased nuclear activities with information operations to advance its strategic narrative. Another growing field in gray zone operations is space warfare. Iran already has developed space and counterpace capabilities, which could be used in gray zone operations.⁴¹⁴ Further research is needed on how Iran has or might use space warfare in gray zone operations. Lastly, further research is needed in discovering successful cases of countering gray zone campaigns so that counter-gray zone strategies can be developed.

⁴¹¹ Jad Mouawad and Steven Erlanger, "Marines Aiding Evacuation in Beirut; New Clash in South," *The New York Times*, July 20, 2006, sec. World, <https://www.nytimes.com/2006/07/20/world/middleeast/20cnd-mideast.html>.

⁴¹² Shawn Snow, "24th MEU Marines Supported the Evacuation and Movement of Yemen's President, Special Operations Forces in 2015," *Marine Corps Times*, August 29, 2019, <https://www.marinecorpstimes.com/news/your-marine-corps/2019/08/29/24th-meu-marines-supported-the-evacuation-and-movement-of-yemen-president-and-special-operations-forces-in-2015/>.

⁴¹³ Eisenstadt, "Iran's Gray Zone Strategy," 85.

⁴¹⁴ Ashley, *Iran Military Power*, 37.

LIST OF REFERENCES

- Abadi, Cameron. "Iran's Revolutionary Year." *Foreign Policy* (blog), December 25, 2022. <https://foreignpolicy.com/2022/12/25/iran-protest-revolution-2022-raisi-irgc/>.
- Al Jazeera. "Iranian Guards Claim Ballistic Missile Attacks in Erbil," March 13, 2022. <https://www.aljazeera.com/news/2022/3/13/missiles-hit-iraqs-kurdish-capital-no-casualties-officials>.
- Al Jazeera. "Saudi Arabia Says 'Booby-Trapped' Boat Destroyed off Yanbu Port," April 27, 2021. <https://www.aljazeera.com/news/2021/4/27/saudi-arabia-says-it-foiled-boat-attack-off-yanbu-port>.
- Al Jazeera. "Seized UK-Flagged Tanker Leaves Iranian Waters," September 27, 2019. <https://www.aljazeera.com/news/2019/9/27/seized-uk-flagged-tanker-stena-impero-leaves-iranian-port>.
- Al Jazeera. "Timeline: Houthis' Drone and Missile Attacks on Saudi Targets," September 14, 2019. <https://www.aljazeera.com/news/2019/9/14/timeline-houthis-drone-and-missile-attacks-on-saudi-targets>.
- Al Jazeera. "Yemen's Houthis Attack Saudi's Abha Airport, Injuring Civilians," July 2, 2019. <https://www.aljazeera.com/news/2019/7/2/yemens-houthis-attack-saudis-abha-airport-injuring-civilians>.
- Al Jazeera. "Yemen's Houthis Reject UN Call to Free UAE-Flagged Ship," January 16, 2022. <https://www.aljazeera.com/news/2022/1/16/houthis-reject-un-call-to-free-uae-flagged-ship>.
- Al Jazeera. "Yemen's Warring Sides Agree to Renew Existing Truce: UN," August 2, 2022. <https://www.aljazeera.com/news/2022/8/2/yemens-warring-sides-agree-to-renew-existing-truce-un>.
- Al Lawati, Abbas, and Nadeen Ebrahim. "The Battle of Narratives on Iran Is Being Fought on Social Media." CNN, October 5, 2022. <https://www.cnn.com/2022/10/05/middleeast/social-media-disinformation-mime-intl/index.html>.
- Anderson, Collin, and Karim Sadjadpour. "Iran's Cyber Threat: Espionage, Sabotage, and Revenge." Carnegie Endowment for International Peace, 2018. <http://www.jstor.org/stable/resrep26913>.

- AP News. “‘External Source’ Causes Oil Tanker Blast off Saudi Arabia.” Accessed January 15, 2023. <https://apnews.com/article/dubai-saudi-arabia-united-arab-emirates-jiddah-yemen-5493fe28dab563c4a457a325b20e3c62>.
- AP News. “Iran-Backed Militias Offer Truce for U.S. Pullout from Iraq,” April 26, 2021. <https://apnews.com/article/iran-us-news-baghdad-middle-east-iraq-f12d77bec74acefc7c4883eb30d832eb>.
- AP News. “Iran’s Army Test Fires Short-Range ‘smart’ Missile,” February 14, 2021. <https://apnews.com/article/tehran-iran-ad9f0bbe47a54853188c2252b54c199b>.
- AP News. “Protesters Attack U.S. Embassy in Baghdad after Airstrikes,” April 20, 2021. <https://apnews.com/article/us-news-ap-top-news-mark-esper-international-news-north-carolina-75228a8a607a44863b57021ac33264dc>.
- AP News. “US Commander Says More Work Needed to Counter Small Drones,” May 22, 2021. <https://apnews.com/article/donald-trump-middle-east-government-and-politics-e39fb650c283cc6e3962752e1d9e339b>.
- Ashley, Robert. *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance*. Washington, DC: Defense Intelligence Agency, 2019.
- Austin, Lloyd. *2022 National Defense Strategy*. Washington, DC: Department of Defense, 2022.
- Babb, Carla. “VOA Exclusive: CENTCOM Chief Says U.S. Can Do Job in Iraq with Fewer Forces.” VOA, July 15, 2020. https://www.voanews.com/a/middle-east_voa-exclusive-centcom-chief-says-us-can-do-job-iraq-fewer-forces/6192870.html.
- Bachner, Michael. “Israel Accuses Iran of Testing 2 Missiles This Year, Violating UNSC Resolution.” *The Times of Israel*, May 24, 2018. <https://www.timesofisrael.com/israel-accuses-iran-of-testing-2-missiles-this-year-violating-uns-c-resolution/>.
- Baezner, Marie. “Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions.” Application/pdf. ETH Zurich, May 2019. <https://doi.org/10.3929/ETHZ-B-000344841>.
- Bahgat, Gawdat, and Anoushiravan Ehteshami. *Defending Iran: From Revolutionary Guards to Ballistic Missiles*. Cambridge, United Kingdom ; New York, NY: Cambridge University Press, 2021.
- Baker, Peter. “Chinese-Brokered Deal Upends Mideast Diplomacy and Challenges U.S.” *The New York Times*, March 11, 2023, sec. U.S. <https://www.nytimes.com/2023/03/11/us/politics/saudi-arabia-iran-china-biden.html>.

- Barel, Ofir. "How Does Iran Wage Its Information Warfare Battle against Israel?" The Washington Institute, September 1, 2021. <https://www.washingtoninstitute.org/policy-analysis/how-does-iran-wage-its-information-warfare-battle-against-israel>.
- BBC News. "Netanyahu Blames Iran for Blast on Israeli-Owned Ship in Gulf of Oman," March 1, 2021. <https://www.bbc.com/news/world-middle-east-56237295>.
- BBC News. "Stena Impero: Seized British Tanker Leaves Iran's Waters," September 27, 2019. <https://www.bbc.com/news/world-middle-east-49849718>.
- Benmansour, Mohammed. "Yemen's Houthis Reach Saudi Capital with Missiles for First Time since COVID Ceasefire." Reuters, June 23, 2020. <https://www.reuters.com/article/us-yemen-security-saudi-idUSKBN23U0KA>.
- Bidar, Musadiq. "Facebook Says Iranian Hackers Targeted U.S. Military Personnel." CBS News, July 15, 2021. <https://www.cbsnews.com/news/facebook-iran-hackers-us-military-defense-contractors-fake-accounts/>.
- Biden, Joseph. *2022 National Security Strategy*. Washington, DC: The White House, 2022.
- Binnie, Jeremy. "Iran Unveils Kheibar Shekan Ballistic Missile." Janes, February 10, 2022. <https://www.janes.com/defence-news/news-detail/iran-unveils-kheibar-shekan-ballistic-missile>.
- Brewster, Thomas. "Big Leak Reveals Iran Targeting U.S. Military With Super Speedy Google Account Hacks." *Forbes*, June 16, 2020, sec. Cybersecurity. <https://www.forbes.com/sites/thomasbrewster/2020/07/16/big-leak-reveals-iran-targeting-us-military-with-super-speedy-google-account-hacks/>.
- Brooking, Emerson T, and Suzanne Kianpour. *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*. Washington, DC: Atlantic Council, 2020.
- Brumfiel, Geoff. "Iran Is Preparing A Launch. But Is It For A Space Rocket Or A Missile?" National Public Radio, January 14, 2019. <https://www.npr.org/2019/01/14/684467347/iran-is-preparing-a-launch-but-is-it-for-a-space-rocket-or-a-missile>.
- Brumfiel, Geoff. "Satellite Imagery Suggests 2nd Iranian Space Launch Has Failed." National Public Radio, February 6, 2019. <https://www.npr.org/2019/02/06/692071812/satellite-imagery-suggests-second-iranian-space-launch-has-failed>.

- Bryce, Robert. "Iran's Power over Iraq Includes Electricity." *The Hill*, January 9, 2020. <https://thehill.com/opinion/energy-environment/477371-irans-power-over-iraq-includes-electricity/>.
- Cavas, Christopher P. "New Houthi Weapon Emerges: A Drone Boat." *Defense News*, February 19, 2017, sec. IDEX. <https://www.defensenews.com/digital-show-dailies/idex/2017/02/19/new-houthi-weapon-emerges-a-drone-boat/>.
- CBS News. "Iran Says Ballistic Missile Capable of Hitting Ships Tested Successfully," March 9, 2017. <https://www.cbsnews.com/news/iran-ballistic-missile-capable-hitting-ships-test-launch/>.
- Chapman, John, ed. *Iran's Networks of Influence in the Middle East*. London, United Kingdom: International Institute for Strategic Studies, 2019.
- Cohen, Sagi. "It's Not an Israeli Site, It's Iranian Propaganda." Ynet, September 6, 2018. <https://www.ynet.co.il/articles/0,7340,L-5342357,00.html>.
- Cohen, Sam. "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests" 3, no. 1 (2019).
- Coles, Isabel, and Dion Nissenbaum. "U.S.: Saudi Pipeline Attacks Originated From Iraq." *Wall Street Journal*, June 28, 2019, sec. World. <https://www.wsj.com/articles/u-s-saudi-pipeline-attacks-originated-from-iraq-11561741133>.
- Crisis24. "Iraq: IED Attack Hits Logistical Convoy in Taji August 11," August 11, 2020. <https://crisis24.garda.com/alerts/2020/08/iraq-ied-attack-hits-logistical-convoy-in-taji-august-11>.
- Crist, David. *The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran*. New York: Penguin Press, 2012.
- Cyber and Infrastructure Security Agency. "Heightened Awareness for Iranian Cyber Activity," January 25, 2022. <https://www.cisa.gov/news-events/alerts/2020/12/03/heightened-awareness-iranian-cyber-activity>.
- Cyber and Infrastructure Security Agency. "Iran Cyber Threat Overview and Advisories." Accessed June 14, 2022. <https://www.cisa.gov/uscert/iran>.
- Cyber and Infrastructure Security Agency. "Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester," November 25, 2022. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a>.

- Cyber and Infrastructure Security Agency. “Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations,” September 14, 2022.
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-257a>.
- Dalton, Melissa G. “How Iran’s Hybrid-War Tactics Help and Hurt It.” *Bulletin of the Atomic Scientists* 73, no. 5 (September 3, 2017): 312–15.
<https://doi.org/10.1080/00963402.2017.1362904>.
- Diotte, Patrick. “The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online.” *Canadian Military Journal* 20, no. 4 (2020): 11.
- DW News. “Saudi Arabia: Houthi Attack Kills 2 in Jizan,” December 25, 2021.
<https://www.dw.com/en/saudi-arabia-houthi-attack-kills-2-in-jizan/a-60254504>.
- Echevarria, Antulio. “How Should We Think about ‘Gray-Zone’ Wars?” *Infinity Journal* 5, no. 1 (2015): 16–20. <https://www.militarystrategymagazine.com/article/how-should-we-think-about-gray-zone-wars/>.
- Eckstein, Megan. “Nimitz Carrier Strike Group to Return Home from Middle East Deployment.” USNI News, December 31, 2020.
<https://news.usni.org/2020/12/31/nimitz-carrier-strike-group-to-return-home-from-middle-east-deployment>.
- Eisenstadt, Michael. “Iran’s Gray Zone Strategy: Cornerstone of Its Asymmetric Way of War.” *Prism* 9, no. 2 (2021): 76–97. <https://www.jstor.org/stable/27008977?pq-origsite=summon>.
- El Gamal, Rania. “Saudi Arabia Halts Oil Exports in Red Sea Lane after Houthi Attacks.” Reuters, July 25, 2018. <https://www.reuters.com/article/us-yemen-security-idUSKBN1KF0XN>.
- Elkus, Adam. “50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense.” War on the Rocks, December 15, 2015. <https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/>.
- Embassy of the United Arab Emirates. *Returning the Houthis to the U.S. Terrorist List*. Washington, DC: Embassy of the United Arab Emirates, 2022.
- Eshel, Tamir. “Houthi’s New Naval Weapons Extend Their Reach 200 Nm into the Gulf of Aden.” *Defense Update*: (blog), September 26, 2022. https://defense-update.com/20220926_houthis-naval-weapons.html.
- Feely, Eric. “Militias Pivot Away from U.S. Targets, Toward Kurdistan and Turkish Bases.” The Washington Institute, October 17, 2022.
<https://www.washingtoninstitute.org/policy-analysis/militias-pivot-away-us-targets-toward-kurdistan-and-turkish-bases>.

- Fitzpatrick, Kitaneh, Johanna Moore, Zachary Coles, and Frederick W. Kagan. “Iran Crisis Update, October 28.” *Critical Threats*, October 28, 2022. <https://www.criticalthreats.org/analysis/iran-crisis-update-october-28>.
- France 24 News. “Rockets Hit near U.S. Embassy in Iraq as Tensions Flare,” December 20, 2020. <https://www.france24.com/en/live-news/20201220-rockets-hit-near-us-embassy-in-iraq-as-tensions-flare>.
- Frantzman, Seth J. “Five Times Iran Used Iraqi Militias to Conduct Drone Attacks – Analysis.” *The Jerusalem Post*, February 4, 2022. <https://www.jpost.com/middle-east/iran-news/article-695541>.
- Frantzman, Seth J. “The Vast Iran-Hezbollah Drone Threat Is Escalating – Analysis.” *The Jerusalem Post*, July 4, 2022. <https://www.jpost.com/middle-east/article-711029>.
- Freedman, Lawrence. *A Choice of Enemies America Confronts the Middle East*. Public Affairs, 2009.
- Guardian, The*. “Iran Claims Responsibility for Missile Strike near U.S. Consulate in Iraq.” March 13, 2022, sec. World news. <https://www.theguardian.com/world/2022/mar/13/iran-claims-responsibility-missile-strike-erbil-iraq-us-consulate>.
- Gibbons-Neff, Thomas. “How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria.” *New York Times* (Online). New York, United States: New York Times Company, May 24, 2018. <https://www.proquest.com/docview/2043078446/abstract/6F29F96A83D84254PQ/1>.
- Goldenberg, Ilan, Nicholas A Heras, Kaleigh Thomas, and Jennie Matuschak. *Countering Iran in the Gray Zone*. Washington, DC: Center for New American Security, 2020.
- Groll, Elias. “Cyberattack Targets Safety System at Saudi Aramco.” *Foreign Policy*, December 21, 2017. <https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/>.
- Gross, Judah Ari. “Air Force Chief: Iranians Fired 32 Rockets at Golan on May 10.” *The Times of Israel*, May 22, 2018. <https://www.timesofisrael.com/air-force-chief-iranians-fired-32-rockets-at-golan-on-may-10/>.
- Haiminis, Itay. “Iran’s Information Warfare.” In *The Cognitive Campaign: Strategic and Intelligence Perspectives*, edited by Yossi Kuperwasser and David Siman-Tov. Tel Aviv University: Institute for National Security Studies, 2019.

- Hamasaeed, Sarhang, and Garrett Nada. "Iraq Timeline: Since the 2003 War." United States Institute of Peace, May 29, 2020. <https://www.usip.org/iraq-timeline-2003-war>.
- Hassaniyan, Allan. "How Longstanding Iranian Disinformation Tactics Target Protests." The Washington Institute, November 1, 2022. <https://www.washingtoninstitute.org/policy-analysis/how-longstanding-iranian-disinformation-tactics-target-protests>.
- Hauptman, Max. "Sailors across Navy Say They're Undermanned, Overworked and Using 'Band Aids' to Get Underway." Task & Purpose, February 19, 2022. <https://taskandpurpose.com/news/navy-sailors-overworked-undermanned-maintenance/>.
- Haynes, Deborah. "Iran's Secret Cyber Files on How Cargo Ships and Petrol Stations Could Be Attacked." Sky News. Accessed March 28, 2023. <https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871>.
- Hicks, Kathleen H., John Schaus, and Michael Matlaga. *Zone Defense: Countering Competition in the Space between War and Peace*. Washington, DC: Center for Strategic and International Studies, 2018. <https://www.csis.org/features/zone-defense>.
- Hubbard, Ben, and Saeed Al-Batati. "Saudi Arabia Declares Cease-Fire in Yemen, Citing Fears of Coronavirus." *The New York Times*, April 8, 2020, sec. World. <https://www.nytimes.com/2020/04/08/world/middleeast/saudi-yemen-ceasefire-coronavirus.html>.
- Hughes, Wayne P., and Robert Girrier. *Fleet Tactics and Naval Operations*. Third edition. The U.S. Naval Institute Blue & Gold Professional Library. Annapolis, Maryland: Naval Institute Press, 2018.
- International Crisis Group. "Flashpoints: Iraq," December 14, 2017. <https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/iraq>.
- International Crisis Group. "Flashpoints: Middle Euphrates River Valley, Syria," December 14, 2017. <https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/middle-euphrates-river-valley>.
- International Crisis Group. "Tehran-U.S. Iran Trigger List," December 14, 2017. <https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/tehran>.
- International Institute for Strategic Studies. "Open-Source Analysis of Iran's Missile and UAV Capabilities and Proliferation," April 2021. <https://www.iiss.org/blogs/research-paper/2021/04/iran-missiles-uavs-proliferation>.

- Iran Primer, The. "Iran Attacks Kurdish Groups in Iraq," September 29, 2022.
<https://iranprimer.usip.org/blog/2022/sep/29/iran-attacks-kurdish-groups-iraq>.
- Iran Primer, The. "Iran Struggles with COVID-19 in 2020," December 16, 2020.
<https://iranprimer.usip.org/blog/2020/dec/16/iran-struggles-covid-19-2020>.
- Iran Primer, The. "Israel-Iran Conflict at Sea," April 14, 2021.
<https://iranprimer.usip.org/blog/2021/apr/14/israel-iran-conflict-sea>.
- Iran Primer, The. "Israel-Iran Cyber War, Gas Station Attack," November 2, 2021.
<https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack>.
- Iran Primer, The. "The Invisible U.S.-Iran Cyber War," October 25, 2019.
<https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war>.
- The Iran Primer. "Timeline of Military and Security Events," August 10, 2021.
<https://iranprimer.usip.org/resource/timeline-military-and-security-events>.
- Iran Primer, The. "U.S. Closes Consulate in Southern Iraq, Blames Iran," September 10, 2018. <https://iranprimer.usip.org/blog/2018/oct/03/us-closes-consulate-southern-iraq-blames-iran>.
- Iran Watch. "Iran Missile Milestones: 1985–2022," June 29, 2022.
<https://www.iranwatch.org/our-publications/weapon-program-background-report/iran-missile-milestones-1985-2022>.
- Islamic World News. "Detail of Ansar Allah Missile and Drone Attacks on Saudi Arabia," June 23, 2020. <https://english.iswnnews.com/13906/detail-of-ansar-allah-missile-and-drone-attacks-on-saudi-arbaia/>.
- Jay, Martin. "Saudi Arabia Looks for a Peace Deal in Yemen, but at What Price?" *Inside Arabia* (blog), April 2, 2020. <https://insidearabia.com/saudi-arabia-looks-for-a-peace-deal-in-yemen-but-at-what-price/>.
- Jones, Seth G, Jared Thompson, Danielle Ngo, Brian McSorley, and Joseph S Bermudez Jr. *The Iranian and Houthi War against Saudi Arabia*. Washington, DC: Center for Strategic and International Studies, 2021.
- Jordan, Javier. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict." *Journal of Strategic Security* 14, no. 1 (2020): 1–24. <https://www.jstor.org/stable/26999974>.
- Kaplan, Michael, and Catherine Herridge. "Army to Award Purple Hearts to 50 Soldiers Injured in Iran Missile Attack Following CBS News Investigation." CBS News, December 20, 2021. <https://www.cbsnews.com/news/purple-heart-iran-missile-attack-50-soldiers/>.

- Kapusta, Philip. *The Gray Zone*. MacDill AFB, FL: U.S. Special Operations Command, 2015. <https://info.publicintelligence.net/USSOCOM-GrayZones.pdf>.
- Kaushal, Sidharth. “Lessons from the Houthi Missile Attacks on the UAE.” Royal United Services Institute, February 3, 2022. <https://rusi.org/explore-our-research/publications/commentary/lessons-houthi-missile-attacks-uae>.
- Kenney, Caitlin M. “Iranian Navy Tries To Steal U.S. Unmanned Vessel At Sea.” *Defense One*, August 30, 2022. <https://www.defenseone.com/threats/2022/08/iranian-navy-tries-steal-us-unmanned-vessel-sea/376513/>.
- Knights, Michael. “Iran-Backed Militias Test the Credibility of Iraq’s Prime Minister.” *The Washington Institute*. Accessed January 24, 2023. <https://www.washingtoninstitute.org/policy-analysis/iran-backed-militias-test-credibility-iraqs-prime-minister>.
- Knights, Michael. “Kataib Hezbollah’s Role in the August 15 al-Tanf Attack.” *The Washington Institute*, August 25, 2022. <https://www.washingtoninstitute.org/policy-analysis/kataib-hezbollahs-role-august-15-al-tanf-attack>.
- Knights, Michael, and Crispin Smith. “Kataib Hezbollah Leads Drone Warfare Inside Iraq.” *The Washington Institute*, May 14, 2021. <https://www.washingtoninstitute.org/policy-analysis/kataib-hezbollah-leads-drone-warfare-inside-iraq>.
- Knights, Michael. “Making Sense of Militia Attacks in Iraq and Syria in Early 2022.” *The Washington Institute*, January 6, 2022. <https://www.washingtoninstitute.org/policy-analysis/making-sense-militia-attacks-iraq-and-syria-early-2022>.
- Knights, Michael, Crispin Smith, and Hamdi Malik. “Iran’s Proxies in Iraq Undertake the World’s Only Terrorist Attack Commemorating 9/11.” *The Washington Institute*. Accessed January 26, 2023. <https://www.washingtoninstitute.org/policy-analysis/irans-proxies-iraq-undertake-worlds-only-terrorist-attack-commemorating-911>.
- Lawlor, Katherine, and Nicholas Carl. “Iran File: Iranian Proxies Increase Attacks on U.S. Forces to Catalyze a U.S. Withdrawal from Iraq.” *Critical Threats*, July 9, 2021. <https://www.criticalthreats.org/briefs/iran-file/iranian-proxies-increase-attacks-on-us-forces-to-catalyze-a-us-withdrawal-from-iraq>.
- Loft, Philip. “Iran’s Influence in the Middle East.” *Research Briefing*. London, United Kingdom: United Kingdom House of Commons, June 2, 2023. <https://commonslibrary.parliament.uk/research-briefings/cbp-9504/>.

- Maltezou, Renee, and Jonathan Saul. "Iran Releases Two Greek Tankers Seized in May." Reuters, November 16, 2022. <https://www.reuters.com/world/greece-iran-agree-release-two-greek-tankers-seized-by-tehran-2022-11-16/>.
- Matlaga, Michael. "Case Study: Israel's Competition with Iran: 1991– 2015." Center for Strategic and International Studies, August 13, 2019. <https://www.csis.org/analysis/case-study-israels-competition-iran-1991-2015>.
- Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Advancing Strategic Thought Series. Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2015.
- Mazarr, Michael J., Joe Cheravitch, Jeffrey W. Hornung, and Stephanie Pezard. "What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression." RAND Corporation, April 19, 2021. https://www.rand.org/pubs/research_reports/RR3142.html.
- Mckenzie, Kenneth F. "CENTCOM Posture Statement." CENTCOM, March 15, 2022. <https://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/>.
- McMillan, Robert. "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years." The Wall Street Journal. Accessed March 28, 2023. <https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036>.
- Meredith, Sam. "Insurance Rates Have 'increased 10-Fold' after Attacks in the Strait of Hormuz, Shipping CEO Says." CNBC, July 9, 2019. <https://www.cnbc.com/2019/07/09/oil-insurance-rates-have-soared-since-tanker-attacks-near-iran.html>.
- Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security. "Iran-Linked DEV-0343 Targeting Defense, GIS, and Maritime Sectors." *Microsoft Security Blog* (blog), October 11, 2021. <https://www.microsoft.com/en-us/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/>.
- Miller, Joshua. "BadBlood: TA453 Targets U.S. & Israel in Credential Phishing | Proofpoint US." Proofpoint, March 30, 2021. <https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential>.
- Ministry of Foreign Affairs, Republic of Korea. "Issuance of Specific License by U.S. Office of Foreign Assets Control (OFAC) related to Compensation in Investor State Dispute Settlement (ISDS) with Dayyani Family." ROK Ministry of Foreign Press Releases, January 12, 2022. https://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=321975&page=1.

- Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War." RAND Corporation, June 27, 2019.
https://www.rand.org/pubs/research_reports/RR2942.html.
- Mouawad, Jad, and Steven Erlanger. "Marines Aiding Evacuation in Beirut; New Clash in South." *The New York Times*, July 20, 2006, sec. World.
<https://www.nytimes.com/2006/07/20/world/middleeast/20cnd-mideast.html>.
- Nada, Garrett, and Mattisan Rowan. "Part 2: Pro-Iran Militias in Iraq." Wilson Center, April 27, 2018. <https://www.wilsoncenter.org/article/part-2-pro-iran-militias-iraq>.
- Nasr, Vali. "All Against All." *Foreign Affairs*, New York, United Kingdom: Council on Foreign Relations NY, February 2022.
<https://www.proquest.com/docview/2616233383/abstract/7E5BA952B0C2492CPQ/1>.
- Nasrallah, Tawfiq. "Video: Saudi-Led Arab Coalition Intercepts Houthi Drones | Saudi – Gulf News." Gulf News, March 25, 2022.
<https://gulfnews.com/world/gulf/saudi/video-saudi-led-arab-coalition-intercepts-houthi-drones-1.1648228385136>.
- Newman, Lily Hay. "A Worldwide Hacking Spree Uses DNS Trickery to Nab Data." *Wired*. Accessed March 28, 2023. <https://www.wired.com/story/iran-dns-hijacking/>.
- Nissenbaum, Dion. "WSJ News Exclusive | Saudi Arabia, U.S. on High Alert After Warning of Imminent Iranian Attack." WSJ. Accessed December 9, 2022.
<https://www.wsj.com/articles/saudi-arabia-u-s-on-high-alert-after-warning-of-imminent-iranian-attack-11667319274>.
- Nuruzzaman, Mohammed. "President Trump's 'Maximum Pressure' Campaign and Iran's Endgame." *Strategic Analysis* 44, no. 6 (November 1, 2020): 570–82.
<https://doi.org/10.1080/09700161.2020.1841099>.
- Office of Public Affairs. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." U.S. Department of Justice, March 23, 2018. <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>.
- Office of Public Affairs. "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over \$30 Million in Losses." U.S. Department of Justice, November 28, 2018.
<https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public>.

- Office of the Director of National Intelligence. “2022 Annual Threat Assessment of the U.S. Intelligence Community.” ODNI. Accessed June 16, 2022.
<https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community>.
- Office of the Director of National Intelligence. *2023 Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2023.
- O’Rourke, Ronald. *Renewed Great Power Competition: Implications for Defense—Issues for Congress*. R43838. Washington, DC: Congressional Research Service. Accessed July 20, 2022.
<https://crsreports.congress.gov/product/details?prodcode=R43838>.
- Ostovar, Afshon. “Deterring Iran: Strategic Behavior and the Maritime Domain.” Technical. Monterey, California: Naval Postgraduate School, October 2022.
- Ostovar, Afshon. “Sectarianism and Iranian Foreign Policy.” In *Beyond Sunni and Shia*, by Afshon Ostovar, 87–112. Oxford University Press, 2018.
<https://doi.org/10.1093/oso/9780190876050.003.0005>.
- Ostovar, Afshon. “The Grand Strategy of Militant Clients: Iran’s Way of War.” *Security Studies* 28, no. 1 (2019): 159–88.
<https://doi.org/10.1080/09636412.2018.1508862>.
- Ostovar, Afshon. *Vanguard of the Imam: Religion, Politics, and Iran’s Revolutionary Guards*. New York, NY: Oxford University Press, 2016.
- Patel, Vedant. “Department Press Briefing – September 29, 2022.” United States Department of State, September 29, 2022.
<https://www.state.gov/briefings/departments-press-briefing-september-29-2022/>.
- Perlroth, Alan Blinder and Nicole. “A Cyberattack Hobbles Atlanta, and Security Experts Shudder.” CNBC, March 28, 2018. <https://www.cnbc.com/2018/03/28/a-cyberattack-hobbles-atlanta-and-security-experts-shudder.html>.
- Popp, George, and Sarah Canna. *The Characterization and Conditions of the Gray Zone*. Boston, MA: NSI Team, 2016. https://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTtA-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf.
- PressTV. “IRGC Warns Israel after Missile Strike on Mossad Bases in Erbil.” PressTV, March 13, 2022. <https://www.presstv.ir/Detail/2022/03/13/678473/Iran-IRGC-Missile-Attack-Israel-Erbil>.

- Price, Megan. "Taming the 'Grey Zone.'" RealClear Defense, December 9, 2021. https://www.realcleardefense.com/articles/2021/12/09/taming_the_grey_zone_807104.html.
- Reuters. "Factbox: Latest on Tanker Attacks South of Strait of Hormuz," June 13, 2019. <https://www.reuters.com/article/us-mideast-tankers-facts/latest-on-suspected-attacks-on-tankers-in-gulf-of-oman-idUSKCN1TE142>.
- Reuters. "Iran Says It Made Successful Submarine Missile Launch in Gulf War Games," February 24, 2019. <https://www.reuters.com/article/us-iran-gulf-wargames-idUSKCN1QD06S>.
- Reuters. "Israeli Officials Say Cargo Ship Possibly Attacked En Route to UAE- Israeli Media." Reuters, July 3, 2021. <https://www.reuters.com/world/middle-east/israeli-officials-say-cargo-ship-possibly-attacked-en-route-uae-israeli-n12-news-2021-07-03/>.
- Reuters. "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces," January 23, 2017. <https://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR>.
- Reuters. "U.S. Blames Iran for Helping Houthi Rebels Shoot down Drone in Yemen," June 16, 2019. <https://www.reuters.com/article/us-mideast-attacks-usa-drone-idUSKCN1TH0LA>.
- Reuters. "U.S. Blames Iran for Helping Houthi Rebels Shoot Down Drone in Yemen," June 16, 2019. <https://www.reuters.com/article/us-mideast-attacks-usa-drone/us-blames-iran-for-helping-houthi-rebels-shoot-down-drone-in-yemen-idUSKCN1TH0LA>.
- Rugge, Fabio. *Confronting an "Axis of Cyber"?* IT: Ledizioni, 2018. <https://doi.org/10.14672/67058655>.
- Sharp, Jeremy. *Yemen: Civil War and Regional Intervention*. Washington, DC: Congressional Research Service, 2021.
- Sharp, Jeremy M., and Carla E Humud. *Attacks Against the United Arab Emirates: Issues for Congress*. Washington, DC: Congressional Research Service, 2022.
- Shelbourne, Mallory. "Iran Temporarily Captures Two U.S. Saildrones in Red Sea." USNI News, September 2, 2022. <https://news.usni.org/2022/09/02/iran-temporarily-captures-two-u-s-saildrones-in-red-sea>.
- Smith, Crispin. "Militia Propaganda Around the Attack on Al-Tanf." The Washington Institute, October 22, 2021. <https://www.washingtoninstitute.org/policy-analysis/militia-propaganda-around-attack-al-tanf>.

- Smith, Crispin, and Hamdi Malik. “The Muqawama Are Focusing Attack Claims on U.S. Bases in Syria.” The Washington Institute. Accessed January 26, 2023.
<https://www.washingtoninstitute.org/policy-analysis/muqawama-are-focusing-attack-claims-us-bases-syria>.
- Snow, Shawn. “24th MEU Marines Supported the Evacuation and Movement of Yemen’s President, Special Operations Forces in 2015.” Marine Corps Times, August 29, 2019. <https://www.marinecorpstimes.com/news/your-marine-corps/2019/08/29/24th-meu-marines-supported-the-evacuation-and-movement-of-yemen-president-and-special-operations-forces-in-2015/>.
- Stanford University. “Mapping Militants Profiles: Asa’ib Ahl al-Haq,” July 2018.
<https://cisac.fsi.stanford.edu/mappingmilitants/profiles/asaib-ahl-al-haq>.
- Stanford University. “Mapping Militants Profiles: Kata’ib Hezbollah,” September 2020.
<https://cisac.fsi.stanford.edu/mappingmilitants/profiles/kataib-hezbollah>.
- Starr, Barbara. “Saudi Arabia Has Paid \$500M toward the Cost of U.S. Troops in Country.” CNN, January 16, 2020.
<https://www.cnn.com/2020/01/16/politics/saudi-arabia-us-troops-payment/index.html>.
- “Statement of General Joseph L. Votel, U.S. Army Commander United States Special Operations Command Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities.” Washington, DC, March 18, 2015.
- Stoker, Donald, and Craig Whiteside. “Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking.” *Naval War College Review* 73, no. 1 (2020): 12–48. <http://www.jstor.org/stable/26868211>.
- Stubbs, Jack, and Christopher Bing. “Exclusive: Iran-Linked Hackers Recently Targeted Coronavirus Drugmaker Gilead – Sources.” Reuters, May 8, 2020.
<https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV>.
- Stubbs, Jack, and Tuqa Khalid. “Fake News Network vs. Bots: The Online War around Khashoggi Killing.” Reuters, November 1, 2018.
<https://www.reuters.com/article/us-saudi-khashoggi-disinformation-idUSKCN1N63QF>.
- Sutton, H. I. “Disguised Explosive Boat May Be New Threat To Tankers Off Yemen.” *Forbes*, March 4, 2020, sec. Aerospace & Defense.
<https://www.forbes.com/sites/hisutton/2020/03/04/new-disguised-explosive-boat-may-threaten-tankers-off-yemen/>.

- Tabatabai, Ariane M. *No Conquest, No Defeat: Iran's National Security Strategy*. New York: Oxford University Press, 2020.
- Taleblu, Behnam. "Collecting and Analyzing Shiite Militia Attacks against the U.S. Presence in Iraq." *Foundation for Defense of Democracies Long War Journal*, May 5, 2020. <https://www.longwarjournal.org/archives/2020/05/collecting-and-analyzing-shiite-militia-attacks-against-the-u-s-presence-in-iraq.php>.
- Theohary, Catherine A. *Iranian Offensive Cyberattack Capabilities*. Washington, DC: Congressional Research Service, 2020. <https://crsreports.congress.gov/product/pdf/IF/IF11406/2>.
- Till, Geoffrey. *Seapower: A Guide For the Twenty-First Century*. 3rd ed. New York, NY: Routledge, 2013.
- Times of Israel. The. "Iranian Hackers Publish CCTV Footage, Workers' Details from Haifa, Ashdod Ports," February 23, 2022. <https://www.timesofisrael.com/iranian-hackers-publish-cctv-footage-workers-details-from-haifa-ashdod-ports/>.
- United Against Nuclear Iran. "The Iranian Cyber Threat Structure," September 2022. <https://www.unitedagainstnucleariran.com/iranian-cyber-threat-structure>.
- United States Department of State. "Country Reports on Terrorism 2020: Saudi Arabia." Accessed January 17, 2023. <https://www.state.gov/reports/country-reports-on-terrorism-2020/saudi-arabia/>.
- U.S. Central Command. "CENTCOM Forces Respond to Attempted Coordinated Rocket Attacks at Conoco, Green Village Ba." Accessed October 20, 2022. <https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/3138816/centcom-forces-respond-to-attempted-coordinated-rocket-attacks-at-conoco-green/https%3A%2F%2Fwww.centcom.mil%2FMEDIA%2FPRESS-RELEASES%2FPress-Release-View%2FArticle%2F3138816%2Fcentcom-forces-respond-to-attempted-coordinated-rocket-attacks-at-conoco-green%2F>.
- U.S. Central Command. "Iranian UAV Attack Against MOTOR TANKER MERCER STREET." MacDill AFB, FL: U.S. Central Command, August 6, 2021. <https://www.centcom.mil/Portals/6/PressReleases/MERCERSTREETATTACK06AUG2%20final.pdf>.
- U.S. Cyber Command. "Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks," February 24, 2022. <https://www.cybercom.mil/Media/News/Article/2945592/iranian-government-sponsored-actors-conduct-cyber-operations-against-global-gov/>.

- U.S. Department of Defense. “DOD Statement on Rocket Attack at Al Asad by Pentagon Press Secretary John F. Kirby.” Accessed January 25, 2023.
<https://www.defense.gov/News/Releases/Release/Article/2522600/dod-statement-on-rocket-attack-at-al-asad-by-pentagon-press-secretary-john-f-ki/>
<https://www.defense.gov/News/Releases/Release/Article/2522600/dod-statement-on-rocket-attack-at-al-asad-by-pentagon-press-secretary-john-f-ki/>
- Votel, Joseph L, Charles T Cleveland, Charles T Connett, and Will Irwin. “Unconventional Warfare in the Gray Zone.” *Joint Force Quarterly*, no. 80 (2016): 101–9.
- Waddell, Joshua C. “Rethink the MEU for Tomorrow’s Expeditionary Operations.” *U.S. Naval Institute* 146, no. 4 (April 1, 2020).
<https://www.usni.org/magazines/proceedings/2020/april/rethink-meu-tomorrows-expeditionary-operations>.
- Wamsley, Laurel. “State Department Orders Nonessential U.S. Government Employees Out Of Iraq.” National Public Radio, May 15, 2019.
<https://www.npr.org/2019/05/15/723466550/state-department-orders-non-emergency-u-s-government-employees-out-of-iraq>.
- Weaver, John. *The U.S. Cybersecurity and Intelligence Analysis Challenges*. York, PA: Palgrave Macmillan, 2022.
- Williams, Ian, and Shaan Shaikh. *The Missile War in Yemen*. Washington, DC: Center for Strategic and International Studies, 2020.
- Winter, Chase. “US Lt. Gen: Yemen’s Missiles Have ‘Iranian Markings.’” DW News, November 10, 2017. <https://www.dw.com/en/us-air-force-missiles-fired-at-saudi-arabia-from-yemen-have-iranian-markings/a-41333618>.
- Wintour, Patrick, and Patrick Wintour Diplomatic editor. “Iran Releases South Korean Tanker Seized in January.” *The Guardian*, April 9, 2021, sec. World news.
<https://www.theguardian.com/world/2021/apr/09/iran-releases-south-korean-tanker-seized-in-january-oil-revenue-us-sanctions>.
- Wirtz, James J. “Life in the ‘Gray Zone’: Observations for Contemporary Strategists.” *Defense & Security Analysis* 33, no. 2 (April 3, 2017): 106–14.
<https://doi.org/10.1080/14751798.2017.1310702>.
- Yaakoubi, Aziz El, and Maha El Dahan. “Saudi Aramco Petroleum Storage Site Hit by Houthi Attack, Fire Erupts.” Reuters, March 26, 2022.
<https://www.reuters.com/world/middle-east/saudi-air-defences-destroy-houthi-drones-state-tv-2022-03-25/>.

Zimmerman, Katherine. *Yemen's Houthis and the Expansion of Iran's Axis of Resistance*. Washington, DC: American Enterprise Institute for Public Policy Research, 2022.

Zimmerman, Katherine. "Yemen's Houthis and the Expansion of Iran's Axis of Resistance." *Critical Threats*, March 14, 2022.
<https://www.criticalthreats.org/analysis/yemens-houthis-and-the-expansion-of-irans-axis-of-resistance>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

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



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE