



# NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

## THESIS

**THE INTEGRATION OF SPECIAL OPERATIONS  
AND ADVANCED TECHNOLOGY: AN ANALYSIS  
OF ITS ENABLING CONDITIONS AND OUTCOMES**

by

Xingyu Louis Liao

June 2023

Thesis Advisor:  
Second Reader:

Ben Gans  
Kevin D. Jones

**Approved for public release. Distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                 |                                                                |                                                            |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------|--|
| <b>REPORT DOCUMENTATION PAGE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                | <i>Form Approved OMB<br/>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                 |                                                                |                                                            |  |
| <b>1. AGENCY USE ONLY<br/>(Leave blank)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                 | <b>2. REPORT DATE</b><br>June 2023                             | <b>3. REPORT TYPE AND DATES COVERED</b><br>Master's thesis |  |
| <b>4. TITLE AND SUBTITLE</b><br>THE INTEGRATION OF SPECIAL OPERATIONS AND ADVANCED TECHNOLOGY: AN ANALYSIS OF ITS ENABLING CONDITIONS AND OUTCOMES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                 |                                                                | <b>5. FUNDING NUMBERS</b>                                  |  |
| <b>6. AUTHOR(S)</b> Xingyu Louis Liao                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                 |                                                                |                                                            |  |
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br>Naval Postgraduate School<br>Monterey, CA 93943-5000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                 |                                                                | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>            |  |
| <b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                 |                                                                | <b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>    |  |
| <b>11. SUPPLEMENTARY NOTES</b> 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                 |                                                                |                                                            |  |
| <b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b><br>Approved for public release. Distribution is unlimited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 |                                                                | <b>12b. DISTRIBUTION CODE</b><br>A                         |  |
| <b>13. ABSTRACT (maximum 200 words)</b><br><p>Special Operations (SO) has become increasingly relevant in contemporary warfare due to its ability to create strategic options and efficient use of resources for policymakers. Rapid advancements in technology from the commercial sector provide significant opportunities for military forces in modern warfare. The lack of research on integrating advanced technology with SO has limited its potential for progression, however. Therefore, this thesis aimed to explore the integration of advanced technology into SO missions to maximize their effectiveness and reduce risk. A comparative case study was conducted to analyze the integration of advanced technology with SO from three operations that employed three different actors in three different domains: Operation Olympic Games, Operation Orchard, and Operation Ocean Shield. The study found that three critical enabling conditions—purpose, integration effort, and compatibility—were necessary for successful integration. Such integration produced a positive synergistic outcome that could significantly reduce risk to forces and missions and/or increase the effectiveness of the mission. The conceptual model derived from this research could help policymakers, military commanders, and technological partners improve their decision-making processes when integrating advanced technology into SO missions.</p> |                                                                 |                                                                |                                                            |  |
| <b>14. SUBJECT TERMS</b><br>Special Operations, advanced technology, effectiveness, risk, system theory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                 |                                                                | <b>15. NUMBER OF PAGES</b><br>139                          |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                 |                                                                | <b>16. PRICE CODE</b>                                      |  |
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>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.**

**THE INTEGRATION OF SPECIAL OPERATIONS AND ADVANCED  
TECHNOLOGY: AN ANALYSIS OF ITS ENABLING CONDITIONS AND  
OUTCOMES**

Xingyu Louis Liao  
Major, Republic of Singapore Navy  
BME, National University of Singapore, 2011

Submitted in partial fulfillment of the  
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2023**

Approved by: Ben Gans  
Advisor

Kevin D. Jones  
Second Reader

Carter Malkasian  
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

## ABSTRACT

Special Operations (SO) has become increasingly relevant in contemporary warfare due to its ability to create strategic options and efficient use of resources for policymakers. Rapid advancements in technology from the commercial sector provide significant opportunities for military forces in modern warfare. The lack of research on integrating advanced technology with SO has limited its potential for progression, however. Therefore, this thesis aimed to explore the integration of advanced technology into SO missions to maximize their effectiveness and reduce risk. A comparative case study was conducted to analyze the integration of advanced technology with SO from three operations that employed three different actors in three different domains: Operation Olympic Games, Operation Orchard, and Operation Ocean Shield. The study found that three critical enabling conditions—purpose, integration effort, and compatibility—were necessary for successful integration. Such integration produced a positive synergistic outcome that could significantly reduce risk to forces and missions and/or increase the effectiveness of the mission. The conceptual model derived from this research could help policymakers, military commanders, and technological partners improve their decision-making processes when integrating advanced technology into SO missions.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

|             |                                                                                             |           |
|-------------|---------------------------------------------------------------------------------------------|-----------|
| <b>I.</b>   | <b>INTRODUCTION.....</b>                                                                    | <b>1</b>  |
| <b>A.</b>   | <b>INTRODUCTION.....</b>                                                                    | <b>1</b>  |
| <b>B.</b>   | <b>GAPS.....</b>                                                                            | <b>5</b>  |
| <b>C.</b>   | <b>RESEARCH QUESTION AND OBJECTIVES .....</b>                                               | <b>6</b>  |
| <b>D.</b>   | <b>RESEARCH DESIGN AND DATA COLLECTION.....</b>                                             | <b>7</b>  |
| 1.          | <b>Research Design .....</b>                                                                | <b>7</b>  |
| 2.          | <b>Data Collection .....</b>                                                                | <b>8</b>  |
| <b>E.</b>   | <b>LIMITATIONS.....</b>                                                                     | <b>9</b>  |
| <b>F.</b>   | <b>THESIS OUTLINE.....</b>                                                                  | <b>9</b>  |
| <br>        |                                                                                             |           |
| <b>II.</b>  | <b>THEORETICAL FRAMEWORK AND CONCEPTUAL MODEL .....</b>                                     | <b>11</b> |
| <b>A.</b>   | <b>INTRODUCTION.....</b>                                                                    | <b>11</b> |
| <b>B.</b>   | <b>LITERATURE REVIEW .....</b>                                                              | <b>11</b> |
| 1.          | <b>Special Operations .....</b>                                                             | <b>11</b> |
| 2.          | <b>Advanced Technology.....</b>                                                             | <b>15</b> |
| 3.          | <b>System Theory .....</b>                                                                  | <b>18</b> |
| <b>C.</b>   | <b>CONCEPTUAL MODEL .....</b>                                                               | <b>21</b> |
| 1.          | <b>Potential Synergy .....</b>                                                              | <b>22</b> |
| 2.          | <b>Enabling Conditions .....</b>                                                            | <b>22</b> |
| 3.          | <b>Emergent Capability.....</b>                                                             | <b>23</b> |
| 4.          | <b>Realized Synergy .....</b>                                                               | <b>23</b> |
| <b>D.</b>   | <b>RELATING CONCEPTUAL MODEL TO CASE STUDIES .....</b>                                      | <b>24</b> |
| <br>        |                                                                                             |           |
| <b>III.</b> | <b>OPERATION OLYMPIC GAMES .....</b>                                                        | <b>25</b> |
| <b>A.</b>   | <b>INTRODUCTION.....</b>                                                                    | <b>25</b> |
| <b>B.</b>   | <b>BACKGROUND .....</b>                                                                     | <b>26</b> |
| <b>C.</b>   | <b>PLANNING AND EXECUTION .....</b>                                                         | <b>29</b> |
| 1.          | <b>Stuxnet .....</b>                                                                        | <b>29</b> |
| 2.          | <b>Covert Operation .....</b>                                                               | <b>29</b> |
| <b>D.</b>   | <b>ANALYSES .....</b>                                                                       | <b>36</b> |
| 1.          | <b>Integration of Special Operations and Advanced Military<br/>        Technology .....</b> | <b>37</b> |
| 2.          | <b>Enabling Conditions .....</b>                                                            | <b>38</b> |
| 3.          | <b>Outcomes .....</b>                                                                       | <b>40</b> |
| <b>E.</b>   | <b>CONCLUSION .....</b>                                                                     | <b>42</b> |

|            |                                                                                      |           |
|------------|--------------------------------------------------------------------------------------|-----------|
| <b>IV.</b> | <b>OPERATION ORCHARD.....</b>                                                        | <b>45</b> |
| <b>A.</b>  | <b>INTRODUCTION.....</b>                                                             | <b>45</b> |
| <b>B.</b>  | <b>BACKGROUND .....</b>                                                              | <b>46</b> |
| <b>C.</b>  | <b>PLANNING AND EXECUTION .....</b>                                                  | <b>52</b> |
|            | 1. The Hotel Raid on Ibrahim Othman by Mossad .....                                  | 52        |
|            | 2. The Soil Sample Collection in the Vicinity of al-Kibar by<br>Sayeret Matkal ..... | 53        |
|            | 3. The Airstrike on al-Kibar by Raam and Sufa Supported<br>by EW Technology .....    | 54        |
| <b>D.</b>  | <b>ANALYSES .....</b>                                                                | <b>58</b> |
|            | 1. Integration of Special Operations and Advanced<br>Technology .....                | 59        |
|            | 2. Enabling Conditions .....                                                         | 60        |
|            | 3. Outcomes .....                                                                    | 62        |
| <b>E.</b>  | <b>CONCLUSION .....</b>                                                              | <b>63</b> |
| <b>V.</b>  | <b>OPERATION OCEAN SHIELD.....</b>                                                   | <b>65</b> |
| <b>A.</b>  | <b>INTRODUCTION.....</b>                                                             | <b>65</b> |
| <b>B.</b>  | <b>BACKGROUND .....</b>                                                              | <b>66</b> |
| <b>C.</b>  | <b>PLANNING AND EXECUTION .....</b>                                                  | <b>71</b> |
|            | 1. Task Force Barracuda.....                                                         | 72        |
|            | 2. Concept of Operation .....                                                        | 73        |
|            | 3. Threats .....                                                                     | 74        |
|            | 4. Enhancement to Operation .....                                                    | 75        |
|            | 5. Challenges.....                                                                   | 79        |
| <b>D.</b>  | <b>ANALYSES .....</b>                                                                | <b>80</b> |
|            | 1. Integration of Special Operations and Advanced<br>Technology .....                | 81        |
|            | 2. Enabling Conditions .....                                                         | 83        |
|            | 3. Outcomes .....                                                                    | 86        |
| <b>E.</b>  | <b>CONCLUSION .....</b>                                                              | <b>88</b> |
| <b>VI.</b> | <b>CONCLUSIONS AND RECOMMENDATIONS.....</b>                                          | <b>89</b> |
| <b>A.</b>  | <b>SUMMARY OF KEY FINDINGS .....</b>                                                 | <b>89</b> |
|            | 1. Integration between Special Operations and Advanced<br>Technology .....           | 89        |
|            | 2. Enabling Conditions .....                                                         | 90        |
|            | 3. Outcomes .....                                                                    | 91        |
| <b>B.</b>  | <b>IMPLICATIONS AND RECOMMENDATIONS.....</b>                                         | <b>92</b> |

|                                              |                                 |     |
|----------------------------------------------|---------------------------------|-----|
| 1.                                           | Conceptual .....                | 92  |
| 2.                                           | Organizational .....            | 93  |
| 3.                                           | Doctrinal .....                 | 93  |
| C.                                           | AREAS FOR FUTURE RESEARCH ..... | 93  |
| D.                                           | CONCLUSION .....                | 94  |
| APPENDIX A. INTERVIEW PROTOCOL .....         |                                 | 95  |
| APPENDIX B. LIST OF INTERVIEWEES .....       |                                 | 97  |
| APPENDIX C. SAMPLE INTERVIEW TRANSCRIPT..... |                                 | 99  |
| APPENDIX D. CONTENT ANALYSIS .....           |                                 | 103 |
| LIST OF REFERENCES .....                     |                                 | 107 |
| INITIAL DISTRIBUTION LIST .....              |                                 | 115 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

|           |                                                                                                        |    |
|-----------|--------------------------------------------------------------------------------------------------------|----|
| Figure 1. | Overview of Thesis .....                                                                               | 10 |
| Figure 2. | Conceptual Model for Synergistic Relationship between Special Operations and Advanced Technology ..... | 22 |
| Figure 3. | Number of Attacks by Somali Pirates (2003–2010) .....                                                  | 68 |
| Figure 4. | Number of Attacks by Somali Pirates (2008–2018) .....                                                  | 70 |
| Figure 5. | Concept of Operation of Task Force Barracuda .....                                                     | 74 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

|          |                                                                                                   |    |
|----------|---------------------------------------------------------------------------------------------------|----|
| Table 1. | Summary of Integration Between Special Operations and Technology in Operation Olympic Games ..... | 37 |
| Table 2. | Qualifying Operation Olympic Games as Special Operations .....                                    | 37 |
| Table 3. | Summary of Integration Between Special Operations and Technology in Operation Orchard .....       | 59 |
| Table 4. | Qualifying Airstrike Conducted by Raam and Sufa as Special Operations .....                       | 59 |
| Table 5. | Core Elements for Special Operations Task Unit .....                                              | 72 |
| Table 6. | Comparison between Command Detonation and Time-Delayed Detonation.....                            | 77 |
| Table 7. | Summary of Integration Between Special Operations and Technology in OOS .....                     | 81 |
| Table 8. | Qualifying Operations Conducted by Task Force Barracuda as Special Operations .....               | 82 |
| Table 9. | Qualifying Technology Used by Task Force Barracuda as Advanced Technology .....                   | 83 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS AND ABBREVIATIONS

|          |                                                    |
|----------|----------------------------------------------------|
| AI       | Artificial intelligence                            |
| AO       | Area of operations                                 |
| EUNAVFOR | European Union Naval Force                         |
| EW       | Electronic warfare                                 |
| HQ       | Headquarters                                       |
| IADS     | Integrated air defense system                      |
| IAEA     | International Atomic Energy Agency                 |
| IAF      | Israeli Air Force                                  |
| IDF      | Israel Defense Forces                              |
| ISIS     | Institute for Science and Security                 |
| NATO     | North Atlantic Treaty Organization                 |
| NCRI     | National Council of Resistance of Iran             |
| OOS      | Operation Ocean Shield                             |
| OPSEC    | Operations security                                |
| PLCs     | Programmable logic controllers                     |
| RHIBS    | Rigid hull inflatable boats                        |
| SAM      | surface-to-air missile                             |
| SLC      | <i>siluro a lenta corsa</i> (slow-running torpedo) |
| SO       | Special Operations                                 |
| SOF      | Special Operations Forces                          |
| TF       | Task force                                         |
| TTP      | Tactics, techniques, and procedures                |
| UN       | United Nations                                     |
| UNSC     | United Nation Security Council                     |
| U.S.     | United States                                      |

THIS PAGE INTENTIONALLY LEFT BLANK

## EXECUTIVE SUMMARY

Special Operations (SO) are inherently risky and specialized, requiring high levels of expertise, precision, and quick decision making. Hence, it is always in the interest of policymakers and military leaders to invest, research, and innovate to develop new methods of increasing SO effectiveness and at the same time reducing the risk of SO missions. While SO missions have often incorporated advanced technology into their operations, the lack of formal research into this area has limited its potential for more widespread use in SO missions.

This thesis explored the relationship between SO and advanced technology. The primary objectives were to identify the conditions that have enabled the integration of advanced technology into SO thus far, to evaluate the effectiveness and risk of missions that have incorporated advanced technology, and to develop a conceptual model that summarizes the research findings with the goal of improving decision making by policymakers, military commanders, and technological partners.

To investigate this topic, an unclassified, comparative case study was conducted analyzing the integration of advanced technology with SO. Data was collected from open-source literature and the author's interviews. A conceptual model, based on well-researched system theory, was adapted and refined to encapsulate the results of the research.

SO are typically well-resourced, and the units conducting them are open to adapting new technology. The successful integration of advanced technology and SO requires three critical enabling conditions—purpose, integration effort, and compatibility—which work synergistically to achieve optimal results. Purpose can be seen as having clear understanding of course of action and objectives. Compatibility refers to the technical feasibility of two components to interact and form a relationship. Integration effort refers to the willingness of policymakers or military commanders to integrate SO and advanced technology. The assessment of the synergistic outcome involves evaluating the effectiveness and risk of the mission and forces involved.

The research focused on three case studies from three operations that employed three different actors in three different domains—Operation Olympic Games, Operation Orchard, and Operation Ocean Shield (OOS)—to analyze the integration of advanced technology into SO.

Operation Olympic Games was a covert operation planned and executed by American and Israeli forces to delay Iran’s nuclear program by using cyberattacks to sabotage uranium enrichment in Iran’s Natanz facilities. This operation involved the deployment of a computer worm, Stuxnet, which targeted the codes of programmable logic controllers (PLCs) and caused approximately 1,000 centrifuges to spin out of control at the enrichment facility. This integration of cyberattack with covert operation fulfilled all three enabling conditions to a high degree, especially in the area of integration effort. Multiple entities—including intelligence, material engineers, and nuclear scientists—collaborated and supported the coders with critical information that was required to design and test the worm. The integration of an advanced cyberattack with SO in Operation Olympic Games was assessed to produce a positive synergistic outcome despite criticisms that the worm had spread to public computers worldwide and resulted in the attribution to United States and Israel.

Operation Orchard was an airstrike coupled with electronic warfare (EW) conducted by Israeli forces to destroy Syria’s nuclear reactor in a secluded area near al-Kibar in the Deir ez-Zor province. The mission’s key objective was to maintain a low signature and deny the destruction of a high-value nuclear reactor to prevent the outbreak of war. The EW technology that manipulated Syria’s integrated air defense system proved to be highly effective in supporting the airstrike mission to achieve this objective. The integration of the high-end airstrike and advanced EW technology in Operation Orchard was a textbook example of a highly synergistic outcome. It met all the enabling conditions and significantly reduced risk to the force and mission while enhancing effectiveness. Overall, Operation Orchard was a great success.

The third case study, OOS, was based on the author’s interviews with operators who were involved in the operation. The study focus was on Task Force (TF) Barracuda, operating under the jurisdiction of OOS. The TF was tasked with two missions in order to

track or disable pirates' motherships in response to the growing piracy occurring off Somalia's coast. The first mission required frogmen to place an improvised beacon on the mothership so that merchant ships knowing the pirates' position could reroute to avoid them and the second mission to disable the pirates' mothership involved frogmen attaching explosives to its hull. For both missions, technology that could be integrated with the mission was available, but there was misalignment of purpose between the HQ and frogmen. Hence, OOS highlighted the criticality of having an alignment in purpose before successful integration between advanced technology and SO could take place.

Analysis of the three case studies strongly supports that the tenets of the conceptual model that was adapted from system theory could be used to successfully integrate SO and advanced technology. This analysis yields three main findings. First, SO are well-suited to integrate advanced technology into missions due to their access to resources and their flexibility in adopting new technology. Second, the three enabling conditions of purpose, integration effort, and compatibility are essential for successful integration. Third, careful consideration of these conditions during integration can produce a synergistic outcome, which is defined by increased effectiveness, reduced risk, or effectiveness outweighing the risk incurred from the mission.

Based on these findings, the conceptual model developed in this research could be used by policymakers, military commanders, and technological partners to guide decision-making processes for integrating advanced technology into SO. To this end, three recommendations are proposed. First, policymakers and military commanders should consider the employment of SO as an instrument of statecraft from a systems perspective, i.e., the forces and technologies should be considered mere components for integration into the SO as a system. Second, policymakers and military commanders should consider the implementation of an adaptive task force structure for SO. This structure unshackles the burden of Special Operations Forces having to conduct all SO and sustain all requisite capabilities and technologies. Third, policymakers, military commanders, and technological partners responsible for strategy development, operational planning, tactical execution, and capability development in SO should consider integrating the conceptual model into their doctrines.

This research is in its early stages, and there are several potential areas for future exploration. One potential avenue for future research is identifying new theories for leveraging advanced technology in SO to sustain a competitive edge. Another area of interest could be examining case studies of conventional military operations to validate the model for integrating advanced technology into military operations.

## ACKNOWLEDGMENTS

I would like to express my deepest gratitude to all those who have supported and guided me throughout the journey of completing this thesis.

First and foremost, this endeavor would not have been possible without my advisor, Dr. Ben Gans, and second reader, Dr. Kevin Jones. I thank you both for your unwavering support and insightful feedback. Your patience and expertise are remarkable, and there is always so much to learn from every meeting we have. I am truly fortunate that both of you agreed to be part of my advisory team.

Next, I am also grateful to the chairman of the Defense Analysis department, Dr. Carter Malkasian, and his team of faculty. I am thankful for the invaluable knowledge I received from the classes over the past six quarters. Most of these classes were important building blocks for my research, while others helped develop me as a better researcher and military officer.

Furthermore, I extend my heartfelt appreciation to my commanders in Singapore for providing me with this unique learning opportunity. I understand that the decision to send me to NPS was not easy, considering the ever-busy schedule back home.

Last but not least, words cannot express my gratitude to my wife and three children. I thank you all for showing your love, care, and understanding throughout these 18 months at NPS. My achievement here is not mine alone, but yours too.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. INTRODUCTION

At approximately 0600 on December 19, 1941, the sailors and crew in the harbor of Alexandria witnessed the sinking of two battleships, *HMS Valiant* and *HMS Queen Elizabeth*, and a tanker, *Sagona*. The destroyer *HMS Jervis* was seriously damaged.<sup>1</sup> This was an exceptional act of bravery by six Italian frogmen from the 10th Light Flotilla: Luigi Durand de la Penne, Emilio Bianchi, Antonio Marceglia, Spartaco Schergat, Vincenzo Martellotta, and Mario Marino. One of the most successful special operations (SO) of World War II was the attack on the Alexandria ships, which highlights the importance of precisely executed underwater missions.<sup>2</sup> In recognition of their valiant actions, all six individuals were awarded the Italian Gold Medal for bravery.<sup>3</sup> Never before in Italian history had an operation seen all of its participants so highly decorated.

During the early stages of World War II, the British had secured vital ports in the Mediterranean Sea, including Alexandria, Gibraltar, and Malta.<sup>4</sup> The ports were key nodes in the supply system between Europe and North Africa. Mussolini saw the importance of regaining naval power in the Mediterranean Sea to ensure consistent resupply of his Italian troops while limiting British supplies. The idea was to enhance and deploy the capability of the 10th Light Flotilla.<sup>5</sup> The 10th Light Flotilla unit was a specialized and secret naval warfare unit called *Decima Flottiglia MAS*. This particular unit displayed innovation by utilizing a team of carefully chosen, extensively trained individuals who utilized unique

---

<sup>1</sup> William Harry McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (Novato (CA): Presidio, 1996), 95–98.

<sup>2</sup> McRaven, 74.

<sup>3</sup> McRaven, 100.

<sup>4</sup> McRaven, 73.

<sup>5</sup> Vincent P O'Hara and Enrico Cernuschi, "Frogmen against a Fleet: The Italian Attack on Alexandria 18/19 December 1941," *Naval War College Review* 68, no. 3 (2015): 119, <https://digital-commons.usnwc.edu/nwc-review/vol68/iss3/8>.

weaponry and delivery systems in order to carry out covert attacks.<sup>6</sup> This included the development of then state-of-the-art manned torpedoes—*siluro a lenta corsa* (slow-running torpedo [SLC])—which would subsequently be used in many attacks, including Alexandria. The SLC was colloquially called the pig by the operators because of its frequent breakdowns and the difficulty in using it.<sup>7</sup>

The SLC – a slow-speed human torpedo. It was 6.7 meters long and manned by two divers. Maximum speed was 2.5 mph with a range of ten nautical miles and a submersion depth of thirty meters. The SLC was propelled by a battery-powered motor, and the pilot maintained buoyancy through forward and aft trim tanks. The tanks were blown dry with air from bottles positioned in the midsection. The pilot steered the torpedo using a magnetic compass and a depth gauge, both luminescent. The warhead, contained in the bow, was a 300 kilogram explosive. It was detachable and could be slung under the ship like a mine. In the mid-section, behind the second diver, was a tool chest containing net cutters, air net lifters, clamps for attaching the explosives, and plenty of line.<sup>8</sup>

The Italians had suffered huge losses during their initial attempts to attack Alexandria, Gibraltar, and Malta.<sup>9</sup> Through these failures, the Italians continued to improve on their tactics and design of their technology, particularly the SLC. For example, they overcame the unreliability of the torpedoes and fit them into watertight canisters mounted on a modified submarine.

Finally, they had their first success in Gibraltar on September 21, 1941, sinking three vessels: the naval tanker *Denby Dale*, the British motorship *Durham*, and the British tanker *Fiona Shell*.<sup>10</sup> They were now ready for Alexandria. The six frogmen were selected for the one-way mission to attack the heavily guarded Alexandria harbor. As Bianchi later said, “we knew that even in the best case there was no chance to avoid capture. There was an escape plan, but it was just for psychological comfort.”

---

<sup>6</sup> Vincent P. O’Hara and Enrico Cernuschi, “Frogmen against a Fleet: The Italian Attack on Alexandria 18/19 December 1941,” *Naval War College Review* 68, no. 3 (2015): 119, <https://digital-commons.usnwc.edu/nwc-review/vol68/iss3/8>.

<sup>7</sup> O’Hara and Cernuschi, 120.

<sup>8</sup> McRaven, *Spec Ops*, 79.

<sup>9</sup> McRaven, 81–85.

<sup>10</sup> McRaven, 84–85.

On December 18, 1941, at 2030, the six frogmen were released along with three SLC by the submarine *Scire*.<sup>11</sup> The first SLC was piloted by De la Penne and co-piloted by Bianchi; their target was *HMS Valiant*.<sup>12</sup> The second SLC was piloted by Marceglia and co-piloted by Schergat; their target was *HMS Queen Elizabeth*. The third SLC was piloted by Martellotta and co-piloted by Marino; their target was an aircraft carrier or a larger tanker. Travelling in convoy and arriving at the entrance of the harbor, they patiently waited for opportunity to enter.<sup>13</sup> The boom of the harbor opened for returning ships at 0024, at which time the six frogmen sneaked past the gates with their SLC. Once in the harbor, they were separated and made their ways to the respective targets.

The frogmen's approaches to their targets were full of obstacles. First, they encountered intermittent small explosive drops.<sup>14</sup> The fear of triggering the explosives in the SLC caused concern for the frogmen, but they pushed through to complete their mission. The first SLC encountered an unknown obstruction near *HMS Valiant*, causing it to sink to the bottom.<sup>15</sup> Adding to the challenge, De la Penne's rubber suit had a tear, causing cold water to leak in, and his partner Bianchi had fainted, leaving De la Penne to complete the task alone. With great effort, he managed to drag the torpedo to the targeted vessel's bottom and set off the fuse. Upon resurfacing, he found Bianchi clinging to a mooring buoy, and they were eventually caught by patrol boats in the harbor.

The second SLC had no trouble identifying the target or breaching the protective nets.<sup>16</sup> They faced issues with the SLC's buoyancy, however, causing it to uncontrollably ascend and descend, ultimately leading to it crashing into the hull of *HMS Queen Elizabeth*. As a result, co-pilot Schergat fell ill, leaving Marceglia to complete the task alone. The fuse was set off at 0325.

---

<sup>11</sup> O'Hara and Cernuschi, "Frogmen against a Fleet," 126.

<sup>12</sup> O'Hara and Cernuschi, 127.

<sup>13</sup> McRaven, *Spec Ops*, 90–93.

<sup>14</sup> O'Hara and Cernuschi, "Frogmen against a Fleet," 127.

<sup>15</sup> O'Hara and Cernuschi, 127–28.

<sup>16</sup> McRaven, *Spec Ops*, 95–97.

For the third SLC, Martellotta was unable to submerge due to dive set malfunctions while approaching the tanker, *Sagona*.<sup>17</sup> As a solution, he maneuvered the SLC on the surface to the tanker's stern, where the pair planted the charges and set off the fuse at 0255. Both Martellotta and Marceglia's teams managed to reach the shore, but they were eventually captured by Egyptian police.

De la Penne and Bianchi were interrogated upon capture, but they refused to reveal any information.<sup>18</sup> At 10 minutes before 0600, De la Penne informed the captain of HMS Valiant that the ship would sink, prompting the crew's evacuation. Eventually, De la Penne and Bianchi were kept onboard but survived the shock caused by the explosion.

At 0547, the explosive detonated on the *Sagona*, followed by *HMS Valiant* at 0606 and *HMS Queen Elizabeth* at 0610, signifying that the frogmen's operation was successful.<sup>19</sup> As a result of the attack, Rome reasserted its dominance over the sea and resumed contact with Africa.<sup>20</sup> Admiral Cunningham expressed his dismay, stating "the damage to the battleships at this time is a disaster."<sup>21</sup>

The assault on Alexandria showcased how a small group of six frogmen could use unconventional techniques, such as underwater infiltration, to execute a SO that, when combined smoothly with advanced technology like the SLC, could produce a strategic outcome—for example, altering the balance of power in the Mediterranean Sea.

The story above is one of the many SO conducted in its history. SO are inherently risky and specialized and require high-level expertise, precision, and quick decision making. Both success and failure are usually accompanied with high strategic implications. Colin Gray asserts that "strategy strictly is only the product of tactics and operations.... 'Strategic' is a quality found in the consequences of tactical and operational behavior."<sup>22</sup>

---

<sup>17</sup> McRaven, 97–98.

<sup>18</sup> McRaven, 94–95.

<sup>19</sup> O'Hara and Cernuschi, "Frogmen against a Fleet," 130.

<sup>20</sup> O'Hara and Cernuschi, 133.

<sup>21</sup> O'Hara and Cernuschi, 133.

<sup>22</sup> Steve Lambakis, "Colin Gray on the Strategic Utility of Special Operations," *Comparative Strategy* 40, no. 2 (March 2021): 206, <https://doi.org/10.1080/01495933.2021.1880841>.

Hence, it is always in the interest of policy makers and military leaders to invest, research, and innovate in developing technology to increase the effectiveness and at the same time reduce the risk of the mission. This claim is also supported by Colin Gray, who describes technological assistance as one of the conditions for SO's success.<sup>23</sup> Special Operations Forces (SOF) require all the technological benefits available to them. The effectiveness of their overall strategy relies on their ability to execute tactics, and when dealing with a small number of heroes who are vastly outnumbered, technical support becomes essential for tactical feasibility.

Such success stories are the motivations of this research, which intends to understand the roles of advanced technology in SO.

## **B. GAPS**

Experts such as Michael O'Hanlon have predicted that the development of technology over the next two decades will outpace the already fast-paced development that the world has witnessed in the past two decades.<sup>24</sup> Buzzwords like cyber, robotics and autonomous systems, big data and analytics, additive manufacturing, and artificial intelligence (AI) are just some examples of language that has crept into the discussion of military technology innovation.<sup>25</sup> While there is much hype about these terminologies, few studies, including Gray and Kiras, had theorized how advanced technologies can be integrated into SO.<sup>26</sup> Even in those studies, the research was not centered on the use of advanced technology.

---

<sup>23</sup> Colin S. Gray, "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?" *The U.S. Army War College Quarterly: Parameters* 29, no. 1 (October 1999): 2–24, <https://doi.org/10.55540/0031-1723.1916>.

<sup>24</sup> Michael E. O'Hanlon, *Forecasting Change in Military Technology, 2020–2040* (Washington, DC: Brookings Institution Press, 2018), 4, [https://www.brookings.edu/wp-content/uploads/2018/09/FP\\_20181218\\_defense\\_advances\\_pt2.pdf](https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf).

<sup>25</sup> "Top 10 Military Technology Trends for 2023," *StartUs Insights* (blog), November 5, 2021, <https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/>.

<sup>26</sup> James D. Kiras, "Future Tasks: Threats and Missions for SOF," *Special Operations Journal* 5, no. 1 (January 2019): 6–24, <https://doi.org/10.1080/23296151.2019.1581424>; and Gray, "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?"

Though the concept of integrating technology with SO sounds valuable, logical, and “sexy,” there exist many unanswered questions about this theory. Examples of these questions include the following: What conditions must be present to integrate technology with SO? Will there be significant benefits to continuing investing and fielding advanced military technology for SO? This paper aims to explore the questions above. While this paper does not prescribe a comprehensive solution to specific circumstances, it could provide readers with a generic yet robust conceptual model to provoke thoughts and frame issues such that advanced military technology can be carefully selected and tailored for SO.

### **C. RESEARCH QUESTION AND OBJECTIVES**

In recognition that there is a lack of understanding and discussion on the topic of application of advanced military technology in SO, this thesis aims to develop a systemic approach to address the following research question:

**How can advanced technology be integrated into Special Operations to maximize their effectiveness and reduce risk during Special Operation missions?**

The value of this study lies in its application. The model presented adopted the tenets of a well-established concept, System Theory. Some revisions were required to suit the context of SO and the details would be elaborated in Chapter II. Analysis of a diverse set of case studies suggests that the model is sufficiently broad and general such that it should be applicable in most SO missions.

There are three objectives for this research:

- To identify the conditions that allow advanced military technology to be fielded in SO and examine the effectiveness of this integration.
- To examine the outcome of the integration of advanced military technology and SO by assessing the effectiveness of the missions and the risks involved.

- To develop a conceptual model to encapsulate the findings of the first two objectives.

## **D. RESEARCH DESIGN AND DATA COLLECTION**

### **1. Research Design**

The approach for this unclassified, qualitative research is a comparative case study. Given the intricate nature and the limited research available on this topic, conducting a qualitative research study could allow for an exploration of the experiences across multiple case studies and lead to the generation of rich and nuanced insights through careful analysis.

Prior to the commencement of case study analysis, a literature review was conducted on three relevant topics—SO, advanced technology, and system theory—to provide a strong understanding on the foundation of this research.

Next, extensive research was conducted on the following cases: Operation Olympic Games, Operation Orchard, and Operation Ocean Shield (OOS). The three cases were selected because they incorporate advanced technology into SO at their start state. Furthermore, they represent a myriad of different domains (cyber, air, maritime, land, and electromagnetic spectrum) and three different actors (U.S., Israel, and North Atlantic Treaty Organization [NATO]) and therefore validate the flexibility of the eventual model developed.

Following the study of the cases, thorough analysis was conducted on the data gathered from the case studies. The main idea is to identify and consolidate recurring themes and concepts from the case studies and literature reviews and then draw conclusions by identifying correlations or patterns on the themes. The first main theme is to identify the causal factors or enabling conditions that contribute to the successful integration of advanced technology in SO and the resulting impact of this integration. The second main theme is to evaluate the outcome of integration between SO and advanced technology.

Finally, the findings from the case studies were consolidated. Based on these findings and conclusions, a conceptual model will be developed and presented in Chapter II to encapsulate the research findings.

## **2. Data Collection**

To develop a deep understanding for the research, two main instruments for data collections were used: open-source literature and author interviews. The following sections elaborate the methodology used for each of these instruments.

### ***a. Open-Source literature***

Open-source literature for this research consisted mainly of unclassified secondary sources of information including but not limited to journals, news articles, reports, and books. To eliminate bias from the literature, multiple sources were consulted to ensure accuracy of data and to gather holistic perspectives on the discussions.

### ***b. Author Interviews***

Semi-structured author interviews were conducted with SO commanders or operators who were involved in the cases, providing non-academic perspectives and uncovering important “ground issues” that may be missed by examining open-source literature alone. Some good practices were maintained in the conduct of these interviews. First, interview protocols were developed based on the conclusions from the literature review. This protocol served to guide the interview proceeding. In the semi-structured interviews, however, respondents were also free to provide further insights beyond the scope of the protocol. See Appendix A for interview protocol. Second, the nature of most SO is classified. Hence, it is a common understanding that confidentiality needs to be maintained in certain aspects of SO as well as for the identity of the operators. To this end, only unclassified data is presented in this research and only the job description, without the names and nationality, of the respondents are revealed. See Appendix B for list of interviewees. Third, interview transcripts were produced following the interviews. See Appendix C for a sample interview transcript. Finally, content analysis was done on the

transcripts. This included placing relevant data into various categories as identified during literature reviews. See Appendix D for an example of content analysis.

***c. Mitigating Research Bias***

As a naval SOF officer for 15 years, I have attempted to maintain neutrality throughout the research process to ensure the validity and quality of the research. I have done so in two ways. First, my personal opinions and experiences have been excluded from the data collection and analysis. Second, the analysis of the data has been cross-checked by my advisory team, which has highly qualified personnel from diverse backgrounds (i.e., military and non-military) and expertise (i.e., operators and engineers).

**E. LIMITATIONS**

The main limitation was the restrictions imposed by the unclassified nature of the thesis. Especially for SO, where the operations are typically surrounded by a certain degree of secrecy, available content available is limited. The data collected, except for the author's interviews, are mainly limited to secondary, open-source information.

**F. THESIS OUTLINE**

Figure 1 provides the overview for the thesis. After the introduction of this thesis in Chapter I, Chapter II begins with a literature review focused on the key elements of this research—SO, Military Technology, and System Theory—followed by elaboration of the conceptual model. Chapters III, IV, and V are three distinct case studies focusing on three different states/organizations (the U.S., Israel, and NATO) across three different domains (cyber, air, maritime). Chapter VI, the concluding chapter, consolidates the insights and analysis gleaned from the various cases, then culminates in recommendations and areas for further research on the integration of SO and advanced military technology.

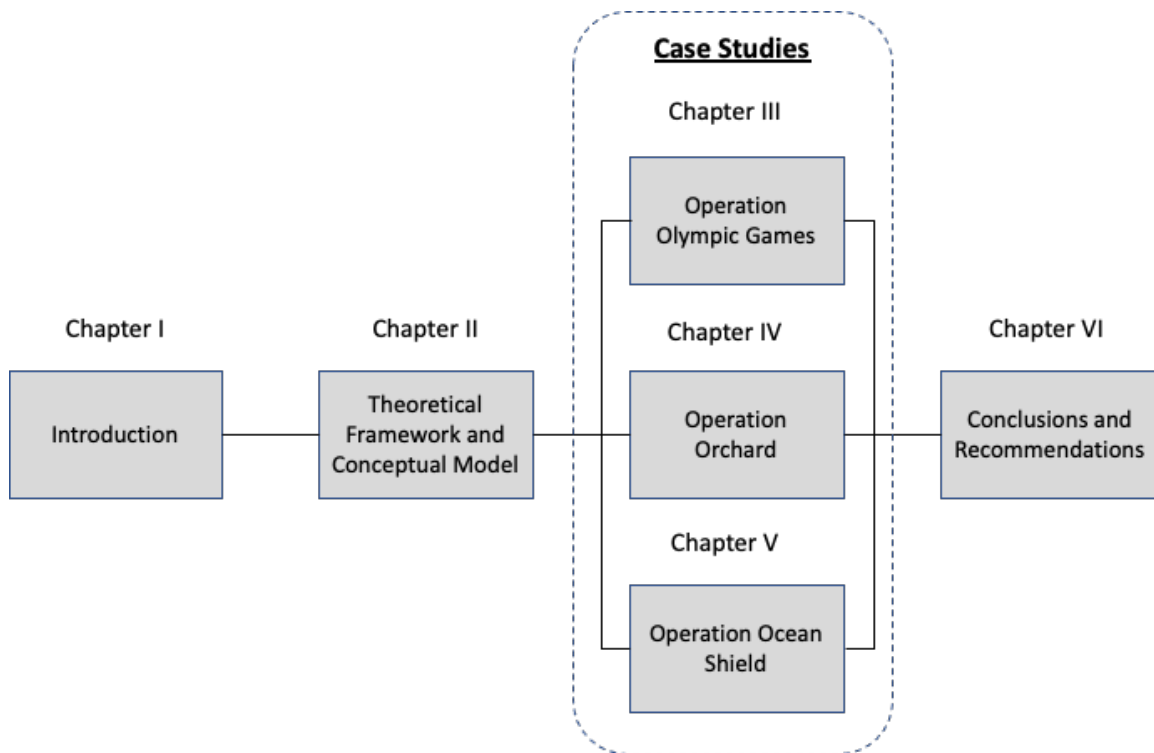


Figure 1. Overview of Thesis

## **II. THEORETICAL FRAMEWORK AND CONCEPTUAL MODEL**

### **A. INTRODUCTION**

In Chapter I, we saw the potential of advanced technology when integrated with SO potentially leading to the outcome of increased effectiveness and reduced risk for operations. This chapter provides a conceptual model to elaborate on this proposition. This model applies a well-researched system theory to a military domain. This model was inspired by the works of Nevo and Wade.<sup>27</sup> Upon thorough examination and in-depth research conducted on the three case studies of this thesis, Nevo and Wade's model can be modified and applied to SO. The conceptual model highlights that a synergistic relationship between SO and advanced technology can lead to a desirable mission outcome of increased effectiveness and reduced risks. A synergistic relationship can occur when three enabling conditions are met: purpose, compatibility, and integration effort.

This chapter begins with a literature review of the key concepts of the research: SO, advanced technology, and system theory. Following that, the tenets of the conceptual model are elaborated. The chapter concludes with how the conceptual model was tested in the case studies.

### **B. LITERATURE REVIEW**

This literature review covers three concepts: SO, Advanced Technology, and System Theory.

#### **1. Special Operations**

SO are crucial in military strategy and national security, offering distinct capabilities and adaptability to accomplish objectives that are beyond the scope of conventional means. The capacity to execute SO is often a critical element in

---

<sup>27</sup> Saggi Nevo and Michael R. Wade, "The Formation and Value of IT-Enabled Resources: Antecedents and Consequences of Synergistic Relationships," *MIS Quarterly* 34, no. 1 (March 2010): 163–83, <https://doi.org/10.2307/20721419>.

accomplishing success in dynamic and complex environments. SO have been a vital military tool for creating strategic effects to fulfill policy objectives and will continue to be highly relevant in modern warfare.

The definition of SO has evolved over time. In 1979, the DOD dictionary defined SO as:

Military operations conducted by specially trained, equipped, and organized DOD forces against strategic or tactical targets in pursuit of national military, political, economic, or psychological objectives. They may support conventional operations, or they may be prosecuted independently when the use of conventional forces is either inappropriate or infeasible. Sensitive peacetime operations, except for training, are normally authorized by the National Command Authorities (NCA) and conducted under the direction of the NCA or designated commander. Special operations may include unconventional warfare, counterterrorist operations, collective security, psychological operations, and civil affairs measures.<sup>28</sup>

While this definition covered the essences of SO, its utility was limited to those within DOD. Agencies and actors outside of DOD conducting operations similar to SO would not be able to associate with the authority and examples of the mission. Therefore, to mitigate the above concern, identifying a more generic and encompassing definition became necessary. In 1984, Maurice Tugwell and David Charters revised it with the following:

Small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.<sup>29</sup>

In this definition, SO could be conducted overtly, covertly, or clandestinely. Overt operation is conducted openly without concealment (i.e., effect and actor known), covert operation is activity planned and conducted to conceal the identity of sponsor (i.e., effect

---

<sup>28</sup> Tugwell and Charters, “Special Operations and the Threats to United States Interests in the 1980s.”

<sup>29</sup> Tugwell and Charters, 35.

known and actor unknown), and clandestine operation is activity conducted in secrecy or concealment (i.e., effect and actor unknown).<sup>30</sup> The inclusion of non-military resources and dropping of specific mission sets made it more applicable to agencies and actors outside DOD.

There are generally two perspectives on how SO can be defined. The first is explained in terms of a significant outcome (e.g., strategic effect, political imperative). The other sees SO as those missions that cannot be fulfilled by conventional forces. Scholars including John Arquilla, Tom Searle, Robert G Spulak, Collin Gray, and Adm (Ret) William McRaven contributed to better understanding of SO.

For the first perspective, Colin Gray asserted that SO should generate strategic outcomes and can offer two main advantages: expansion of choice and economy of force.<sup>31</sup> The first aspect pertains to how SO can supply policymakers with more choices beyond the scope of what regular military operations can provide, thereby filling some of the void left by conventional military forces. Meanwhile, the economy of force is what propels this increase in options. Essentially, Gray contends that SO can yield a substantial impact compared to the military power and financial resources they consume, leading to a favorable strategic-value ratio. This makes SO an appealing option for decision makers at the strategic level due to the potential for high returns on investment especially in peacetime.<sup>32</sup>

Adm (Ret) William McRaven, former USSOCOM commander, also highlighted the strategic nature of SO: “A special operation is conducted by forces specially trained, equipped, and supported for a specific target whose destruction, elimination, or rescue (in the case of hostages), is a political or military imperative.”<sup>33</sup> He admitted that his definition

---

<sup>30</sup> Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1 (Washington, D.C.: Joint Chiefs of Staff Washington, 2010), <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/Reference-Series/>.

<sup>31</sup> Colin S. Gray, *Explorations in Strategy* (Westport, Conn: Greenwood Press, 1996).

<sup>32</sup> Gray.

<sup>33</sup> McRaven, *Spec Ops*, 2.

was skewed toward direct action missions, however.<sup>34</sup> In his theory of SO, he viewed relative superiority as critical condition for a smaller force to gain advantage over a bigger force.<sup>35</sup> Relative superiority can be obtained when six conditions are met: simplicity, security, repetition, purpose, speed, and surprise.<sup>36</sup>

Similarly, Robert G. Spulak also agrees that SO are to accomplish strategic objectives and goes on to compare the characteristics of conventional forces and SOF to investigate why SO often favor the latter.

Special operations are missions to accomplish strategic objectives where the use of conventional forces would create unacceptable risks due to Clausewitzian friction. Overcoming these risks requires special operations forces that directly address the ultimate sources of friction through qualities that are the result of the distribution of the attributes of SOF personnel.<sup>37</sup>

Spulak goes on to describe the necessary characteristics of SOF personnel and says they are elite warriors, flexible and creative. Such emphasis on SOF has created a confusion over who owns or can conduct SO, however. This may inevitably create tension among non-SOF units conducting risky, unconventional operations yet who cannot identify themselves as conducting SO.

For the latter perspective to view SO as operations that cannot be performed by conventional forces, John Arquilla viewed SO as “a class of military (or paramilitary) actions that fall outside the realm of conventional warfare during their respective time periods.”<sup>38</sup> Similarly, Tom Searle mentions that “Special operations are operations outside the conventional operation box.”<sup>39</sup> Both definitions consider SO as a dependent variable

---

<sup>34</sup> McRaven, 3.

<sup>35</sup> McRaven, 4.

<sup>36</sup> McRaven, 8.

<sup>37</sup> Robert G. Spulak, *A Theory of Special Operations: The Origin, Qualities, and Use of SOF*, JSOU Report 07-7 (Hurlburt Field, FL: Joint Special Operations University, 2007), 21, <https://apps.dtic.mil/sti/pdfs/ADA495521.pdf>.

<sup>38</sup> John Arquilla, *From Troy to Entebbe: Special Operations in Ancient and Modern Times* (Lanham, Md: University Press of America, 1996), xv-xvi.

<sup>39</sup> Tom Searle, *Outside the Box: A New General Theory of Special Operations*, JSOU Report 17-4 (MacDill AFB, FL: Joint Special Operations University, 2017), 14.

that may change based on the abilities of conventional forces. If conventional forces become more capable of performing the tasks of SO, then SO forces would have to shift their focus to higher-level operations.

While no definition can convince or satisfy everyone, the discussions among the scholars have provided a clear understanding of the characteristics and purposes of SO. For this thesis, I adopted the definition from Maurice Tugwell and David Charters as it is not overly restrictive towards the actors and the purpose of the SO.

Recognizing the crucial nature of the desired outcome that SO must achieve, it is imperative to explore ways to supplement or enhance their capabilities. Utilizing advanced technology is one promising means of doing so.

## **2. Advanced Technology**

Throughout history, the purpose of military technology has been to enable military forces to counter adversarial threats to create a competitive advantage over them. Such technology also provides military and non-military alternatives to the policymakers and military commanders.<sup>40</sup>

Use of military technology dates back to ancient times when warriors used tools as weapons. For example, the building of the stone wall of Jericho around 8000 BCE was a clear use of technology for defense against adversaries.<sup>41</sup> Military technology has refined and advanced through different times. Through these successful innovations and development, the world saw technology emerge such as shields, helmets, and armor used in the classical age. Later, around the 14th and 20th centuries, the development of gunpowder and nuclear weapons, respectively, revolutionized warfare in the respective times.<sup>42</sup>

---

<sup>40</sup> “Maintaining Military Advantage Through Science & Technology Investment,” 2019.

<sup>41</sup> *Britannica*, s.v. “military technology,” accessed March 17, 2023, <https://www.britannica.com/technology/military-technology/Prehistory#ref57563>.

<sup>42</sup> Michael Marshall, “Timeline: Weapons Technology,” *New Scientist*, last modified July 7, 2009, <https://www.newscientist.com/article/dn17423-timeline-weapons-technology/>.

While it is important to understand the history of the development of technology, it is equally critical to understand how technology impacts the modern era. In recent years, technology has continued to advance and evolve. Some of the recent developments include the use of drones, cyber weapons, and AI. In the case of drones, surveillance has been the main use, although in some cases, they have also been used for targeted killing. An example is the killing of al-Qaida leader Ayman al-Zawahiri by a U.S. drone missile in Kabul in August 2022.<sup>43</sup> In the case of cyber weapons, we saw the first known cyberweapon, Stuxnet, in 2010 when the U.S. and Israel allegedly used the computer worm to disable Iran's nuclear program. In the case of AI, the potential it possesses to influence future warfare has sent superpowers such as the U.S. and China to invest heavily in this technology.<sup>44</sup> Even Russian president Vladimir Putin has asserted that "Whoever becomes the leader in this sphere (AI) will become the ruler of the world."<sup>45</sup> Applications such as ChatGPT have proven their astounding ability to generate human-like text.<sup>46</sup> It was reported that even the Pentagon has used ChatGPT to write a report about a new counter-drone task force (TF).<sup>47</sup>

Such rapid development and adaptation of technology are not only seen in government agencies or military; because of the ease of access and low cost, non-state actors may also take advantage of these technologies for political violence. Professor Audrey Cronin, who was a specialist in terrorism at the Congressional Research Service, explained, "the worldwide dispersal of emerging technologies, such as commercial drones, cyber weapons, 3D printing, military robotics, and autonomous systems, is generating

---

<sup>43</sup> Jim Garamone, "U.S. Drone Strike Kills al-Qaida Leader in Kabul," *DOD News*, August 2, 2022, <https://www.defense.gov/News/News-Stories/Article/Article/3114362/us-drone-strike-kills-al-qaida-leader-in-kabul/>.

<sup>44</sup> Zachary Arnold, "What Investment Trends Reveal about the Global AI Landscape," *Brookings* (blog), September 29, 2020, <https://www.brookings.edu/techstream/what-investment-trends-reveal-about-the-global-ai-landscape/>.

<sup>45</sup> Radina Gigova, "Who Vladimir Putin Thinks Will Rule the World," *CNN*, September 2, 2017, <https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>.

<sup>46</sup> Alex Hughes, "ChatGPT: Everything You Need to Know about OpenAI's GPT-4 Tool," *BBC Science Focus Magazine*, March 16, 2023, <https://www.sciencefocus.com/future-technology/gpt-3/>.

<sup>47</sup> Matthew Gault, "Even the Pentagon Is Using ChatGPT Now," *Motherboard Tech by Vice*, last modified February 9, 2023, <https://www.vice.com/en/article/5d37y3/even-the-pentagon-is-using-chatgpt-now>.

gaping fissures in the ability of conventional armed forces to combat lethal capabilities of non-state actors, most notably terrorists, but also rogue lone actors, insurgent groups, and private armies.”<sup>48</sup> Therefore, government agencies and the military must not become complacent, but rather strive to continuously push boundaries and progress at a faster pace than their adversaries.

To this end, Cronin also discussed the criticality to adapt and keep up with the development of open technologies.<sup>49</sup> She argued that there is a shift from close to open technology in the 21st century as open innovation is led by commercial processes, not by militaries. According to Everett Rogers, the spread of open technology superseded the closed technology, stating, “Instead of proliferating like nuclear, chemical, or biological weapons, these technologies diffuse spreading globally as telegraphs, railroads, radios, or automobiles did.”<sup>50</sup> Cronin offered suggestions on how the United States should respond in view of this shift. Essentially, the U.S. military must adapt to the reality of commercially driven and open technology, reorganize around new strategic concepts that take into account the whole-of-society approach and the power of commercial tech companies, and focus on training personnel to address unpredictable threats arising from various sources, including small groups, individuals, and private commercial entities.<sup>51</sup>

In the context of applying technology in SO, James D. Kiras posits that “one of the mega trends relate to the (SOF) operator integrating with technology as a necessity to maintain a competitive edge.”<sup>52</sup> He further elaborates with examples such as swarm UAV, gene therapy, and cybernetic enhancements as possible developments for SO.<sup>53</sup>

---

<sup>48</sup> Audrey K. Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow’s Terrorists* (New York, NY: Oxford University Press, 2020), 1.

<sup>49</sup> Audrey K. Cronin, “Technology and Strategic Surprise: Adapting to an Era of Open Innovation,” *The U.S. Army War College Quarterly: Parameters* 50, no. 3 (August 2020): 71–84, <https://doi.org/10.55540/0031-1723.2675>.

<sup>50</sup> Everett M. Rogers, *Diffusion of Innovations*, 4th ed. (New York: Free Press, 1995).

<sup>51</sup> Cronin, “Technology and Strategic Surprise.”

<sup>52</sup> Kiras, “Future Tasks.”

<sup>53</sup> Kiras, 20.

While it is important to keep informed of the latest trends and developments in technology, and at the same time to continue imagining what future technology could look like, one must recognize that there is no “one size fits all” technology when applied to military or SO. This thesis exclusively examines advanced technologies that can be integrated into SO. These advanced technologies shall meet the following criteria: they should be relatively new and/or have a limited user base, but they should demonstrate the potential to deliver significant benefits.<sup>54</sup> The choice to apply advanced technology in SO needs to be thoroughly examined so that it could enhance the outcome.

### **3. System Theory**

System theory is a valuable tool for theorizing SO because it provides a framework for understanding complex systems and making informed decisions based on a comprehensive understanding of how different factors interact and influence each other. SO can be viewed as a system with a wide range of interconnected sub-systems or components. By comprehending this concept, SO planners and commanders can attain an improved perception of the interdependent relationships among these subsystems and their impact on each other.

System theory is a well-researched concept that consists of several concepts. One of the most famous definitions was offered by Ludwig von Bertalanffy:

General system theory, therefore, is a general science of wholeness. ... The meaning of the somewhat mystical expression, ‘The whole is more than the sum of its parts’ is simply that constitutive characteristics are not explainable from the characteristics of the isolated parts. The characteristics of the complex, therefore, appear as new or emergent.<sup>55</sup>

While it is beyond the scope of this paper to explain system theory in full, a brief elaboration of these concepts will establish the derivation of the conceptual model. The

---

<sup>54</sup> “Definition of Advanced Technology,” Gartner, accessed May 1, 2023, <https://www.gartner.com/en/information-technology/glossary/advanced-technology>.

<sup>55</sup> Ludwig von Bertalanffy, *General System Theory: Foundations, Development, Applications* (New York, NY: Braziller, 1984), 55.

first concept of system theory is that the world is made up of things and things possess properties.<sup>56</sup>

Second, “a system is a regularly interacting or interdependent group of items forming a unified whole,” i.e., systems are made up of groups of things (or components).<sup>57</sup> The properties of a system are derived from the interaction of the components. The system may exhibit similar properties to the sub-components’ new values, or it may be totally different from its original properties.<sup>58</sup> Systems can be closed or open. According to Ludwig von Bertalanffy, closed systems, are “systems that are considered isolated from their environment.”<sup>59</sup> He added that the final condition of the system is a direct result of the initial condition. Most of the systems are not closed but are in constant interaction with the environment to arrive at a steady state, however. The same final state of a system can occur with different permutations of initial condition and environmental factors. Such interaction is an open system. Open system is defined as a “system in exchange of matter with its environment, presenting import and export, building-up and breaking down of its material components.”<sup>60</sup> With regard to this thesis, SO are categorized as open systems due to their susceptibility to external factors. The favorable environmental conditions can significantly enhance the execution of a mission, while the opposite can also hold true.

Third, these new properties give rise to emergent capabilities. Emergent capabilities can be positive, neutral, or negative.<sup>61</sup> Positive emergent capabilities are advantageous and lead to an improvement in the system’s state. Neutral emergent capabilities do not have any significant impact, positive or negative, on the system. Negative emergent capabilities, on the other hand, deteriorate the system’s performance and lead to a worse state than before. Whether benefit can be derived from an emergent capability, however, is often a

---

<sup>56</sup> Nevo and Wade, “The Formation and Value of IT-Enabled Resources,” 165.

<sup>57</sup> *Merriam-Webster*, s.v. “system,” accessed May 12, 2023, <https://www.merriam-webster.com/dictionary/system>.

<sup>58</sup> Nevo and Wade, “The Formation and Value of IT-Enabled Resources,” 166.

<sup>59</sup> Bertalanffy, *General System Theory*, 39.

<sup>60</sup> Bertalanffy, 141.

<sup>61</sup> Nevo and Wade, “The Formation and Value of IT-Enabled Resources,” 168.

matter of perspective.<sup>62</sup> The perspective is influenced by the purpose the emergent capability aims to achieve. Thus, components are said to be having synergy or synergistic relationship when they produce positive emergent capability, i.e., the emergent capability provides beneficial outcome to purpose.

Fourth, Nevo and Wade defined synergy as two systems working together that result in positive outcome.<sup>63</sup> They elaborated there are two types of synergy: potential synergy and realized synergy. They defined: “Potential synergy is the *ex ante* assessment of the range and extent of possible emergent capabilities.”<sup>64</sup> In other words, it can be seen as the possibility that the components can achieve a synergistic relationship. They also defined: “Realized synergy is the *ex post* evaluation of the positive emergent capability that accrues from the relationship.”<sup>65</sup> In other words, it can be seen as the synergistic outcome or effects that derive from fielding a positive emergent capability.

Lastly, Nevo and Wade asserted that two components will only interact and turn into a system if the enabling conditions are present.<sup>66</sup> The conditions are different in each system, but they can be generally classified as compatibility and integration effort. According to Nevo and Wade, “compatibility is an assessment of the ability of a system’s components to interact. Components are compatible when certain properties match or are in alignment.”<sup>67</sup> For an integration effort, management is an essential element for components to interact and transport into a new emergent capability because of the need to organize and coordinate numerous parts of a component into a united system to perform a certain task.<sup>68</sup>

---

<sup>62</sup> C. West Churchman, *The Design of Inquiring Systems: Basic Concepts of Systems and Organization* (New York: Basic Books, 1971).

<sup>63</sup> Nevo and Wade, “The Formation and Value of IT-Enabled Resources,” 168.

<sup>64</sup> Nevo and Wade, 169.

<sup>65</sup> Nevo and Wade, 169.

<sup>66</sup> Nevo and Wade, 170–74.

<sup>67</sup> Nevo and Wade, 170–74.

<sup>68</sup> Nevo and Wade, 170–74.

When considering the integration of advanced technology with SO, fulfilling Nevo and Wade’s two enabling conditions may lead to the development of new capabilities. It does not guarantee a synergistic outcome from the integration, however. In fact, if the capability does not have utility, it can result in a waste of resources. Therefore, in order to align the integration with mission objectives and intent, a third enabling condition—purpose—is essential to mitigate this gap.

A simple search on Google for application of system theory will yield results from social works, psychology, and business organization. Little has been studied with regard to application in military and SO. This research will attempt to view SO and technology as individual components and use a system theory to examine the outcome of this interaction.

### C. CONCEPTUAL MODEL

This section elaborates upon the conceptual model used in this study. See Figure 2. Employing the principles of system theory from the literature review, specifically its four key concepts, I aimed to investigate how the interplay between two variables, namely SO and advanced technology, in favorable enabling conditions leads to a synergistic relationship. This synergistic relationship produces a positive emergent capability that ultimately results in a favorable outcome for the SO mission by enhancing effectiveness and mitigating risk. Because this model is to be applied to military organizations, I will use common military tenets of ways, means, ends, and risk coupled with system theory to elaborate the model.<sup>69</sup> As Lykke mentioned, “strategists, planners, corps commanders and squad leaders are all concerned with *ways* to employ *means* to achieve *ends*.”<sup>70</sup>

---

<sup>69</sup> Arthur F. Lykke Jr, “Toward an Understanding of Military Strategy,” in U.S. *Army War College Guide to Strategy*, Joseph R. Cerami and James F. Holcomb, eds. (Cumberland County, VA: U.S. Army War College, 2001), 180.

<sup>70</sup> Lykke Jr., 180.

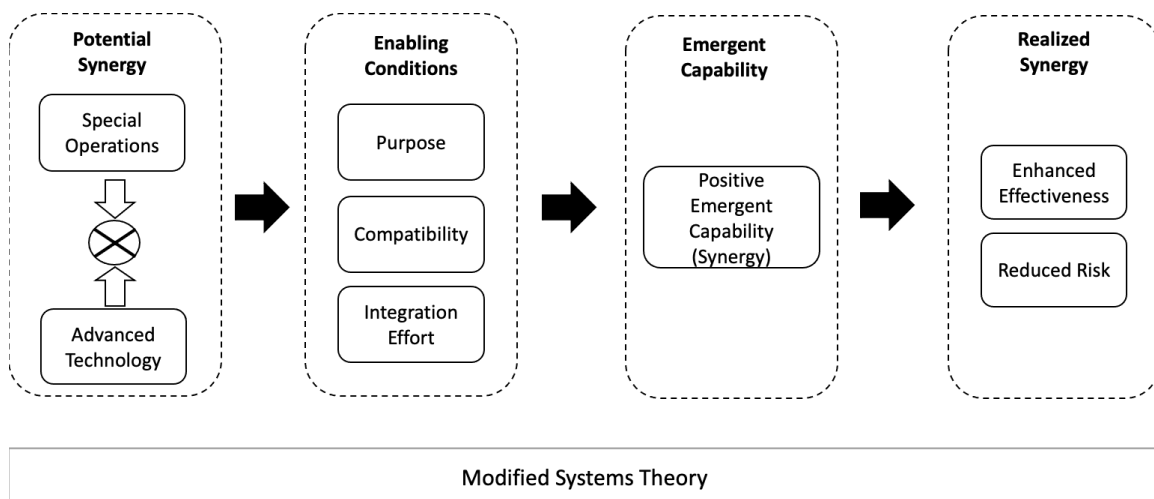


Figure 2. Conceptual Model for Synergistic Relationship between Special Operations and Advanced Technology

### 1. Potential Synergy

The two components that were to be studied were SO and advanced technology. SO are highly suitable for integration with advanced technology because of their unique characteristics. Their small scale and unorthodox nature to generate high-end strategic effect are often well resourced and adaptable to innovation and new technology. To this end, advanced technology is often considered for SO to enhance their capabilities. In this thesis, the consideration without in-depth study to predict that two components—SO and advanced technology—form a system that is able to generate positive outcome is known as potential synergy. For the purpose of this research, this system is said to have synergy when the objective could be achieved in an effective manner and risk has been reduced.

### 2. Enabling Conditions

For SO and advanced technology to have a synergistic relationship so as to develop a positive emergent capability, three enabling conditions—purpose, compatibility, and integration effort—must be fulfilled. Purpose can be seen as having clear understanding of course of action (or ways) and objectives (or ends). As we will see later in Chapter V, while an advanced technology (i.e., a tracking beacon) well integrated with SO could meet the objectives (i.e., monitoring pirates' motherships), the lack of understanding of the course

of action (i.e., higher HQ inclination to primarily disable ship as main strategy) resulted in the lack of utility and a waste of resources. Compatibility refers to the technical feasibility of two components to interact and form a relationship. In Chapter V, the ability for Israeli electronic warfare (EW) systems to be carried onboard their airplanes (e.g., F-16 or Gulfstream) to manipulate Syria's radar systems demonstrated the importance of compatibility between technology and the forces involved in SO. Integration effort refers to the willingness of policymakers or military commanders to integrate SO and advanced technology. In Chapter III, integration is demonstrated by multiple entities (i.e., intelligence, software coders, and material engineers), with oversight from the President of the U.S., developing the Stuxnet malware.

### **3. Emergent Capability**

As indicated in the literature review, a system has the potential to generate new properties or modify existing properties. The outcome of such modifications could result in a positive, neutral, or negative impact. This paper proposes that integrating advanced technology with SO would lead to a positive emergent capability, given that all enabling conditions are met. Only positive emergent capability would give rise to a synergistic outcome.

### **4. Realized Synergy**

Realized synergy or synergistic outcome is the ex-post evaluation of the system's performance against the objectives—i.e., it is an assessment on the integration of SO and advanced technology used in the mission after the positive outcome has been achieved. In this research, there are two criteria used to assess if the system (i.e., integration between SO and advanced technology) has achieved synergistic outcome, namely (combat) effectiveness and risk. Effectiveness is the extent to which the systems is successful towards meeting the outcome. Specifically for this research, it measures the quality of the outcome by evaluating the ability of forces conducting SO to accomplish their objectives. Effectiveness shall not be confused with efficiency, which measures the ability to maximize resources.

This model analyzes two types of risks: risk to the mission and risk to the force. Risk to the force pertains to the likelihood of loss of personnel or casualties during SO to accomplish goals. On the other hand, risk to the mission relates to factors that may result in failure to achieve objectives. Although it may seem logical to assume that a higher risk to the force will lead to a higher risk to the mission, this is not always the case as the two risks may not be directly related. Therefore, it is important to evaluate each risk independently.

#### **D. RELATING CONCEPTUAL MODEL TO CASE STUDIES**

The following three chapters will assess the conceptual model's principles—such as potential synergy, enabling conditions, emergent capability, and realized synergy—through the examination of three case studies. The conceptual model will form the basis of analysis for the case studies. For each case study, the analysis will begin with a bottom-line-up-front approach by stating the summary of the integration between advanced technology and SO. Subsequently, the analysis will explore the details of the model's tenets, starting with qualifying the mission in the case study as a SO and ascertaining the integration of advanced technology within the mission. These qualifications are crucial to ensure consistency in the variables (i.e., SO and advanced technology) being tested. The analysis will then investigate the presence of the three enabling conditions for integration in each mission. The aim is to verify if enabling conditions are necessary for a successful integration. Finally, the outcome of the integration, whether it is positive (synergistic), neutral, or negative, will be evaluated in terms of the mission's effectiveness and risk.

### III. OPERATION OLYMPIC GAMES

Military action would always be on the table, but it would be my last resort... One thing is certain. The United States should never allow Iran to threaten the world with a nuclear bomb.

—George W. Bush<sup>71</sup>

#### A. INTRODUCTION

Operation Olympic Games was a covert operation that reportedly was planned and executed by American and Israeli forces.<sup>72</sup> The main goal was to delay Iran's program to develop nuclear weapons by uranium enrichment. The process of enrichment required a large number of centrifuges to be installed at Iran's nuclear facilities. One such facility was housed in Natanz. Iran would be a threat to the region if it were to create a nuclear weapon.

The options to delay Iran's nuclear ambition were an air strike, a covert raid, or a cyberattack.<sup>73</sup> These options presented policymakers with a wide range of potential effects. On one end of the spectrum, there was the highly destructive effort, such as an airstrike or, to some extent, a covert raid, which carried a significant risk of escalation. On the other end, there was the more gradual approach of delaying the nuclear program, exemplified by a cyberattack, which carried a lower risk of attribution. Cyberattack was chosen in this operation and it involved the spread of a "worm," Stuxnet.<sup>74</sup> When Stuxnet was first discovered and announced to the public, it sent the cyber security industry into panic and confusion due the sophisticated design of the code and the potential detrimental effect it

---

<sup>71</sup> George W. Bush, *Decision Points* (New York: Crown Publishers, 2010).

<sup>72</sup> Ellen Nakashima and Joby Warrick, "Officials Say U.S., Israel Were behind Cyberattack on Iran," *The Washington Post*, June 2, 2012, ProQuest.

<sup>73</sup> Ewen MacAskill and Chris McGreal, "George Bush's Memoirs Reveal How He Considered Attacks on Iran and Syria," *The Guardian*, November 8, 2010, ProQuest; and Paul Wagenseil, "Obama, Bush Behind Stuxnet Worm, Report Says," *NBC News*, June 1, 2012, <https://www.nbcnews.com/id/wnba47647550>.

<sup>74</sup> A worm virus refers to a malicious program that replicates itself, automatically spreading through a network.

could pose to all computer systems globally.<sup>75</sup> Stuxnet was an unprecedented kind of cyberattack in Natanz that affected first the virtual dimension, subsequently perpetuating into the physical and cognitive dimensions. Stuxnet altered the code in controlling the programmable logic controllers (PLCs), destroying about 1,000 centrifuges.<sup>76</sup> Experts have suggested that this operation delayed Iran's nuclear program by one to two years.<sup>77</sup>

This case study will be analyzed through the lens of the conceptual model presented in Chapter II (i.e., examination of the integration of SO and advanced technology, enabling conditions, and outcomes). This chapter will be laid out as follows: It will begin with a background of the operation with focus on the circumstances that led to the operation. Next, details of the operation will be elaborated on so as to provide readers an understanding of the key elements of the operation. Third, the analysis of the case will be presented alongside the assessment of the applicability of the conceptual model. Finally, the key findings from this case study will be presented in the conclusion.

## **B. BACKGROUND**

After the breakdown of the relationship between Iran and the West following the Islamic Revolution and hostage crisis in Tehran (1979), the United States terminated diplomatic ties with Iran and effectively ended the support to its nuclear program.<sup>78</sup> Ayatollah Ruhollah Khomeini, the Iran's first Supreme Leader, initially had no interest in developing nuclear capability, stating that it was against Islam.<sup>79</sup> Mohsen Rafighdoost,

---

<sup>75</sup> Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014), 13–14.

<sup>76</sup> Mariusz Antoni Kamiński, "Operation 'Olympic Games.' Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Programme," *Security and Defence Quarterly* 29, no. 2 (2020): 63–71, <https://doi.org/10.35467/sdq/121974>.

<sup>77</sup> David Albright et al., *Preventing Iran from Getting Nuclear Weapons: Constraining Its Future Nuclear Options* (Washington, D.C.: Institute for Science and International Security, 2012), 16, [https://www.researchgate.net/profile/David-Albright-2/publication/267689515\\_Preventing\\_Iran\\_from\\_getting\\_nuclear\\_weapons\\_constraining\\_its\\_future\\_nuclear\\_options\\_p\\_10\\_5\\_March\\_2012/links/56f2884608ace034d8c635a5/Preventing-Iran-from-getting-nuclear-weapons-constraining-its-future-nuclear-options-p-10-5-March-2012.pdf](https://www.researchgate.net/profile/David-Albright-2/publication/267689515_Preventing_Iran_from_getting_nuclear_weapons_constraining_its_future_nuclear_options_p_10_5_March_2012/links/56f2884608ace034d8c635a5/Preventing-Iran-from-getting-nuclear-weapons-constraining-its-future-nuclear-options-p-10-5-March-2012.pdf).

<sup>78</sup> "Policy & History," U.S. Virtual Embassy Iran, accessed April 6, 2023, <https://ir.usembassy.gov/our-relationship/policy-history/>.

<sup>79</sup> Gareth Porter, "When the Ayatollah Said No to Nukes," *Foreign Policy*, October 16, 2014, <https://foreignpolicy.com/2014/10/16/when-the-ayatollah-said-no-to-nukes/>.

who formerly served as minister of the Islamic Revolutionary Guard Corps, recalled in an interview that Ayatollah Khomeini told him, “it doesn’t matter whether it is on the battlefield or in cities; we are against this... It is *haram* [forbidden] to produce such weapons. You are only allowed to produce protection.”<sup>80</sup>

It was reported, however, that Ayatollah Khomeini had change his mind following the death of around one million Iranians during the Iran-Iraq war, which lasted eight years.<sup>81</sup> As a result, Iran began secretly rebuilding its nuclear program in 1987 with the assistance of Abdul Qadeer Khan, and this continued for the next two decades.<sup>82</sup> A report from SPIEGEL International detailed the secret facility, “the Kalaye Electric watch factory in a Tehran suburb is converted into a facility to house a centrifuge, and a new, secret nuclear complex is built near Natanz, 250 kilometers south of the capital.”<sup>83</sup>

On August 14, 2002, the National Council of Resistance of Iran (NCRI), a coalition of Iranian opposition groups in exile, convened a press conference to announce that Iran had been illegally pursuing nuclear capability.<sup>84</sup> While the United States’ intelligence agencies had been informing the Institute for Science and Security (ISIS) about the existence of secret nuclear facilities in Iran, the NCRI’s information provided the evidence ISIS required to take further investigative actions.<sup>85</sup> The United States was concerned about Iran’s nuclear development, as this capability might threaten Israel’s existence and result in a shift of power in the Middle East, leading to unrest in the region as well as the rest of the world.<sup>86</sup> A statement from President George W. Bush highlighted that the

---

<sup>80</sup> Porter.

<sup>81</sup> Erich Follath and Holger Stark, “The Birth of a Bomb: A History of Iran’s Nuclear Ambitions,” *Der Spiegel*, June 17, 2010, <https://www.spiegel.de/international/world/the-birth-of-a-bomb-a-history-of-iran-s-nuclear-ambitions-a-701109.html>; and Ian Black, “Iran and Iraq Remember War That Cost More than a Million Lives,” *The Guardian*, September 23, 2010, ProQuest.

<sup>82</sup> Follath and Stark, “The Birth of a Bomb.”

<sup>83</sup> Follath and Stark.

<sup>84</sup> Alireza Jafarzadeh, “Remarks by Alireza Jafarzadeh on New Information on Top Secret Projects of the Iranian Regime’s Nuclear Program | Iran Watch,” August 14, 2002, <https://www.iranwatch.org/library/ncri-new-information-top-secret-nuclear-projects-8-14-02>.

<sup>85</sup> Zetter, *Countdown to Zero Day*, 34–44.

<sup>86</sup> Kamiński, “Operation ‘Olympic Games,’” 65.

attainment of offensive nuclear capability by Iran would be catastrophic to the world and placed Iran in the same category as Iraq and North Korea, labelling them as an “axis of evil.”<sup>87</sup>

Despite the repeated finding by the International Atomic Energy Agency (IAEA) that Iran did not adhere to the safeguard agreement of early 2006, Iran continued to provide excuses and argue that the development of its nuclear program was only for civilian purposes.<sup>88</sup> The IAEA had no choice but to declare Iran as noncompliant.<sup>89</sup> Thereafter, the UN Security Council raised multiple Resolutions—1737 (2006), 1747 (2007), 1803 (2008), and 1835 (2008)—to impose heavy sanctions and called on Iran to immediately halt all programs related to offensive nuclear capability.<sup>90</sup> Iran refused to comply and continued to develop its program, however. According to ISIS president, David Albright, by mid-2009, there were around 8,000 centrifuges installed in one of the halls of the Natanz facility.<sup>91</sup>

The noncompliance by Iran and persistent pressure by Israel left the United States with no choice but to consider offensive actions against Iran. Despite a proposal by Israel to conduct a joint strike on the Natanz facilities, the United States refused. President Bush wrote in his memoirs that “Military action would always be on the table, but it would be my last resort.”<sup>92</sup> Instead, the United States offered Israel the opportunity to participate in a joint covert operation that would slow Iran’s nuclear program via a cyberattack.<sup>93</sup>

---

<sup>87</sup> Office of the Press Secretary, “President Delivers State of the Union Address,” The White House, January 29, 2002, <https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html>.

<sup>88</sup> Zetter, *Countdown to Zero Day*, 77–83.

<sup>89</sup> Zetter, 77–83.

<sup>90</sup> Kelsey Davenport, *UN Security Council Resolutions on Iran* (Washington, D.C.: Arms Control Association, 2022), <https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran>.

<sup>91</sup> Albright et al., *Preventing Iran from Getting Nuclear Weapons*, 12–13.

<sup>92</sup> MacAskill and McGreal, “George Bush’s Memoirs Reveal How He Considered Attacks on Iran and Syria.”

<sup>93</sup> Kamiński, “Operation ‘Olympic Games,’” 66.

## C. PLANNING AND EXECUTION

### 1. Stuxnet

Stuxnet is a codename for a malware (i.e., a worm) that was discovered in Belarus in June 2010 by a firm called “VirusBlokAda.”<sup>94</sup> Designers of Stuxnet leveraged the knowledge obtained from the intelligence community and cyberspace domain to develop a weapon capable of attacking the physical, virtual, and cognitive dimension of its target.<sup>95</sup> After months of examining the Stuxnet worm, Symantec Security Response Supervisor Liam O’Murchu and his team reverse engineered the code and provided a detailed report.<sup>96</sup> He stated, “we’ve definitely never seen anything like this before... the fact that it can control the way physical machines work is quite disturbing.”<sup>97</sup>

The total count of computers infected by Stuxnet exceeded 60,000.<sup>98</sup> More than half of the infected computers were found in Iran; other countries affected included Australia, Azerbaijan, China, Finland, Germany, India, Indonesia, Malaysia, South Korea, the United Kingdom, and the United States. The spread of Stuxnet was the result of a larger joint operation by the United States and Israel, codenamed Olympic Games.

### 2. Covert Operation

Operation Olympic Games was a covert operation to undermine Iran’s nuclear ambitions.<sup>99</sup> The main purpose of the operation was not to destroy the facilities but to delay

---

<sup>94</sup> Zetter, *Countdown to Zero Day*, 5, and Kupreev Oleg and Ulasen Sergey, “Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.Gen.2 Review” (VirusBlokAda, July 2010), [https://archive.f-secure.com/weblog/archives/new\\_rootkit\\_en.pdf](https://archive.f-secure.com/weblog/archives/new_rootkit_en.pdf).

<sup>95</sup> It would be elaborated in later paragraphs that the worm caused physical damage to centrifuges, corrupt the software controlling the nuclear plants, and caused confusion among Iranian nuclear scientists.

<sup>96</sup> Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32. Stuxnet Dossier*, Version 1.3 (Cupertino, CA: Symantec Security Response, 2011), [https://www.wired.com/images\\_blogs/threatlevel/2010/11/w32\\_stuxnet\\_dossier.pdf](https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf).

<sup>97</sup> Robert McMillan, “Siemens: Stuxnet Worm Hit Industrial Systems,” *Computerworld*, September 14, 2010, <https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html>.

<sup>98</sup> James P. Farwell and Rafal Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival* 53, no. 1 (February 2011): 23, <https://doi.org/10.1080/00396338.2011.555586>.

<sup>99</sup> Nakashima and Warrick, “Officials Say U.S., Israel Were behind Cyberattack on Iran.”

the program for as long as possible. As a former CIA officer on Iran explained to The Daily Telegraph:

The goal is delay, delay, delay until you can come up with some other solution or approach. We certainly don't want the current Iranian government to have those weapons. It's a good policy, short of taking them out militarily, which probably carries unacceptable risks.<sup>100</sup>

To achieve the outcome, the attackers had to affect the production of uranium without the attention of the scientists.<sup>101</sup> First, according to Sanger, the malware had to leap the air gap systems to infect the computer network.<sup>102</sup> This could be done by a knowing or unknowing scientists, engineers or other personnel that had access to the nuclear facilities, inserting a thumb drive into the computer in Natanz. Second, they altered the code to collect intelligence and control the PLCs such that they affected the production of the enriched uranium, which was a substance essential for development of nuclear weapons. Third, they spoofed the monitoring system to indicate normal operations.<sup>103</sup> The poor yielding of enriched uranium despite “normal” operation sowed confusion among the Iranian scientists such that they would think they were incapable of running the nuclear facilities. Because this operation was intended to occur over an extended duration, its impact was random and mild so as not to arouse suspicion. An article from The Washington Post on June 2012 highlighted this intent: “The idea was to string it out as long as possible... If you had wholesale destruction right away, then they generally can figure out what happened, and it doesn't look like incompetence.”<sup>104</sup>

For simplicity, this operation can be broken down into two distinct phases. The first phase was conducted during President George W. Bush's administration, and the second phase was conducted during President Barack Obama's administration.

---

<sup>100</sup> Philip Sherwell, “Israel Launches Covert War against Iran,” *The Daily Telegraph*, February 16, 2009, ProQuest.

<sup>101</sup> Zetter, *Countdown to Zero Day*, 323–27.

<sup>102</sup> David E Sanger, “Obama Order Sped Up Wave Of Cyberattacks Against Iran,” *New York Times*, June 1, 2012, 194–95, ProQuest.

<sup>103</sup> David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), 198–200.

<sup>104</sup> Nakashima and Warrick, “Officials Say U.S., Israel Were behind Cyberattack on Iran.”

*a. Phase 1*

In 2007, President Bush reportedly requested and received \$400 million from Congress to fund a highly classified covert operation that would expand the U.S. effort to destabilize Iran's ruling regime.<sup>105</sup> The primary objective, according to a report from the Washington Post, was "gathering intelligence on Iran's nuclear program as well as assisting Iranian opposition groups in their bid to undermine the current regime."<sup>106</sup>

According to Kim Zetter, Stuxnet was reportedly part this covert operation.<sup>107</sup> While the expansion of funding only occurred in 2007, it was reported that preparation for the operation had commenced long before that. Zetter believed that the U.S. had the Stuxnet code ready by then and only pulled it out in 2006 when the diplomatic means had failed to coerce Iran into terminating their nuclear program.<sup>108</sup> One such indicator was that the timestamps of the codes that were injected into the PLCs were compiled between 2000 and 2003.<sup>109</sup>

During the development phase in the early 2000s, intelligence agencies such as the CIA were already actively collecting information on Iran's nuclear facilities.<sup>110</sup> They had information on the companies that supported Iran's nuclear program.<sup>111</sup> Coupled with the lists of equipment procured for the Natanz facilities obtained during an inspection conducted by IAEA in 2003, the facility information was sufficient to commence initial works.<sup>112</sup> Equipment lists were insufficient for a robust and foolproof attack, however. Detailed information about the facilities such as the frequency of the key components, exact configuration of the equipment, network layout of Natanz's computers, and details

---

<sup>105</sup> Joby Warrick, "U.S. Is Said to Expand Covert Operations in Iran; Plan Allows Up to \$400 Million for Activities Aimed at Destabilizing Government," *The Washington Post*, June 30, 2008, ProQuest.

<sup>106</sup> Warrick.

<sup>107</sup> Zetter, *Countdown to Zero Day*, 308–9.

<sup>108</sup> Zetter, 310–12.

<sup>109</sup> Zetter, 310.

<sup>110</sup> Zetter, 311.

<sup>111</sup> Zetter, 311.

<sup>112</sup> Zetter, 312.

of Step 7 software,<sup>113</sup> were needed to design the code with such sophistication.<sup>114</sup> As such, further intelligence collection on the facilities commenced. While the details of the collection process have not been disclosed, there is certainty that the intelligence collection was complete, and the attackers had all the information they needed to develop the code to achieve the desired outcome. Once this information had been obtained, the codes could be fully developed and compiled.

But how can the attacker be confident in the effects of the codes they created? The answer was to test the code on the actual centrifuges. A report from 16 January 16, 2011 *New York Times* states:

By early 2004, a variety of federal and private nuclear experts assembled by the Central Intelligence Agency were calling for the United States to build a secret plant where scientists could set up the P-1's and study their vulnerabilities. 'The notion of a test bed was really pushed,' a participant at the C.I.A. meeting recalled.<sup>115</sup>

A few conditions were needed for this test. First, was the availability of the actual centrifuge. According to a report from the Independent in December 2003, Libya had given up its nuclear ambition in exchange for sanctions to be lifted.<sup>116</sup> Jo Warrick reported in the Washington Post that the materials turned over by Libya included machine parts used for enriching uranium weighing up to 50,000 pounds.<sup>117</sup> According to Sanger, those parts included P-1 that were the same model as those used in the Natanz facilities.<sup>118</sup> These centrifuges were housed and used for testing at Oak Ridge National Laboratory. With the availability of these devices, an exact replica of the Natanz facilities could now be set up

---

<sup>113</sup> Step 7 is the software used for programming the programmable logic controllers (PLC) of the Natanz facility's centrifuges.

<sup>114</sup> Zetter, *Countdown to Zero Day*, 313.

<sup>115</sup> William J. Broad, John Markoff, and David E. Sanger, "Israel Tests Called Crucial In Iran Nuclear Setback," *New York Times*, January 16, 2011, ProQuest.

<sup>116</sup> Nigel Morris and Andrew Buncombe, "Libya Gives up Nuclear and Chemical Weapons," *The Independent*, December 20, 2003, <https://www.independent.co.uk/news/world/politics/libya-gives-up-nuclear-and-chemical-weapons-83350.html>.

<sup>117</sup> Joby Warrick, "U.S. Displays Nuclear Parts Given by Libya; Abraham Calls Haul A 'Big, Big Victory,'" *The Washington Post*, March 16, 2004, ProQuest.

<sup>118</sup> Sanger, *Confront and Conceal*, 197–98.

for testing. Second, a team of materials scientists and centrifuge experts were assembled for these tests.<sup>119</sup> Testing began subsequently and codes were adjusted such that the desired outcome was achieved. After the proof of concept was completed, the findings were presented to President Bush and the first ever cyberweapon was finally ready to be launched.<sup>120</sup> According to a report by Langner, the initial version of Stuxnet—version 0.5—appeared in the field in 2007.<sup>121</sup>

The report from Symantec explained that Stuxnet version 0.5 could only be spread by infecting Step 7 project files and was believed to have spread in the same manner where the intelligence was collected.<sup>122</sup> According to Zetter, once the Step 7 files were infected, they were copied with new codes to provide 417 PLCs with new commands.<sup>123</sup> He added that the main target for this version of Stuxnet was the valve of the centrifuges. The worm caused the centrifuge valves to open and close at abnormal rates to disrupt the flow of uranium gas, causing pressure buildup within the centrifuges and affecting the yield of enriched uranium gas.

According to Zetter, the attackers had ingeniously designed the code to avoid detection.<sup>124</sup> First, Zetter reported that the code did not unleash the attack immediately. It observed and collected data until certain conditions were met before commencing the attack. Second, he added that each time an attack took place, it only lasted for a short duration (two hours) and did not affect all the centrifuges at the same time. The algorithm was created such that the attacks were random.<sup>125</sup> Third, Zetter explained that, during the attack, the reading of the pressure on the monitoring systems was tampered with such that

---

<sup>119</sup> Zetter, *Countdown to Zero Day*, 316.

<sup>120</sup> Zetter, 322.

<sup>121</sup> Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (Arlington, Hamburg, Munich: The Langner Group, 2013), 5, <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.

<sup>122</sup> Falliere, Murchu, and Chien, *W32. Stuxnet Dossier*, 3.

<sup>123</sup> Zetter, *Countdown to Zero Day*, 323.

<sup>124</sup> Zetter, 322–27.

<sup>125</sup> Zetter, 325.

they always reflected a normal reading.<sup>126</sup> Fourth, Zetter stated that the code disabled the safety systems that were supposed to isolate the centrifuges before they could cause damage.<sup>127</sup> The combination of these measures was believed to have caused a great deal of confusion among technicians in the Natanz facilities as they could not pinpoint the cause or detect any pattern for the issues they were facing.

From an ISIS report in 2010, it indicated that Natanz did not have a consistent production of enriched uranium between 2007 and 2009.<sup>128</sup> The erratic behavior of the centrifuges continued to frustrate the Iranians.<sup>129</sup> Whenever the Iranians thought they had sufficient understanding of the enrichment process and began to scale things up rapidly, they encountered another problem. For example, from May to November 2008, Iran had increased the number of centrifuges from 3280 to 3772.<sup>130</sup> Shortly after, they were faced with issues of centrifuges failing and poor yield of the enriched gas. From November 2008 to February 2009, only a few centrifuges were added.<sup>131</sup> In 2009, Iran added new centrifuges to the facilities, but they were not fed with gas. According to Zetter, while no one could be sure that Stuxnet 0.5 was the main reason for these failures, the problems that arose from the facilities seemed to be consistent with its design.<sup>132</sup>

#### ***b. Phase 2***

When President Barack Obama assumed the presidency in 2009, he was briefed on Operation Olympic Games by outgoing President George W. Bush.<sup>133</sup> Given that diplomatic means were not working out and the unwillingness to pursue military action,

---

<sup>126</sup> Zetter, 325.

<sup>127</sup> Zetter, 326.

<sup>128</sup> David Albright and Christina Walrond, *Iran's Gas Centrifuge Program: Taking Stock*, Iran Reports (Washington, D.C.: ISIS, 2010), <https://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock/8>.

<sup>129</sup> Zetter, *Countdown to Zero Day*, 327–32.

<sup>130</sup> Albright and Walrond, *Iran's Gas Centrifuge Program: Taking Stock*.

<sup>131</sup> Albright and Walrond.

<sup>132</sup> Zetter, *Countdown to Zero Day*, 327–32.

<sup>133</sup> Sanger, *Confront and Conceal*, 200–201.

Obama reauthorized the operation. With the pressure to see results and the worry that Israel might take matters into its own hands, however, time was not in the President's favor. As such, he accelerated the development of Stuxnet.<sup>134</sup> The aim was to set Iranian nuclear development back more effectively and sow more confusion among the Iranian scientists.

This variant, Stuxnet 1.001, targeted frequency converters instead of only the valves, which was a faster and more direct attack.<sup>135</sup> It had an initial reconnaissance period of 13 days (similar to Stuxnet 0.5) before launching an attack. Then, it would increase the frequency of the converters to 1,410 Hz for fifteen minutes before returning them to the normal operating frequency of 1,046 Hz for 26 days. During this time, it would collect data on the setup. Next, it would launch a second attack by dropping the frequency to 2 Hz for 15 minutes, then return it to normal frequency. After another 26 days, the attack sequence repeated itself. Similar to Stuxnet 0.5, this variant also fed false information into the monitoring system and disabled the safety system.<sup>136</sup>

Symantec's report indicates that Stuxnet 0.5 was only able to infect Step 7 project files, but it had two additional means of propagating the worm.<sup>137</sup> One of these methods involved spreading through USB flash drives with the assistance of the Windows Autorun feature. The other technique involved utilizing the print spooler zero-day exploit to infect a victim's local network.<sup>138</sup>

Report from Dark Reading indicates that the code was launched in June 2009 to five companies with connections to the Natanz facilities including Behpajoo and Neda.<sup>139</sup> It was believed that the code managed to reach the facilities and delivered the attack

---

<sup>134</sup> Sanger, "Obama Order Sped Up Wave Of Cyberattacks Against Iran."

<sup>135</sup> Zetter, *Countdown to Zero Day*, 235.

<sup>136</sup> Zetter, 235.

<sup>137</sup> Falliere, Murchu, and Chien, *W32. Stuxnet Dossier*, 21–28.

<sup>138</sup> Falliere, Murchu, and Chien, 21–28.

<sup>139</sup> Sara Peters, "Stuxnet 'Patient Zero' Attack Targets Revealed," *Dark Reading*, November 11, 2014, sec. attacks-breaches, <https://www.darkreading.com/attacks-breaches/stuxnet-patient-zero-attack-targets-revealed>.

sequences. By the end of 2009, the number of centrifuges enriching uranium was reduced to 3772, which is a reduction of about 23% compared to June 2009.<sup>140</sup>

Even with the effects from Stuxnet 1.001, the pressure on the U.S. to halt Iran's nuclear program was still growing. It was made worse when another enrichment facility—the Fordow plant—was discovered by U.S. intelligence in September 2009.<sup>141</sup> While it was a smaller plant compared to Natanz, it posed a greater threat because it was secretly held at a military base, underground without IAEA's knowledge. In the wake of the discovery, Israel further pressured the U.S. to take action with regard to Iran's nuclear program. In March 2010, President Obama decided to launch another attack. According to Zetter, “the payload was identical to the one unleashed the previous June, but this version included the larger collection of zero-day exploits and other spreading mechanisms, including the .LNK exploit that ultimately led to its discovery.”<sup>142</sup>

Unfortunately, the effect of the 2010 attack remains unknown. This was because IAEA stopped publishing detailed information to the media following threats from Iran to withdraw its approval for IAEA's inspection.<sup>143</sup>

#### **D. ANALYSES**

Operation Olympic Games saw the first use of a cyberattack reportedly sponsored by the United States and Israel. Applying the tenets from the conceptual model in Chapter II, this segment will examine the enabling conditions that resulted in the integration of the highly sophisticated malware into a covert operation as well as the outcome of the integration presented in terms of risk and effectiveness.

With reference to Table 1, the overall synergistic relationship for the integration between advanced technology and SO is assessed to be positive for Operation Olympic

---

<sup>140</sup> Zetter, *Countdown to Zero Day*, 337–44.

<sup>141</sup> Ian Traynor and Julian Borger, “Iran Admits Secret Uranium Enrichment Plant,” *The Guardian*, September 25, 2009, <https://www.theguardian.com/world/2009/sep/25/iran-admits-uranium-plant>.

<sup>142</sup> Zetter, *Countdown to Zero Day*, 349.

<sup>143</sup> Zetter, 354–55.

Games. It had fulfilled the tenets of the conceptual model in Chapter II. Details will be provided in subsequent segments.

Table 1. Summary of Integration Between Special Operations and Technology in Operation Olympic Games

| <b>Integrating cyberattack with a covert operation</b>            |          |
|-------------------------------------------------------------------|----------|
| <u>Specs Ops – Advanced Technology Integration</u>                |          |
| Is it a Special Operation?                                        | Yes      |
| Does it use Advanced Technology?                                  | Yes      |
| <u>Enabling Conditions</u>                                        |          |
| Does this integration have a clear purpose?                       | Yes      |
| Is the technology compatibility with Special Operation?           | Yes      |
| Is there integration effort?                                      | Yes      |
| <u>Outcome</u>                                                    |          |
| Is it effective for the mission?                                  | Yes      |
| Does it reduce risk to mission/force?                             | Yes      |
| <u>Overall synergistic relationship</u>                           |          |
| What is the synergistic relationship for the emergent capability? | Positive |

## 1. Integration of Special Operations and Advanced Military Technology

It has been more than a decade since Stuxnet was launched as part of Operation Olympic Games. Today, it remains a classic example of a kinetic cyberattack. Examining this operation using the definition of SO adopted in Chapter II, Operation Olympic has displayed all the tenets of a SO, as seen in Table 2.

Table 2. Qualifying Operation Olympic Games as Special Operations<sup>144</sup>

| <b>Special Operations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|------------------------------------------------------------------------------------------------|
| Definition: “Small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.” |                            |                                                                                                |
| Key Tenets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Demonstrated in Operation? | Elaboration                                                                                    |
| Small scale, clandestine, <b>covert</b> or overt operation                                                                                                                                                                                                                                                                                                                                                                                                                                           | Yes                        | It is a <b>covert</b> operation where the effects could be seen but the actors remain unknown. |
| Unorthodox                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Yes                        | First use of a kinetic cyberweapon.                                                            |

<sup>144</sup> Adapted from: Tugwell and Charters, “Special Operations and the Threats to United States Interests in the 1980s,” 35.

| <b>Special Operations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Definition: “Small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.” |                                   |                                                                                                                                     |
| <b>Key Tenets</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Demonstrated in Operation?</b> | <b>Elaboration</b>                                                                                                                  |
| High-risk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Yes                               | Risk of mission failure is high if the code is detected.                                                                            |
| <b>Significant political</b> or military objectives in support of foreign policy                                                                                                                                                                                                                                                                                                                                                                                                                     | Yes                               | Iran’s nuclear program needs to be delayed urgently because they may pose a threat to the region where U.S. allies may be affected. |
| Oversight at the highest level                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Yes                               | President Bush and President Obama authorized the covert operation.                                                                 |
| Use of military and non-military resources, including intelligence assets                                                                                                                                                                                                                                                                                                                                                                                                                            | Yes                               | Entities from intelligence community, coders, nuclear scientist, material engineers were reported to be involved in the operations. |

In terms of advanced military technology, Stuxnet was the key to the execution of Operation Olympic Games. While the ability to use cyberspace to attack computers systems has existed, it had never been used in a SO to produce a kinetic effect. The common understanding for using technology in SO generally involved equipment to help a SOF team to achieve their mission more effectively. This is supported by SOF Truths #1, “Humans are more important than hardware.”<sup>145</sup> For the case of Stuxnet, however, the technology was the primary attack capability and effector for the operation. The various entities (intelligence agencies, coders, engineers, etc.) were assembled to support the development as well as the delivery of the technology. This is a demonstration of the integration of SO and advanced military technology to a different level. At this level, technology is equally as important as, if not more important than, humans.

## **2. Enabling Conditions**

### ***a. Purpose***

The purpose for selecting a cyberattack by the United States and Israel compared to a raid by SOF or airstrike was clear. The diplomatic means against Iran had not been effective after several years of trying. A raid by SOF and airstrikes posed a high risk to the

<sup>145</sup> “SOF Truths,” USSOCOM, accessed April 6, 2023, <https://www.socom.mil/about/sof-truths>.

force and there was a potential risk of escalation in doing so. A covert cyberattack will minimize these risks and gradually slow Iran's nuclear ambition.

The purpose had changed when President Obama decided to take a more aggressive approach to speed up the effects of the destruction, however, following pressure from Israel. The original intent of conducting the entire operation in secrecy become a challenge because the design of Stuxnet 1.001 was "highly contagious" and the exposure to public computers could not be prevented, therefore leading to its detection by the cybersecurity community and attribution to the United States and Israel.

***b. Integration Effort***

The integration effort of Operation Olympic Games demonstrated the United States' and Israel's willingness to execute the operation. Supports were given by the highest authority, President George W. Bush and later President Barack Obama, during the leadup to the attacks. The amount of 400 million U.S. dollars that President Bush requested from Congress was a significant amount considering the operation was a cyberattack with no force physically present in Iran. Cross-department sharing of classified information on the Natanz facilities between intelligence agencies and coders could not have taken place if there were no strong push to fulfill the operation. Furthermore, setting up a full replica of the Iran nuclear facilities to test the effect of the Stuxnet worm showed the desire to understand every possible outcome from the operation.

One of the most significant integration efforts occurred during the delivery of Stuxnet 0.5 into the system. The computer systems in the Natanz facilities run on an air-gapped network. In order to deliver the code into the network, a person, knowingly or unknowingly, had to be physically present to deliver the code via a connection to the network. While we do not know exactly how it happened, given the criticality of the operation, we can be certain that every possible effort would be taken to ensure that the source reached the target.

*c.      Compatibility*

The Stuxnet worm was a sophisticated technology that was highly compatible with the covert operation to delay Iran's nuclear program. The entire process to design code to generate deceptive and destructive effect on computer systems in the Natanz facilities, based on intelligence gathered, required a high level of technical compatibility. Software, like Step 7, was controlling the activities in the uranium enrichment process. The ability to alter the Step 7 codes without detection essentially allowed the attacker to tailor the desired effect they aimed to deliver to the facilities. Such ability was demonstrated in both Stuxnet 0.5 and 1.001 as the valves of the systems and the frequency of the centrifuges were adjusted to run at an irregular tempo. Furthermore, the same code was able to deceive the monitoring and safety systems, feeding false information indicating normal operation.

**3.      Outcomes**

To recap, the assessment of the outcome of the operation is based on two criteria: risk and effectiveness (see Chapter II). Also, the strategy should not be viewed from the methods used in isolation; it has to be compared to the alternatives available. More often than not, scholars have been quick to criticize the methods used and to emphasize the shortfalls but have failed to recognize that it may have been the best solution for that situation.

*a.      Risk*

The risk of Operation Olympic Games can be viewed in two levels: risk to force and risk to mission, which also includes risk of collateral damage. In terms of risk to the force, it was very minimal. The fact that the mission was conducted outside of Iran, except for intelligence collection and the process to deliver the code, significantly reduced the exposure of any U.S. force to Iran's security forces to a minimum. The alternative of a raid by SOF or airstrike would have required U.S. forces to physically infiltrate the Iranians' defense system (i.e., security forces, security cameras, air radars, etc.). In terms of risk to the mission, using cyberattack offered a low risk.

The main risk to the mission was the management of the operations security (OPSEC). At the point of the attack, it would be close to impossible for the Iranians to know the issues behind their nuclear facilities because the unorthodox method of kinetic cyberattack had not ever existed. Hence, the attacker could maintain the strategic surprise over the Iranians until the discovery of the worm. To this end, a poor OPSEC management could have jeopardized the mission, negating the effects caused by Stuxnet.

Next, the risk of collateral damage for the mission was high, especially during phase 2 of the operation, when President Obama had increased the “lethality” of Stuxnet after the U.S. was pressured to halt Iran’s nuclear ambitions. The creation of code that could have spread via multiple means indicates that the infection to Iran’s nuclear facilities was a game of probability, i.e., the more external computers of the chosen companies infected, the likelier one or a few of the computers would be connected to the network in Iran’s nuclear facilities and infect the computers within.<sup>146</sup> This game of probability also caused the highly infectious code to spread to 60,000 public computers, however. Minimizing collateral damage was probably never the aim of the mission. To support this claim, according to Zetter, “Obama’s advisors had reminded him that Stuxnet was a precision weapon designed to only unleash the payload under very specific condition, and it would not harm other infected computers.”<sup>147</sup>

#### ***b. Effectiveness***

Assessing the effectiveness of Operation Olympic Games is a highly subjective endeavor. Proponents such as David Albright believed that the mission of delaying Iran’s nuclear ambition was achieved. His view is supported by the fact that the Natanz facilities were only operating at less than one-third of their capacity after a decade of operation.<sup>148</sup> Furthermore, according to Yossi Melman, the timeline of Iran obtaining nuclear weapons

---

<sup>146</sup> The chosen companies are those believed to have worked closely with the Iran nuclear facilities. For example, Behpajoo and Neda Industrial Group.

<sup>147</sup> Zetter, *Countdown to Zero Day*, 357.

<sup>148</sup> David Albright and Andrea Stricker, “Iran’s Nuclear Setbacks: A Key for U.S. Diplomacy,” *PBS*, January 19, 2011, <http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2011/01/irans-nuclear-setbacks-a-key-for-us-diplomacy.html>.

was believed to be pushed back from 2007 to 2015.<sup>149</sup> Opponents, on the other hand, do not believe Stuxnet was effective due to the increased rate of production of enriched uranium despite the Stuxnet attack happening. According to an interview by Szoldra, “so whoever initiated this—and was very proud of themselves to see that little dip in Iran’s centrifuge numbers—should look back now and acknowledge it was a major mistake.”<sup>150</sup>

Viewed from the lens of using airstrikes and SOF raid as alternatives, while they may have caused a greater destruction to the facilities, they may also have triggered the Iranians to retaliate with offensive action. The use of a covert operation prevented an escalated response.

A critique on the effectiveness was that Stuxnet’s effect was short-lived and the same weapon cannot be used again. Stuxnet delayed Iran’s nuclear program up to the point at which the worm was discovered. After that, a patch was made available to prevent further attacks from the worm. Now that the world has learned about the cyberweapon, it would be challenging to repeat this technique with the expectation that it would not be discovered, hence limiting its effectiveness in the long run.

When considering an alternative perspective, however, the wide spread of the worm to public computers could be effective if its purpose was covert signaling. It is plausible that the worm was intentionally released to both the public and Iran as a means of signaling to Iran and other rogue states with illicit nuclear ambitions. In this context, the code would need to demonstrate its capability to spread extensively and its potency in destroying targeted systems, serving as a deterrent to other rogue actors pursuing nuclear ambitions.

## **E. CONCLUSION**

Operation Olympic Games demonstrated the creative integration of advanced technology with SO could provide strategic options for policymakers. Specifically, the use

---

<sup>149</sup> Yossi Melman, “Outgoing Mossad Chief: Iran Won’t Have Nuclear Capability before 2015,” *Haaretz*, January 7, 2011, <https://www.haaretz.com/2011-01-07/ty-article/outgoing-mossad-chief-iran-wont-have-nuclear-capability-before-2015/0000017f-e993-dea7-adff-f9fba1f80000>.

<sup>150</sup> Paul Szoldra, “A New Film Gives a Frightening Look at How the U.S. Used Cyberwarfare to Destroy Nukes,” *Business Insider*, July 7, 2016, <https://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016-7>.

of cyberattack to destroy uranium enriching facilities and sow confusion among Iranian scientists without sending physical forces on the ground was commendable.

This integration incorporated all the tenets in the conceptual model (see Chapter II), producing a positive emergent capability that led to an overall synergistic outcome. The only critique was with regard to the collateral damage that resulted in 60,000 computers infected with Stuxnet, which eventually led to its discovery and attribution to the United States and Israel. The change in purpose to speed up the destruction during President Obama's administration was probably the root cause and the result was an increased risk to the mission (i.e., creating opportunity to attribute blame to the attackers) and a reduced effectiveness (i.e., incapability of further destruction once the patch was developed).

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. OPERATION ORCHARD

### A. INTRODUCTION

Syria's development of nuclear weapons is a pressing existential threat to the region, particularly Israel, with whom it has had a longstanding animosity. To counter this threat, Israel launched Operation Orchard in 2007, a sophisticated air strike coupled with EW tactics, to destroy Syria's nuclear reactor near al-Kibar in the Deir ez-Zor Province along the Euphrates River. Israel's primary reason for the attack was the potential for a war to break out between Syria and Israel, so Israel executed a precise and covert attack on the nuclear reactor, aiming to destroy it without causing collateral damage to other critical infrastructure.

The success of the operation meant that Syria was faced with a difficult choice: either go to war with Israel and face international condemnation for illegally pursuing a nuclear program or downplay the attack and deny the development of nuclear weapons. To Israel's relief, Syria chose the latter.<sup>151</sup> This outcome helped to prevent a possible escalation of conflict between the two nations and served as a deterrent to other countries in the region pursuing nuclear weapons.

The success of the operation was primarily due to the seamless integration of advanced technology and SO by Israel. Specifically, Israel utilized advanced EW to manipulate Syria's integrated air defense systems (IADS), which enabled a covert and surgical airstrike on al-Kibar that was swift, precise, and localized.

This chapter will provide background information on the events leading up to Israel's decision to attack the nuclear reactor. It will then delve into the details of the three key missions planned and executed by Israel to eliminate Syria's nuclear capabilities, namely the hotel raid on Ibrahim Othman by the Mossad, the soil sample collection in the vicinity of al-Kibar by Sayeret Matkal, and the airstrike (supported by EW technology) on

---

<sup>151</sup> Hugh Naylor, "Syria Tells Journalists Israeli Raid Did Not Occur," *New York Times*, October 11, 2007, <https://www.nytimes.com/2007/10/11/world/middleeast/11syria.html?ref=world>.

al-Kibar by the Raam and Sufa fighter squadrons. Detailed analysis will be conducted on the integration of EW into the airstrike, using the conceptual model from Chapter II to provide insights on the enabling conditions and outcomes of this approach in achieving Israel's objectives.

## **B. BACKGROUND**

After the death of Syrian leader Hafez Assad's oldest son, Bassel Assad, in 1994, his other son, Bashar, returned to Syria to undergo military training as the next potential candidate to succeed his father in heading the Syrian regime. Israel's intelligence agency, the Mossad, did not see Bashar as a likely candidate as he was seen as being more modern than Bassel—for example, he had Christian friends and had pursued postgraduate degree studies in ophthalmology.<sup>152</sup> After Hafez Assad's death in 2000, Bashar, at the age of 34, won the presidency of Syria with 97.29 percent of the vote, being the only candidate.<sup>153</sup> When Bashar first took over, he was seen by the Syrian people as a reformer and was expected to be more moderate than his father, who was seen as a ruthless leader.<sup>154</sup> Bashar was no different, however, or was in fact worse than his father. In the years to come, Basher killed over 500,000 Syrians to ensure his own survival.<sup>155</sup>

After Bashar Assad took over as President, there were suspicions by Israel that Syria had been conducting illicit activities with North Korea but the evidence was insufficient.<sup>156</sup> For instance, according to Klieger, there were sign of cooperation between Syria and North Korea when an advanced weapons system was delivered to Syria in 2001.<sup>157</sup> Klieger also noted that intelligence suspected that a nuclear weapon was also part

---

<sup>152</sup> Yaakov Katz, *Shadow Strike: Inside Israel's Secret Mission to Eliminate Syrian Nuclear Power* (New York: St. Martin's Press, 2019), 192–94.

<sup>153</sup> David W. Lesch, *Syria: The Fall of the House of Assad* (New Haven, CT: Yale University Press, 2012), 3.

<sup>154</sup> Katz, *Shadow Strike*, 190.

<sup>155</sup> Katz, 213.

<sup>156</sup> Katz, 203–9.

<sup>157</sup> Noah Klieger, "A Strike in the Desert," *Ynetnews*, November 2, 2009, <https://www.ynetnews.com/articles/0,7340,L-3799227,00.html>; and Katz, *Shadow Strike*, 209.

of the agenda between the two nations. This suspicion was dismissed because Israel was in the middle of peace talks with Palestine and Syria, however, so that suspicion did not fall into the narrative.<sup>158</sup> Another trigger came again in 2004, according to Katz, when Israel identified an unusual government building in the middle of nowhere in the desert area of al-Kibar. Katz added that Amos Yadlin, Head of Aman, held strong suspicion over the possibility of illicit nuclear weapons in Syria and persuaded Mossad to gather more evidence.

The suspicion by Yadlin was confirmed after the shocking discovery of the evidence following the raid on Ibrahim Othman, director of Syria's Atomic Energy Commission in Vienna.<sup>159</sup> The opportunity for intelligence gathering arose when Othman was attending meetings in Vienna. According to Makovsky, Mossad conducted a raid in March 2007 on a Vienna hotel where Othman was staying, and the results were shocking.<sup>160</sup> A report by Der Spiegel reported that the raid was targeted at Othman's computer and in his hard drive, it contained photos, letters, and construction plans of the al-Kibar nuclear reactor.<sup>161</sup> These photographs confirmed Israel's suspicion that the building at al-Kibar was a highly classified plutonium nuclear reactor.<sup>162</sup> The photographs depicted North Korean workers present at the site, which was located far away from Syria's major cities. According to Mossad's analysis, the reactor's sole purpose was to manufacture an atomic bomb.<sup>163</sup> The reactor's internal design bore many similarities to the North Korean reactor in Yongbyon, which had been constructed exclusively by North

---

<sup>158</sup> Klieger, "A Strike in the Desert"; and Katz, *Shadow Strike*, 209.

<sup>159</sup> Katz, *Shadow Strike*, 39–41.

<sup>160</sup> David Makovsky, "The Silent Strike," *The New Yorker*, September 10, 2012, <https://www.newyorker.com/magazine/2012/09/17/the-silent-strike>.

<sup>161</sup> Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel*, November 2, 2009, <https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html>.

<sup>162</sup> Yossi Melman, "Outside The Box: Israel's Strike on Syria's Nuclear Plant," *The Jerusalem Post*, April 6, 2018, <https://www.jpost.com/arab-israeli-conflict/outside-the-box-israels-strike-on-syrias-nuclear-plant-547870>.

<sup>163</sup> Makovsky, "The Silent Strike."

Korea within the past 35 years. Mossad Chief Meir Dagan then presented the critical piece of information to Ehud Olmert, Prime Minister of Israel, with urgency.

Olmert was clear that Syria's possession of a nuclear weapon could pose an immediate threat to Israel and was certain that it needed to be destroyed.<sup>164</sup> According to Katz, Olmert first sought U.S. assistance to understand North Korea's involvement in Syria's nuclear program and also to terminate that program.<sup>165</sup> Dagan was sent to inform the U.S. of the new revelation. Dagan met Dick Cheney, Vice President of the U.S., and Stephen Hadley, National Security Advisor, to explain to them that Syria had been secretly building a nuclear reactor.<sup>166</sup> He supported this statement with the photographs that were obtained from the hotel raid, including a picture of Chon Chibu, a key nuclear scientist for North Korea, and Othman.

The U.S. had to confirm the intelligence through their own intelligence agencies and consider the possible responses to Israel's request. According to Makovsky, President Bush directed his team to confirm the intelligence and come up with a proposal on what to do with the reactor.<sup>167</sup> While Israel's evidence was convincing, the U.S. undertook extensive efforts to verify the intelligence through their own channels. During that time, the U.S. was particularly skeptical about any intelligence due to their recent intelligence failure in Iraq.<sup>168</sup> For the intelligence agency, after cross examination of the evidence, Director of the CIA Michael Hayden presented the findings and everyone was convinced that Syria was building a nuclear reactor.<sup>169</sup> There was one caveat, however. The team could not identify the weapons team capable of assembling a weapon or warhead. Hence, Hayden concluded his finding of Syria's nuclear weapon effort as "low confidence." On

---

<sup>164</sup> Katz, *Shadow Strike*, 43.

<sup>165</sup> Katz, 29 and 47.

<sup>166</sup> Katz, 15–17.

<sup>167</sup> Makovsky, "The Silent Strike."

<sup>168</sup> Makovsky.

<sup>169</sup> Katz, *Shadow Strike*, 53.

the other end, a drafting group, consisting of principal deputies and overseen by Stephen Hadley, National Security Adviser, came up with three possibilities.<sup>170</sup> According to Katz,

The group came up with three rough tracks. The first was the most straightforward: simply attack. The second was not to attack but to extend Israel any assistance it might need in carrying out the strike on its own. The third was to expose Syria's nuclear violation by revealing the existence of the reactor to the United Nations Security Council and the International Atomic Energy Agency (IAEA).<sup>171</sup>

The U.S. had decided that the most appropriate response was to pursue a diplomatic response; if that failed, a military option was backup.<sup>172</sup> The drafting group had disagreement between the diplomatic and military options. Cheney urged the military option but Secretary of Defense Robert Gates and Secretary of State Condoleezza Rice disagreed. After Hayden's team reported the intelligence was low confidence, however, diplomacy seemed the clear first choice. A military option would only come into play if diplomacy failed. Cheney concluded later that the intelligence failure on Iraq continued to affect the U.S.'s decision making even though the evidence was credible.<sup>173</sup>

Israel disagreed with the U.S. proposal and made the decision to destroy the target by themselves.<sup>174</sup> When Bush informed Olmert of the U.S.'s position, the prime minister was disappointed and disagreed with the proposal, finding it "very disturbing." The prime minister said, "Mr. President, I understand your reasoning and your arguments, but don't forget that the ultimate responsibility for the security of the State of Israel rests on my shoulders, and I'll do what needs to be done and trust me—I will destroy the atomic reactor."<sup>175</sup> Bush respected Olmert's decision and acceded to Olmert's request to continue

---

<sup>170</sup> Katz, 47.

<sup>171</sup> Katz, 60.

<sup>172</sup> Katz, 115.

<sup>173</sup> Bruce Riedel, "Lessons of the Syrian Reactor," *The National Interest*, no. 125 (June 2013): 46, <http://www.jstor.org/stable/42896512>.

<sup>174</sup> Katz, *Shadow Strike*, 121–22.

<sup>175</sup> Katz, 121–22.

keeping the information a secret. The U.S. would continue to support Israel with intelligence cooperation but not military action.<sup>176</sup>

Israel considered two options to destroy the target and narrowed them to a surgical airstrike with minimum signature and collateral damage because the likelihood of Syria retaliating to such attack and taking escalatory actions was the lowest.<sup>177</sup> Following Bush's response, Israel was on its own with this attack. According to Makovsky, Israel developed three options to destroy Syria's nuclear reactor: the first was a land raid by commandos, the second was an extensive air strike that attacked multiple targets, and the third was a surgical air strike on the nuclear reactor only.<sup>178</sup> According to Katz, one concept that aided the decision making was the idea of "Deniability Zone" by the head of Aman's research department.<sup>179</sup> Another report by Trevithick explained that the Israelis believed that allowing Assad to maintain a plausible deniability regarding the nature of the building in al-Kibar, which was suspected to be a North Korean-designed nuclear facility, could decrease the likelihood of a retaliatory action.<sup>180</sup> Therefore, a quick and precise strike, would also limit the chances of the Syrians perceiving the operation as a precursor to a full-scale war.

After further intelligence was gathered to assess the progress of Syria's nuclear program, Israel decided they had to destroy the al-Kibar nuclear reactor before it was too late. Multiple sources reported that a clandestine reconnaissance operation was conducted by Sayeret Matkal in August 2007 to assess the progress of Syria's nuclear development.<sup>181</sup> The Israeli commandos successfully conducted the operation and returned with the required soil sample. Following the lab test, it was confirmed that the

---

<sup>176</sup> Katz, 122.

<sup>177</sup> Makovsky, "The Silent Strike."

<sup>178</sup> Makovsky.

<sup>179</sup> Katz, *Shadow Strike*, 131.

<sup>180</sup> Joseph Trevithick, "Israel Details Long Secret Raid On Syrian Nuclear Reactor, Says It's Willing To Do It Again," *The Drive*, June 30, 2019, <https://www.thedrive.com/the-war-zone/19492/israel-details-long-secret-raid-on-syrian-nuclear-reactor-says-its-willing-to-do-it-again>.

<sup>181</sup> Katz, *Shadow Strike*, 160–63; and Dan Magen, *Operation Orchard: Israel's Strike On The Syrian Reactor*, 2016, 11–15.

nuclear reactor was turning operational, and the attack had to occur soon. Additionally, as time passed before the attack, the probability of Syria becoming aware that their secret had been revealed would rise.<sup>182</sup> In such a scenario, Syria would bolster the protection of their infrastructure, thus making the attack more challenging to execute.<sup>183</sup> Israel wasted no time and Olmert ordered the airstrike following the final meeting with his security cabinet on September 5, 2007.<sup>184</sup>

The surgical airstrike was successfully conducted.<sup>185</sup> It took place on the evening of September 5, 2007, lasting for about four hours. The nuclear reactor was successfully destroyed, and all the planes returned safely. According to Fulghum and Wall, Israel also used EW to support the airstrike, which prevented Syrian air defenses from picking up the incoming attack.<sup>186</sup> The mission was a success, but Israel was worried that Assad would retaliate leading to an all-out war.<sup>187</sup> To the relief of Israel, Syria did not retaliate after the attack. Instead, on the afternoon of September 6, 2007, the Syrian Arab News Agency reported that Syrian airspace was violated by Israeli fighter jets in the morning.<sup>188</sup> It was further mentioned that “Air defense units confronted them and forced them to leave after they dropped some ammunition in deserted areas without causing any human or material damage.” Later, in a BBC interview after the attack, Assad claimed that Israel had hit “buildings and construction related to the military” but which were unused.<sup>189</sup> He added that Syria would not react militarily because by doing so, it would advance Israel’s agenda.

---

<sup>182</sup> Katz, *Shadow Strike*, 172–73.

<sup>183</sup> Melman, “Outside the Box: Israel’s Strike on Syria’s Nuclear Plant.”

<sup>184</sup> Katz, *Shadow Strike*, 178–82.

<sup>185</sup> Katz, 238–42.

<sup>186</sup> David A. Fulghum and Douglas Barrie, “Israel Used Electronic Attack in Air Strike against Syrian Mystery Target,” *ABC News*, October 8, 2007, <https://abcnews.go.com/Technology/story?id=3702807&page=1>.

<sup>187</sup> Trevithick, “Israel Details Long Secret Raid on Syrian Nuclear Reactor, Says It’s Willing to Do It Again.”

<sup>188</sup> Follath and Stark, “The Story of ‘Operation Orchard.’”

<sup>189</sup> *BBC News*. “Israel Admits Striking Suspected Syrian Nuclear Reactor in 2007,” March 21, 2018, <https://www.bbc.com/news/world-middle-east-43481803>.

The reaction from Assad fell right into Israel's playbook of deniability zone and both countries escaped an outbreak of war.<sup>190</sup>

### **C. PLANNING AND EXECUTION**

The operation to terminate Syria's nuclear program consisted of several key missions, including,

1. The hotel raid on Ibrahim Othman by Mossad
2. The soil sample collection in the vicinity of al-Kibar by Sayeret Matkal
3. The airstrike on al-Kibar by Raam and Sufa supported by EW technology

As the intent of this research is to analyze the use of advanced technology in SO, the details of the hotel raid and soil sample collection will be covered in brevity and elaborated on for the airstrike.

#### **1. The Hotel Raid on Ibrahim Othman by Mossad**

After the discovery of the strange building in the desert area of al-Kibar, Mossad sought to gather more intelligence by tracking Ibrahim Othman. According to Makovsky, the Israelis found an opportunity to collect intelligence to confirm their suspicion on Syria when Ibrahim Othman visited Vienna in March 2007.<sup>191</sup> After Prime Minister Olmert approved the mission, Mossad's Keshet branch, consisting of young men and women, was sent on a mission to break into Ibrahim Othman's hotel room.<sup>192</sup>

The Mossad operators were divided into teams.<sup>193</sup> One team, which included a female operative, was set to distract and engage Othman while he was at the bar so as to "buy time" for the second team to accomplish their task. The task of the second team was to break into his hotel room and search for evidence. They downloaded the contents of

---

<sup>190</sup> Katz, *Shadow Strike*, 241–42.

<sup>191</sup> Makovsky, "The Silent Strike."

<sup>192</sup> Katz, *Shadow Strike*, 38.

<sup>193</sup> Magen, *Operation Orchard*, 7.

Othman's laptop and transferred it back to Mossad headquarters (HQ).<sup>194</sup> They also installed a Trojan horse that enabled Mossad's HQ to track the subsequent activities on Othman's laptop. Within about 15 minutes, after the files were received by Mossad HQ, the female operative bid goodbye to Othman and both teams left the scene.<sup>195</sup>

## **2. The Soil Sample Collection in the Vicinity of al-Kibar by Sayeret Matkal**

The evidence collected from the raid of Othman's hotel room was dated, so Israel needed to ascertain the progress of al-Kibar's development. As such, Sayeret Matkal, the Israel Defense Forces (IDF) commando unit, was sent on an intelligence gathering operation.<sup>196</sup> Sayeret Matkal was known to be expert at conducting intelligence activities, including reconnaissance behind enemy lines.<sup>197</sup> The mission involved infiltrating near al-Kibar's "reactor," collecting soil samples and taking pictures in its vicinity.<sup>198</sup> It was reported that another purpose was to assess whether troops could be successfully landed in the area as a land raid remained one of the options. The risk of the mission was very high; if the mission were compromised, not only would it jeopardize Israel's chance to attack the reactor, it would also lead to a possible war between Israel and Syria.<sup>199</sup> Under normal circumstances, the elite force would receive ample time to prepare for such mission. Due to the time urgency to complete obtain the evidence, however, the preparation time was reduced.<sup>200</sup>

According to Katz, on the night of the mission, the commandos were dressed like Syrian soldiers, complete with AK-47s.<sup>201</sup> They boarded two transport helicopters that

---

<sup>194</sup> Katz, *Shadow Strike*, 40; and Magen, *Operation Orchard*, 8.

<sup>195</sup> Magen, *Operation Orchard*, 8.

<sup>196</sup> Follath and Stark, "The Story of 'Operation Orchard.'"

<sup>197</sup> "Sayeret Matkal," Jewish Virtual Library, accessed April 26, 2023, <https://www.jewishvirtuallibrary.org/sayeret-matkal>.

<sup>198</sup> Follath and Stark, "The Story of 'Operation Orchard.'"

<sup>199</sup> Magen, *Operation Orchard*, 12.

<sup>200</sup> Katz, *Shadow Strike*, 161.

<sup>201</sup> Katz, 159.

flew into Syria at low altitude to prevent radar detection. It is interesting to note that the Israelis were confident their helicopters would not be detected. The stealth helicopters were first used by the U.S. during the Osama Bin Laden raid in 2011.<sup>202</sup> As such, it would not be probable for the technology to be deployed in Syria in 2007. Hence, while the use of EW was not reported in this mission, it could have also been deployed for this mission. Another possibility included landing helicopters in a friendly area, e.g., Turkey, and infiltrating to the target via vehicles.

After being dropped a few miles away from al-Kibar, the Israelis commenced their stealth infiltration. To aid their mission, they were armed with high-end equipment such as night vision goggles, anti-tank missiles, explosives, and satellite communication.<sup>203</sup> If those were insufficient, they also had specialized technical teams that would modify equipment to their needs. At the target, once they had established that the area was safe, they commenced their soil collection in accordance with the instruction from Israeli scientists. Collection took only a few minutes. Afterward, they covered their traces and left the scene. A few days later, the lab tests on the soil returned positive for traces of a radioactive substance, indicating that the reactor was nearly operational.

### **3. The Airstrike on al-Kibar by Raam and Sufa Supported by EW Technology**

Concluding that Syrian's nuclear reactor was nearly operational, Israel decided to launch an air strike independent of the U.S. on the al-Kibar facility in September 2007.<sup>204</sup> According to Makovsky, this mission was known as Skinny Shkedi, named after General Eliezer Shkedi, commander of the Israeli Air Force (IAF).<sup>205</sup> Katz reported that pilots were picked from the Raam (Thunder) Squadron, which operated F-15s, and the Sufa (Storm) Squadron, which operated F-16s.<sup>206</sup> Preparation went on for months, but the pilots

---

<sup>202</sup> Tom Geoghegan and Sarah Shenker, "'Stealth Helicopters' Used in Bin Laden Raid," *BBC News*, May 6, 2011, <https://www.bbc.com/news/world-us-canada-13297846>.

<sup>203</sup> Katz, *Shadow Strike*, 162.

<sup>204</sup> Katz, 172–73.

<sup>205</sup> Makovsky, "The Silent Strike."

<sup>206</sup> Katz, *Shadow Strike*, 171–72.

received very little information about the target. Shkedi frequently reminded them of three points: “the need to avoid detection, to destroy the target, and to get home safely.”<sup>207</sup>

According to Katz, on September 4, 2007, the night before the attack, Shkedi and Gabi Ashkenazi, IDF’s Chief of Staff, observed the final rehearsal and then announced the target to the pilots: “Your mission is to bomb a nuclear reactor in Syria.”<sup>208</sup>

On the evening of September 5, key Israeli figures including Prime Minister Olmert gathered at the Bor, IDF’s main command center, to witness the beginning of the mission.<sup>209</sup> At around 2230, four F-15s and four F-16s made their way to the target.<sup>210</sup> The eight non-stealth jets flew over the Mediterranean Sea, then along the Turkish-Syrian border, before making their final approach into Syria to the nuclear reactor.<sup>211</sup>

According to Katz, to avoid detection, the Israeli planes employed both traditional tactics and advanced technology.<sup>212</sup> First, they maintained communication silence. This would reduce the possibility of pickup by SIGINT. Second, they flew at a low altitude, i.e., under 200 feet, for most of the infiltration phase. They only climbed to a higher altitude during the final infiltration phase to release the bombs. There was no certainty that these traditional tactics would enable them to evade radar detection. As such, advanced technology was introduced to provide the assurance. While the details of the specific technology used in the attack were not specified, scholars including Fulghum, Barrie, and Adee attributed the success to EW or cyber-attack.<sup>213</sup> Fulghum and Wall also stated that Israel had received advice from the U.S. to overcome the Syrian IADS.<sup>214</sup>

---

<sup>207</sup> Katz, 171.

<sup>208</sup> Katz, 182.

<sup>209</sup> Magen, Operation Orchard, 16.

<sup>210</sup> Magen, 16.

<sup>211</sup> Magen, 16.

<sup>212</sup> Katz, *Shadow Strike*, 186.

<sup>213</sup> Fulghum and Barrie, “Israel Used Electronic Attack in Air Strike against Syrian Mystery Target”; and Sally Adee, “The Hunt for The Kill Switch,” *IEEE Spectrum*, May 1, 2008, <https://spectrum.ieee.org/the-hunt-for-the-kill-switch>.

<sup>214</sup> David A. Fulghum and Robert Wall, “U.S. Electronic Surveillance Monitored Israeli Attack On Syria,” *Aviation Week*, November 21, 2007, <https://www.worldsecuritynetwork.com/Israel-Palestine/AviationWeek.com/U.S.-Electronic-Surveillance-Monitored-Israeli-Attack-On-Syria>.

In a report by the Jerusalem Post in September 2010, the commander of the IAF's Sky Crows Squadron, the unit responsible for Israel's EW capability, admitted to using EW capability for all IAF operations. He said:

The bottom line is that the IAF's EW capabilities are relevant in every theatre of operations and on every front... There is no IAF operation that we are not part of—from special operations, to routine operations and all-out wars.<sup>215</sup>

He added, “the current theatre of operations for aircraft is challenged and threatened by advanced surface-to-air missile systems in enemy territory.... Our objective is to activate our systems and to disrupt and neutralize the enemy's systems.”<sup>216</sup> Experts in the U.S. aerospace industry have suggested that the Israeli military may have utilized a technology akin to the “Suter” airborne network attack system. This system, developed by BAE Systems and incorporated into unmanned aerial vehicle (UAV) (or fighter planes) operations by L-3 Communications in the United States, is believed to bear similarities to the Israeli approach. Israel has a well-established track record of proficiently employing unmanned systems to manipulate Syrian IADS, a practice that traces back to the Bekaa Valley confrontations in 1982.<sup>217</sup>

The EW attack was reported to have worked in two steps.<sup>218</sup> The first was to use network-centric collaborative targeting that would “enable a network of sensors to collaborate in determining the location of a target with minimal human intervention” to locate the IADS.<sup>219</sup> Next, the Suter technology enabled users to infiltrate communication networks, gain access to the same sensor data as their enemies, and even take control as the system administrator.<sup>220</sup> This capability enabled them to manipulate sensors, placing

---

<sup>215</sup> Yaakov Katz, “And They Struck Them with Blindness,” *The Jerusalem Post*, September 29, 2010, <https://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness>.

<sup>216</sup> Katz.

<sup>217</sup> Fulghum and Barrie, “Israel Used Electronic Attack in Air Strike against Syrian Mystery Target.”

<sup>218</sup> CMSAdmin, “The Israeli ‘E-Tack’ on Syria – Part I,” *Airforce Technology*, March 9, 2008, <https://www.airforce-technology.com/features/feature1625/>.

<sup>219</sup> CMSAdmin.

<sup>220</sup> Fulghum and Barrie, “Israel Used Electronic Attack in Air Strike against Syrian Mystery Target.”

them in positions where incoming aircraft could not be detected. The process involved accurately identifying enemy emitters and then precisely sending data streams into them, including false contacts and distorted messages that facilitated a range of activities, including gaining control.<sup>221</sup> Such a system could be installed onboard modified planes and its capability would involve network hopping to seek the targeted network by jumping from network to network.<sup>222</sup>

The second method that was less speculated to have contributed to the successful infiltration into Syrian airspace was through cyberattack that was deliberately created by chip makers, according to report from IEEE.<sup>223</sup> The idea was to hide a “backdoor” within the microprocessor. When a code was sent to the backdoor, it would activate a kill switch, which is a group of transistors with hidden code that cause all or part of the chip to become dysfunctional. This method would be effective because there are many ways and locations where kill switches can be hidden.<sup>224</sup> Standard testing methods focus on the performance of the functions that the chip was supposed to perform, but not on every transistor of the entire chip. Even for the U.S. military, which was the largest buyer of the microprocessors, it was non-economical to produce an in-house risk-free chip.<sup>225</sup> For states with smaller militaries, such as Syria, that task would be impossible. Hence, there remained a possibility that on the day of the airstrike, a kill switch hiding in one of the Syrian air defense systems was activated to blind the system.

As reported by Melman, after the eight fighter jets arrived at the target undetected, they each released two bombs, which amounted to a total of 17 tons of explosives, on the nuclear reactor.<sup>226</sup> Within minutes the buildings were destroyed, and then came the moment everyone in the Bor was waiting for, the pilots reported “Arizona,” which was a

---

<sup>221</sup> Fulghum and Barrie.

<sup>222</sup> David A. Fulghum, Robert Wall, and Amy Butler, “Israel Shows Electronic Prowess,” *Aviation Week*, November 25, 2007, [http://www.aviationweek.com/aw/generic/story\\_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess](http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess).

<sup>223</sup> Adee, “The Hunt for The Kill Switch.”

<sup>224</sup> Adee.

<sup>225</sup> Adee.

<sup>226</sup> Melman, “Outside the Box: Israel’s Strike on Syria’s Nuclear Plant.”

codeword that represented mission success.<sup>227</sup> The mission had not been completed though. Now that silence had broken, the pilots had to escape quickly. Relatedly, Katz also reported that the airplanes were engaged by Syrian air defense but the attempt to take down the airplanes was unsuccessful. In the midst of escape, the airplanes jettisoned additional fuel tanks to shed some weight and landed in Turkey which resulted in Israel later apologizing for the intrusion.<sup>228</sup> All eight airplanes returned to base unharmed after less than four hours of operation.

#### **D. ANALYSES**

Operation Orchard exemplified a sophisticated operation that effectively employed advanced technology to outmaneuver adversaries. Based on an analysis of the reports regarding both EW and cyberattacks, it appears that the EW attack was the more likely method employed in the Israeli forces' air strike, as opposed to a cyberattack involving a kill switch. Additionally, there were no subsequent discussions regarding the methodology, except for the report published by IEEE. Therefore, for the purposes of this research, I will assume that EW was utilized to support the airstrike, and the analysis will proceed based on this assumption.

Referring to Table 3, the overall synergistic relationship is assessed to be positive in this integration of advanced technology, i.e., EW systems, with the SO, i.e., covert airstrike. It fulfilled all the tenets of the conceptual model in Chapter II.

---

<sup>227</sup> Bor is Israel's underground command post.

<sup>228</sup> "Turkey Puts Israeli Sortie behind It," *Jewish Telegraphic Agency*, November 6, 2007, <http://www.jta.org/cgi-bin/iowa/breaking/105120.html>.

Table 3. Summary of Integration Between Special Operations and Technology in Operation Orchard

| <b>Integrating EW with Airstrike</b>                              |          |
|-------------------------------------------------------------------|----------|
| <u>Specs Ops – Advanced Technology Integration</u>                |          |
| Is it a Special Operation?                                        | Yes      |
| Does it use Advanced Technology?                                  | Yes      |
| <u>Enabling Conditions</u>                                        |          |
| Does this integration have a clear purpose?                       | Yes      |
| Is the technology compatibility with Special Operation?           | Yes      |
| Is there integration effort?                                      | Yes      |
| <u>Outcome</u>                                                    |          |
| Is it effective for the mission?                                  | Yes      |
| Does it reduce risk to mission/force?                             | Yes      |
| <u>Overall synergistic relationship</u>                           |          |
| What is the synergistic relationship for the emergent capability? | Positive |

### 1. Integration of Special Operations and Advanced Technology

While airstrikes are typical missions conducted by fighter jets, I argue that the attack on Syria’s nuclear reactor could also be qualified as SO. With reference to the details in Table 4, Operation Orchard fulfilled all the tenets of a SO.

Table 4. Qualifying Airstrike Conducted by Raam and Sufa as Special Operations<sup>229</sup>

| <b>Special Operations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition: “Small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.” |                                   |                                                                                                                                                                                                           |
| <b>Key Tenets</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Demonstrated in Operation?</b> | <b>Elaboration</b>                                                                                                                                                                                        |
| <u>Small scale</u> , clandestine, <u>covert</u> or overt operation                                                                                                                                                                                                                                                                                                                                                                                                                                   | Yes                               | It was a surgical attack on a single facility by only eight aircraft. Both Israel and Syria maintained deniability over the actual reason for the airstrike. The pilots were handpicked for this mission. |
| Unorthodox                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Yes                               | The methods used to evade detection, including communication silence, flying at low altitude, and                                                                                                         |

<sup>229</sup> Adapted from: Tugwell and Charters, “Special Operations and the Threats to United States Interests in the 1980s,” 35.

| <b>Special Operations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------|
| Definition: “Small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.” |                                   |                                                                                                         |
| <b>Key Tenets</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Demonstrated in Operation?</b> | <b>Elaboration</b>                                                                                      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                   | integrated advanced EW or cyber capabilities, were unorthodox.                                          |
| High-risk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Yes                               | The risk of entering foreign airspace defended by IADS was extremely high.                              |
| <u>Significant political</u> or military objectives in support of foreign policy                                                                                                                                                                                                                                                                                                                                                                                                                     | Yes                               | Syria’s possession of nuclear weapon would be a threat to the region.                                   |
| Oversight at the highest level                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Yes                               | Prime minister and other key members were directly involved in decision making for the operation.       |
| Use of military, non-military resources, including intelligence assets.                                                                                                                                                                                                                                                                                                                                                                                                                              | Yes                               | Besides air force, multiple agencies, including Sayeret Matkal and Sky Crows, complemented the mission. |

In terms of advanced technology, the utilization of EW to manipulate the Syrian IADS played a crucial role in facilitating a covert airstrike. EW capability was highly classified, exceptionally sophisticated, and not commonly accessible for commercial or military purposes. The ownership of these EW systems was attributed to the Sky Crows, who had the capability to integrate them with SO whenever the need arose.<sup>230</sup> Hence, EW capability qualified as an advanced technology.

## **2. Enabling Conditions**

### ***a. Purpose***

The integration of airstrike and EW systems in Operation Orchard had a clear purpose: to enable Israeli airplanes to enter Syrian airspace without being detected and to destroy the target: Syria’s nuclear reactor. In other word, the integration of these two components enabled the operation to be conducted covertly. It further provided Israeli leaders and pilots with an added level of confidence, as traditional military tactics, such as flying at low altitude and exercising communication silence, were not as effective, hence

<sup>230</sup> Katz, “And They Struck Them with Blindness.”

the likely use of an accompanying EW capability. Additionally, the inability to detect Israeli planes fell within Israel's "deniability zone" playbook, allowing Israel to remain silent about the attack, at least during the initial stages post-attack, and for Syria to downplay the location and extent of the destruction caused.

***b. Integration Effort***

The specifics of how the advanced technologies were integrated into the operation remain classified. Given the high stakes involved, however, it is likely that the solution underwent rigorous testing and multiple trials in order to generate confidence in executing the high-risk mission. Noting that the EW systems were not organically part of the Raam or Sufa squadrons, using them to support the airplanes' infiltration required careful coordination. This coordination involved a detailed understanding of Israel's flight plan from the fighter pilot, intelligence on Syria's IADS capability from the intelligence planner, and precise timing and effects of the EW from the EW planners. The success of this multi-agency coordination demonstrated the high level of integration effort required for the mission.

***c. Compatibility***

Although there was a strong desire to utilize this emerging capability, the success of the integration was largely dependent upon the compatibility between the advanced technology and the SO infiltration. This compatibility remains a fundamental factor in ensuring the success of the integration effort. For the Suter system to work, it had to be either installed onboard the fighter jets or supported separately by another airplane such as the Gulfstream G550, which has been reported to have such capability.<sup>231</sup> Such installation can only be possible if the system were technically feasible to be carried and operated in these planes.

---

<sup>231</sup> CMSadmin, "The Israeli 'E-Tack' on Syria – Part II," *Airforce Technology*, March 10, 2008, <https://www.airforce-technology.com/features/feature1669/>.

### **3. Outcomes**

#### ***a. Risk***

The introduction of the EW system significantly reduced both the risk to the mission and the risk to Israeli forces involved. The system served two critical purposes.

First, the primary objective of the system was to protect the Israeli airplanes and ensure their survival. By making the Israeli planes undetectable to the Syrian IADS, the system prevented the Syrians from launching SAMs at the planes, reducing the risk of the planes being destroyed and loss of life.

Second, the system was also designed to maintain anonymity and conceal the identity of the attacker and its target, even from the Syrians. This was essential to avoid provoking a larger conflict with Syria, and Israel wanted the Syrians to play down the attack. By blinding the Syrian IADS, there was no trace of an air intrusion, and the details of the attack were not tracked, allowing Israel and Syria to present their own narratives without contradicting each other.

Overall, the successful implementation of the EW system significantly reduced the risks to the Israeli mission and forces involved, and helped Israel achieve its strategic objectives while avoiding further escalation of the conflict with Syria.

#### ***b. Effectiveness***

The Israeli government's primary objective was to neutralize Syria's nuclear reactor while minimizing the risk of escalation, which they achieved through a combination of covert airstrike and EW. This approach proved to be highly effective, as they were able to destroy the al-Kibar facility with only eight planes, without being detected by Syrian defenders. The Israelis were well aware of the potential backlash from international organizations and predicted that the Syrian government would not want to publicize their nuclear ambitions. Therefore, Israel had to conduct the attack on the nuclear infrastructure with extreme precision, without causing collateral damage or destroying other critical infrastructure. This was precisely what happened, thanks to the successful integration of

EW with the airstrike, which played a crucial role in enabling Israel to execute this delicate operation with precision and success.

## **E. CONCLUSION**

While the U.S. did not agree to taking military action against Syria for illegally developing a nuclear reactor, it did not forbid Israel from acting unilaterally. Israel's decision to conduct a surgical airstrike proved to be a critical move to not only terminate Syria's nuclear program, but also to prevent backlash in the aftermath of the attack.

The success of the low-signature surgical airstrike could largely be attributed to the integration with advanced EW to manipulate the Syrian IADS, however. The integration was not coincidental. The presence of the enabling conditions—a clear purpose to enable Syria to deny the operation, the EW system being fixed on the airplanes and the integration effort of various entities—enabled seamless integration of technology and SO to achieve the strategic objective of eliminating the nuclear threat.

Without this approach, Israel would have faced the challenge of Syria's IADS, which could have led to retaliation and a less effective mission. Overall, Israel's success in Operation Orchard demonstrated that the successful integration of advanced technology could greatly enhance the overall effectiveness of a SO as per the utility of the conceptual model from Chapter II.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. OPERATION OCEAN SHIELD

### A. INTRODUCTION

OOS was a NATO-led counter piracy operation following a request from the United Nations (UN) to gather international support to curb piracy and armed robbery at sea off Somalia's coast.<sup>232</sup> Throughout the seven years of deployment from 2009 to 2016, the number of piracies plummeted, and the operation was seen as a success. When the operation was concluded in December 2016, NATO Spokesperson Oana Lungescu said, "Operation Ocean Shield has been a great success—making an essential contribution to combatting piracy in the seas off Somalia and therefore keeping one of the world's most important waterways safe and secure."<sup>233</sup>

This chapter uses the tenets of the conceptual model in Chapter II to examine the application of advanced technologies by a maritime SO task unit that operates under TF Barracuda, which falls under the jurisdiction of OOS. The unit was tasked with tracking or disabling rogue ships in response to the increasing threat posed by pirates using captured "motherships." After several months of planning, innovation, and preparation, the unit devised unique solutions to carry out both tasks. Due to the HQ's preference for disabling missions rather than tracking missions, however, five disabling missions and one tracking mission were executed. All five disabling missions were successful but, unfortunately, the single deployment for the tracking mission was unsuccessful.

In contrast to the other two case studies, which heavily relied on secondary sources from the research of other scholars, this particular case study is based on primary sources of information gathered through interviews with three individuals who were involved in the operation. The interview protocol, list of interviewees, and transcript and content

---

<sup>232</sup> United Nations Security Council (UNSC), "Resolution 1851," S/RES/1851 § (2008).

<sup>233</sup> "NATO Concludes Successful Counter-Piracy Mission," *NATO*, December 15, 2016, [http://www.nato.int/cps/en/natohq/news\\_139420.htm](http://www.nato.int/cps/en/natohq/news_139420.htm).

analysis for Respondent 1 are found in the appendices. The names and countries will be omitted for anonymity, however.

The following paragraphs will begin by providing the background of OOS, which includes the events that prompted the launch of counter-piracy operations in Somali waters. Next, I will delve into the specifics of the operations, beginning with the higher-level campaign of OOS before narrowing down to the mission carried out by the maritime SO task unit. I will then use the conceptual model presented in Chapter II to analyze this case study. The chapter will conclude by highlighting the key findings.

## **B. BACKGROUND**

In 1991, the president of Somalia, Mohamed Siad Barre, fled the country following a rebellion launched by the opposition. The central government collapsed following his departure. Opposition groups, warlords, and clan militias took the opportunity to seize power in various regions, resulting in a civil war.<sup>234</sup> The civil war lasted for about a decade. Throughout this period, instability of the country coupled with drought, famine, and disease, resulted in widespread violence, poverty, and other social issues. The situation was described by Mike Whitlam, the British Red Cross Director-General:

I have never seen so many people in one place starving and dying... The smell of death and of the feeding kitchens is a combination I will not forget. The other feeling is of sheer frustration at trying to get food into place and being prevented by conflict from delivering it to the starving.<sup>235</sup>

Although the government was re-established in 2000 when Abdiqasim Salad Hassan was elected as the president of Somalia, the issues did not go away. Somalia continues to face numerous challenges, including poverty, corruption, and the threat of terrorism, which have hindered the progress of the nation. Furthermore, the 2004 tsunami

---

<sup>234</sup> Abdisalam M. Issa-Salwe, *The Collapse of the Somali State: The Impact of the Colonial Legacy* (London: Haan, 1996), 100–105.

<sup>235</sup> Issa-Salwe, 118.

that killed an estimated 289 people and destroyed approximately 800 buildings and over 600 fishing vessels exacerbated Somali's already dire situation.<sup>236</sup>

Since then, there has been a rise in the number of Somalis turning to piracy. The Somalis claimed they were forced by circumstances into piracy. It was a reaction to two main issues that were happening in their waters: illegal fishing and dumping of radioactive waste.<sup>237</sup> On the issue of fishing, the Somalis blamed European ships for illegal fishing, which included excessive trawling that affected the marine livestock and resulted in a shortage of fish in Somali waters. On the issue of illegal dumping of waste, there was a trend of European ships dumping radioactive waste off the coast of Somalia after the government collapsed, which resulted in the coastal population suffering from radiation disease.<sup>238</sup> From the perspectives of the Somali pirates, they did not view themselves as pirates. They felt that they were victims in the situation and that their response was necessary to maintain order in the region. This understanding is reflected in the following two descriptions:

- I believe the title of pirates should be given to those who come to our waters illegally.<sup>239</sup>
- We had to defend ourselves. We became watchmen of our coasts and took up our duty to protect the country. Don't call us pirates. We are protectors.<sup>240</sup>

With the widespread belief of the new identity among the Somali pirates, piracy soon became a problem in that region as the numbers escalated. As shown in Figure 3, the piracy incidents trended upward from 2006 and have increased exponentially over the next

---

<sup>236</sup> Martin Plaut, "Tsunami: Somalia's Slow Recovery," *BBC*, December 26, 2005, <http://news.bbc.co.uk/2/hi/africa/4560246.stm>.

<sup>237</sup> Wanjohi Kabukuru, "Somali Piracy: In Search of Remedies for a Global Malady," *Africa Renewal*, January 17, 2012, <https://www.un.org/africarenewal/web-features/somali-piracy-search-remedies-global-malady>.

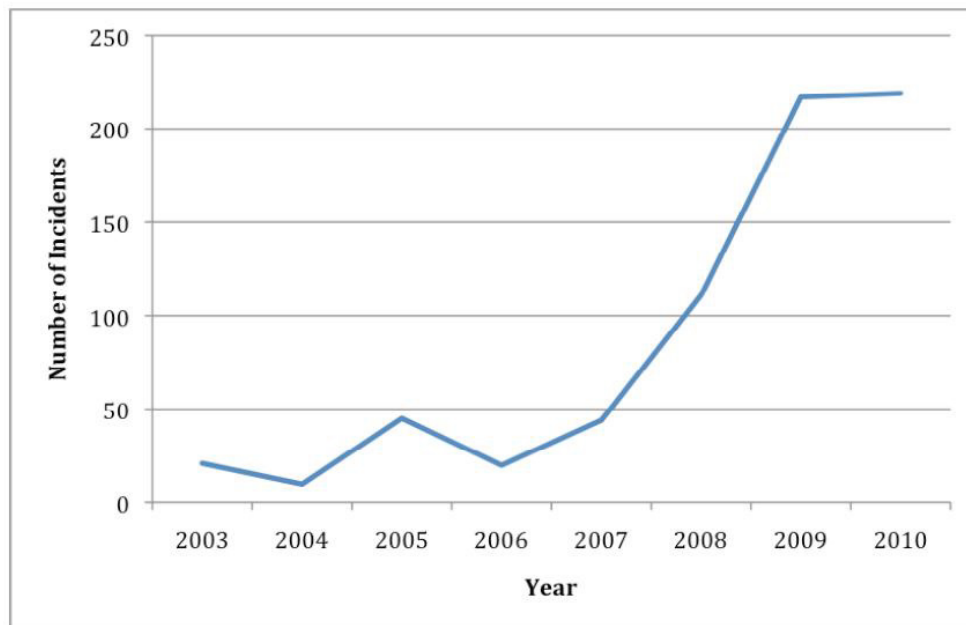
<sup>238</sup> Johann Hari, "You Are Being Lied to About Pirates," *The Independent*, January 5, 2009, <https://www.independent.co.uk/voices/commentators/johann-hari/johann-hari-you-are-being-lied-to-about-pirates-1225817.html>.

<sup>239</sup> Tristan McConnell, "Interview with a Pirate," *GlobalPost*, June 12, 2009, <https://theworld.org/stories/2009-06-12/interview-pirate>.

<sup>240</sup> Noah Shachtman, "Exclusive Interview: Pirate on When to Negotiate, Kill Hostages," *Wired*, July 28, 2009.

few years. Ships have been attacked, hijacked, and held hostage for ransom. In 2012, the estimated cost of Somali piracy was between \$5.7 and 6.1 billion, which included payment of insurance, rerouting to a safer passage, increased speed of merchant vessels, enhancement of ships defense and security, naval patrols, and other related prosecution efforts.<sup>241</sup>

**Attempted and Successful Attacks by Somali Pirates**



Source: <https://natoassociation.ca/somali-piracy-and-the-worlds-response/>

Figure 3. Number of Attacks by Somali Pirates (2003–2010)

In order to curb the pressing issue of piracy in Somalia to restore shipping confidence as well as offer protection for World Food Program vessels, the UN passed multiple Resolutions including 1814, 1816, 1838, 1846, and 1851 to seek support from NATO, the EU, and other countries to participate in humanitarian assistance, mitigate

<sup>241</sup> Jonathan Bellish, “The Economic Cost of Somali Piracy 2012” (One Earth Future Foundation, 2013), 1, [https://oneearthfuture.org/sites/default/files/documents/publications/View%20Full%20Report\\_3.pdf](https://oneearthfuture.org/sites/default/files/documents/publications/View%20Full%20Report_3.pdf).

disruption in shipping, and reduce piracy in Somalia.<sup>242</sup> UN Security Council (UNSC) Resolution 1851 on December 16, 2008 encouraged,

All States and regional organizations fighting piracy and armed robbery at sea off the coast of Somalia to establish an international cooperation mechanism to act as a common point of contact between and among states, regional and international organizations on all aspects of combating piracy and armed robbery at sea off Somalia's coast.<sup>243</sup>

Commencing in 2008, NATO and the European Union Naval Force (EUNAVFOR) have been the two main organizations leading the counter piracy effort. The operations, including NATO's Operation Allied Protector, Operation Atlantic Alliance and OOS and EUNAVFOR's Operation Atalanta, coordinated efforts among 20 and 30 international vessels daily to counter piracy efforts in 2012.<sup>244</sup>

Before the intervention of foreign forces, the pirate attacks were concentrated near the Gulf of Aden. The Somali pirates adapted their methods to operate farther from the Gulf of Aden, in the Somali Basin, near Mozambique and the Indian Ocean island nations of The Seychelles and Maldives, following the introduction of counterpiracy activities.<sup>245</sup> To execute this method, the Somali pirates used hijacked fishing trawlers and commercial vessels as motherships to sustain prolonged duration at sea.<sup>246</sup> Responding to these tactics, TF Barracuda as part of OOS was organized to surgically target these motherships.

The combination of various efforts reduced the piracy numbers drastically. There were various explanations for the decrease in piracy numbers.<sup>247</sup> From a military

---

<sup>242</sup> "Resolutions Adopted by the Security Council in 2008" (United Nations Security Council), accessed April 10, 2023, <https://www.un.org/securitycouncil/content/resolutions-adopted-security-council-2008>.

<sup>243</sup> United Nations Security Council (UNSC), Resolution 1851.

<sup>244</sup> James M. Bridger, "Safe Seas at What Price? The Costs, Benefits and Future of NATO's Operation Ocean Shield," *NATO*, no. 95 (September 2013): 2, [https://www.files.ethz.ch/isn/169344/rp\\_95.pdf](https://www.files.ethz.ch/isn/169344/rp_95.pdf).

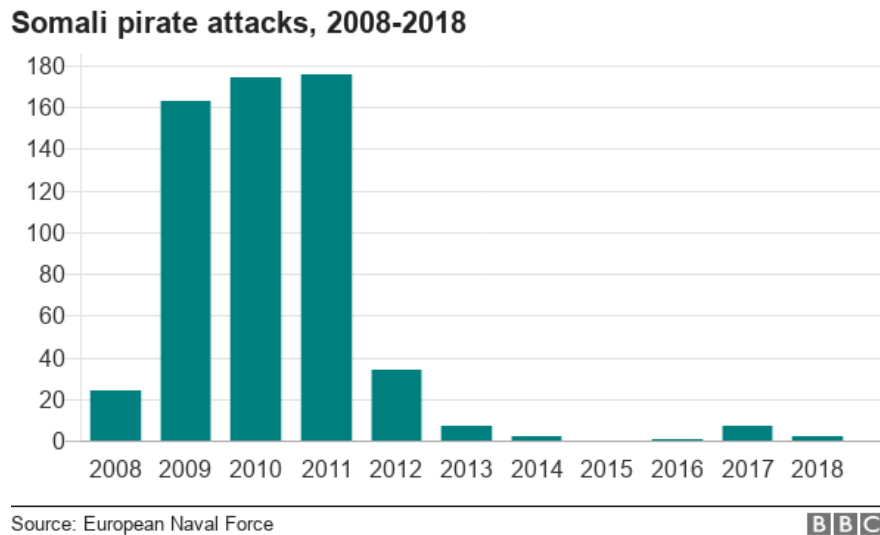
<sup>245</sup> Raymond Knops, "The Challenge of Piracy: International Response and Nato's Role" (NATO Parliamentary Assembly, November 2012), 2.

<sup>246</sup> Bridger, "Safe Seas at What Price? The Costs, Benefits and Future of NATO's Operation Ocean Shield," 2.

<sup>247</sup> Jonathan Bellish, "The Economic Cost of Somali Piracy 2012," 1.

standpoint, the success can be attributed to the effective coordination among different international naval forces and their prompt adjustment of countermeasures, specifically by targeting motherships. From a merchant shipping perspective, the improvement in the best management practices and the use of armed guards has made it harder for the pirates to attack the vessels. It was reported that in 2012, 50% of merchant vessels were armed, up from 30% in 2011.<sup>248</sup>

With the decline of piracy activities and after no major incidents were reported after 2012 (see Figure 4), the situation in Somalia was assessed to be under control, and OOS was stood down in 2016 after seven years of protecting the sea lanes in Somali waters.<sup>249</sup>



Source: <https://www.bbc.com/news/world-africa-46454055>

Figure 4. Number of Attacks by Somali Pirates (2008–2018)

<sup>248</sup> Jonathan Bellish, 1.

<sup>249</sup> NATO, “Counter-Piracy Operations (2008–2016),” NATO, accessed April 10, 2023, [https://www.nato.int/cps/en/natohq/topics\\_48815.htm](https://www.nato.int/cps/en/natohq/topics_48815.htm).

## C. PLANNING AND EXECUTION

OOS was a multinational effort involving various conventional and non-conventional forces. This operation evolved from two NATO operations: Operation Allied Protector and Operation Allied Provider.<sup>250</sup> It was stood up on August 17, 2009 and stood down on December 15, 2016.<sup>251</sup> The key participants of OOS were NATO, EUNAVFOR, the U.S.-led Combined TF 151, and independent deployers.<sup>252</sup> Their area of operation was the Horn of Africa, including the Gulf of Aden and the Western Indian Ocean up to the Strait of Hormuz, an area of about 2 million square miles. The Somali authorities gave consent to vessels participating in OOS to enter the territorial waters of Somalia.

This operation consisted of four main objectives:

- Deter and disrupt pirate operations at sea
- Coordinate international counter-piracy efforts
- Enhance the maritime community's capacity to counter piracy effectively
- Develop a regional counter-piracy capability<sup>253</sup>

Each day, an average of four to five vessels were deployed in the area of operations (AO) to fulfill the anti-piracy mission. As described in the background, the pirates evolved their tactics over time, eventually using motherships to conduct piracy farther from the coast. At the same time, OOS responded to the new tactics by “[eroding] the pirates’ logistics and support-base by, among other things, disabling pirate vessels or skiffs, attaching tracking beacons to mother ships and allowing the use of force to disable or destroy suspected pirate or armed robber vessels.”<sup>254</sup> One of the entities assigned this new task was TF Barracuda.

---

<sup>250</sup> Bridger, “Safe Seas at What Price? The Costs, Benefits and Future of NATO’s Operation Ocean Shield.”

<sup>251</sup> “Operation Ocean Shield,” NATO, accessed April 10, 2023, <https://mc.nato.int/missions/operation-ocean-shield.aspx>.

<sup>252</sup> “Counter-Piracy Operations.”

<sup>253</sup> NATO.

<sup>254</sup> NATO.

## 1. Task Force Barracuda

TF Barracuda had a range of assets and forces under its command, including a flagship where the HQ was stationed, helicopters for surveillance, rigid hull inflatable boats (RHIBs) for inserting troops, maritime SOF teams (frogmen), and other support units. Table 5 shows the core elements, composition, and responsibilities specific to the SO Task Unit under TF Barracuda.

Table 5. Core Elements for Special Operations Task Unit

| Element                      | Composition | Responsibility                                                                                                 |
|------------------------------|-------------|----------------------------------------------------------------------------------------------------------------|
| Special Operations Commander | 1 x LTC     | Exercise command and control if the mission is a special operation                                             |
| Company Commander            | 1 x MAJ     | Liaison between HQ and ground forces                                                                           |
| Maritime SOF teams (frogmen) | 2 x 6-man   | One team specializes in diving (sub-surface)<br>One team specializes in boarding ship (surface) <sup>255</sup> |

Two main tasks were assigned to the SO Task Unit. Their primary objective was to respond to and thwart the advanced tactics employed by pirates, such as the mothership strategy for staging attacks farther from the coast. The first task involved tracking and avoiding the pirate motherships by placing a beacon on it. The beacon emitted signals at regular intervals to indicate the location of the mothership, and this information was then shared with other forces in OOS. This information was then passed on to merchant vessels, enabling them to alter their routes and avoid any encounters with pirates. According to R1, who was company commander of the task unit for the operation,

The concept for placing the beacon was to see and avoid. The whole thinking was that all the navies would know where the (pirates) motherships were and then they could warn the merchant vessels that the pirates are there. They will then take another route.

The second task was to search and disable. This task was conducted by surgically placing explosives at critical spots to disable the motherships or skiffs. The idea was not to sink the ship but to create sufficient damage such that the boats were incapable of

---

<sup>255</sup> While the teams have different specializations, they are trained in both diving and boarding.

conducting or supporting piracy activities. As R1 explained, “the amount of explosive use would not sink the ship, ‘right’ amount of explosive is used to stop the pirates from driving the ship.”

In total, the task unit completed three rotations spanning three years. During the first two deployments, it executed one track-and-avoid mission along with five search-and-disable missions. During the third deployment, however, despite being prepared for action, no missions were conducted due to a significant reduction in piracy incidents and the absence of any operational motherships. R3 shared his experience in the third deployment: “we trained a lot for it, but in the end, it was just waiting for a ship that never came.”

## **2. Concept of Operation**

Both tasks shared a similar concept of operation. The key difference lay in the way the payload was deployed, however. The process (see Figure 5) began with frogmen transferring from a larger naval vessel, such as a flagship, to smaller boats (e.g., RHIBs) that could bring them closer to the target vessel. Once the frogmen were at a suitable location within diving range, they were dropped off by the boats and proceeded to infiltrate the target vessel via diving. At the target vessel, they placed the payload (i.e., beacon or explosive) at the designated location, and then exfiltrated to a safe spot where they were picked up by boats and returned to the naval ship, all while attempting to remain undetected. Although the concept of the operation was simple, the success or failure of the mission ultimately depended on the intricate details of the execution by the frogmen.

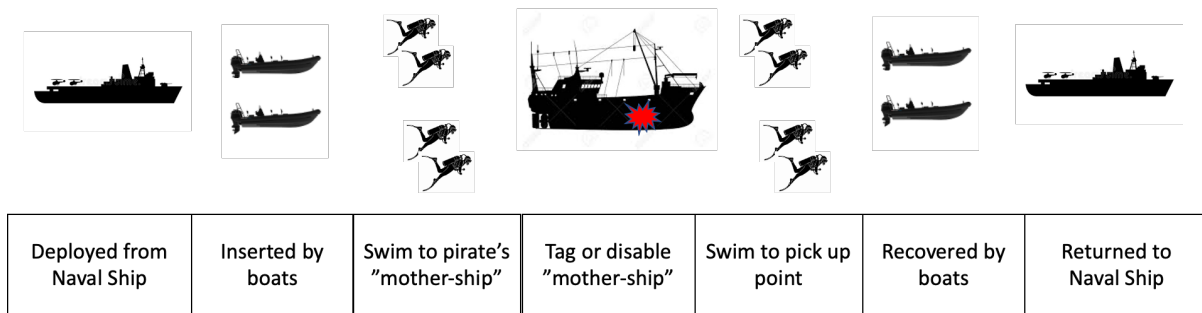


Figure 5. Concept of Operation of Task Force Barracuda<sup>256</sup>

### 3. Threats

#### a. *Sea Conditions*

The sea conditions were harsh and unpredictable in the AO. The Indian Ocean is susceptible to monsoons. Each year, there is roughly a window of two months in which conditions are suitable for the execution of diving missions. For the diving mission, the wind, sea state, current, swell, and illumination could all affect the frogmen's ability to swim to the target. R1 explained the difficulty of predicting where the divers would drift to when the current and wind acted in different directions. R3 also elaborated the challenge in navigation: "As the frogmen were required to dive underwater for up to 2–3 km to a target vessel of about 30 m, any deviation off course may result in missing the target."

#### b. *Dangerous Marine Animals*

Another environmental threat was the presence of sharks in the Indian Ocean. The frogmen's mission is most effective when executed in the hour of darkness. But unfortunately, that timing coincided with the feeding time of the sharks. Operating in a shark-infested area posed concern for the frogmen.

<sup>256</sup> The figure is created by the author based on his interpretation of the concept of operation from the interviews. It is to aid readers to create a mental picture the mission. The ships, boats, or divers are not the representation of the actual assets, forces, or target from the operation.

*c. Pirates*

One crucial aspect of threat assessment was to comprehend the enemy's stance. The evaluation concluded that the Somali pirates were both armed and aggressive, and they maintained vigilance throughout the night. As a non-military and unconventional force, however, they were inadequately equipped with high-end surveillance devices like night vision goggles and had poor training. Nonetheless, the frogmen had to remain undetectable; otherwise, they risked facing casualties from potential firefights.

**4. Enhancement to Operation**

Now that they had a grasp on the operation's concept and potential threats, the frogmen had to employ tactics to mitigate risk and increase the likelihood of success during their operations. In order to safely and effectively carry out a mission involving tracking or disabling, the frogmen had to prioritize updating their intelligence, enhancing their equipment, finding ways to increase their chances of survival, and improving their navigation methods. These factors are crucial for ensuring a successful mission.

*a. Updating Intelligence*

The information related to the possible targets was updated in a database. Each time the boarding team conducted boarding missions, they would use the opportunity to gather information to build the database.<sup>257</sup> The information was shared with the frogmen to aid their planning for the tagging or disabling mission. For example, when the database contained information on the same or a similar type of vessel used by the pirates' mothership, this information could be used by frogmen to determine where to place the payload to achieve maximum effectiveness.

Despite the information sharing from the boarding team, not all required information for the operations could be obtained, especially those details related to the exterior parts of the vessels below the waterline. At times, the frogmen would be tasked

---

<sup>257</sup> Boarding tasks are part of the mission of OOS but are not elaborated in this paper.

with conducting a surveillance dive on the actual mothership or a ship of a similar class. This action would provide them the information required for planning prior to execution.

***b. Integrating New Technology***

**(1) Beacon**

The functionality of the payload was a critical part of the mission assigned to the frogmen. For the first task, track-and-avoid mission, a beacon suitable for the maritime environment was designed. The frogmen first identified a suitable beacon that was used by police from their homeland. The battery life of this beacon enabled a target to be tracked up to a month. Beyond that, the battery needs to be replaced. The beacon was not designed for operations in a maritime environment, however, rendering it unsuitable for such environments due to its lack of waterproofing, conspicuous appearance that hindered discreet attachment, and inability to be affixed to the ship's hull. The frogmen spent months of cooperation with the police partners to innovate and modify the beacon. Eventually, they designed a self-made watertight container to house the beacon and made modifications to the appearance such that the device camouflaged with the hull of the ship. Lastly, two methods to attach the payload onto the hull of the target vessels were identified. The first one was by means of using glue that worked in water to stick the beacon onto the hull; the second was to drill and fix the beacon with screws to secure its. All these modifications produced an advanced technology—the improvised beacon. Tests on the improvised beacon were conducted in multiple locations under different environmental conditions but, crucially, not in the actual Indian Ocean AO.

**(2) Explosive**

For the search-and-disable mission, the details to design an effective explosive were equally complicated. There were two modes of detonating the explosive. The explosive could either be activated via command detonation or a timer (see Table 6).

Table 6. Comparison between Command Detonation and Time-Delayed Detonation

|                    | <b>Command detonation</b>                                                 | <b>Time-delayed detonation</b>                            |
|--------------------|---------------------------------------------------------------------------|-----------------------------------------------------------|
| Flexibility        | Able to decide when to detonate explosive.                                | Explosive detonates when timer elapsed.                   |
| Ease of setting up | Have to set up floating canister to house circuitry and antenna.          | Entire circuit can be set up underwater.                  |
| Reliability        | Minor leak to the canister may short circuit the system, causing misfire. | Low chance of leak and misfire as the system is enclosed. |

For the initial years of OOS, the primary mode of detonation used was time-delayed detonation. Five disabling operations were successfully conducted via this mode of detonation. Even when the damage from the explosion was not severe, the pirates' *modus operandi* was to return to shore. Hence, time-delayed detonation was successful in removing threats from the pirates' motherships.

Later in the operation, HQ decided that they wanted to have more control over the detonation, citing the risk of collateral damage as the reason. The inability to control the detonation may have caused harm to innocent vessels and its personnel if they unexpectedly transited near the target vessel during detonation. From the frogmen's perspective, they preferred the time-delay detonation because they would spend less time at the target vessel and reduce their risk of exposure. Furthermore, time-activated detonation had higher reliability compared to using a command-detonated explosive because the canister consisting of the circuitry and receiver unit was susceptible to leakage. As R3, a demolition specialist, explained, "once the canister is leaking, it will sink. It's not possible to use (the explosive) anymore."

While the frogmen had other opinions, they worked with their army counterparts and obtained a remote firing device that was waterproof to 30m depth. They conducted an in-depth study with the manufacturer to ascertain whether it was suitable for maritime usage before eventually fielding it in OOS during the later years. While the advanced technology (command-detonated explosive) was eventually ready to be used for OOS, it was never deployed because the rate of piracy had declined significantly by the time the capability was available.

*c. Improving Survivability*

(1) Shark Shield

To overcome the threat of shark attack, the frogmen wore shark shields on their ankles to repel the sharks. It was a device that sent out an electric pulse that was capable of repelling sharks. While the device might not be suitable when dealing with conventional forces, due to the possible deployment of underwater sensors that could pick up an electric signal, detection was not an issue in AO waters. Somali pirates were poorly equipped and used non-conventional methods.

(2) Night Vision Goggles

In order to avoid confrontations, it was crucial for the frogmen to have the capability to detect the enemy before they were detected. They were equipped with night vision goggles (NVGs) that enabled them to see under low-light conditions. With this technology, they could spot the target vessel from a distance, and as they approached the vessel, they were able to observe the activities of the pirates on deck. This gave the frogmen a significant advantage over the pirates, who lacked the NVG technology and were unable to operate at night with the same level of efficiency.

(3) GPS-Enabled Radio

The GPS-enabled radio allowed frogmen to send their location to the HQ and supporting boat. This feature enabled HQ to keep track of the progress of the mission, rendering assistance when required. It also provided the specific location for the supporting boats to pick up the frogmen after they had exfiltrated from the target vessel. Additionally, the availability of the radio set allowed frogmen to receive last-mile updates from HQ. For example, if a supporting intelligence, surveillance, and reconnaissance asset spotted unusual activity on the target vessel that could be a threat, the frogmen could be ordered to abort the mission.

**d. *Improving Navigation***

**(1) Dive Propulsion System**

The dive propulsion system, colloquially known as “jet boots,” is a body-mounted, battery-operated, mobility system that enabled the frogmen to “swim” at a higher speed. The primary purpose is to assist the diver in navigation by reducing the effect of the current. It would not be powerful enough to overcome a head-on current in an area such as the Indian Ocean, however. R2 explained the utility of this equipment, “the jet boots is just to get you to the right spot. With stronger current, it is impossible to get against it.”

**(2) Update Diving Tactics, Techniques, and Procedures**

Since the dive propulsion system was not able to overcome the current in the location, the frogmen had to adapt the tactics, techniques, and procedures (TTPs) to the environment. Understanding the flow of current and illumination were key to the updated TTPs. The frogmen had to be dropped off from the boat upstream of the current, thus, enabling the current to carry them towards the target vessel. Once they had placed the payload, the frogmen could exfiltrate with the drift of the current and be picked up by support boats downstream of the current. The drop-off and pick-up distance depended on the illumination and traffic density. The brighter the illumination, the farther the drop-off and pick-up locations because the distance at which the frogmen could be spotted by the pirates on the mothership increased according to the illumination. The pick-up and drop-off were preferably in areas with low traffic.

**5. Challenges**

**a. *Actual Sea Conditions Were Different from Test Environment***

According to R1, while the beacon was successfully placed by the means of glue in the tracking mission, there was no signal received by the HQ. The mission was considered unsuccessful. Though the exact reason for failure to receive the signal cannot be determined, one possibility was that the glue was not strong enough to withstand the rocking of the vessel in the harsh environment. The other possibility was that the equipment

had failed during the infiltration by diving. As R1 described the equipment's functionality in their mission,

You think seawater is seawater, but there is a very big difference in seawater in one place and at the other ... The equipment will break down frequently in salty water. I think the maintenance was the biggest thing in keeping the technology up.

***b. Different Expectations between HQ and Ground Force***

In the track-and-avoid mission, the degree of effort required to modify and test the beacon did not justify its use for only one mission. The main reason was for this low deployment rate difference in understanding the purpose of the mission. As R1 described,

We anticipated that it would, but when we were there, they asked why tag when you can just immobilize? Our response was, "sure we can." And they said, "Do it." Our SOF unit thought that [tagging] was something they wanted, but the assessment was wrong.

In the search and disable mission, the change activation mechanism from time-delayed detonation to command-detonation was not fully understood by the frogmen because the risk to the force was higher. However, the consideration from the HQ was to prevent to reduce the risk to the mission, i.e., prevent a strategic backlash in the event of collateral damage.

**D. ANALYSES**

For this operation, since there is integration of technology with SO in both the tasks, I shall examine both of these integrations independently. Table 7 summarizes the overall analysis for the two integrations. For the improvised beacon used in the track-and-avoid mission, the overall synergistic relationship of the integration is negative. For the improvised explosive used in the search-and-disable mission, the overall synergistic relationship is assessed to be neutral.

Table 7. Summary of Integration Between Special Operations and Technology in OOS

|                                                                   | <b>Integrating Improvised Beacon with “Track-and-avoid” Mission</b> | <b>Integrating Command Detonated Explosive with “Search-and-disable” Mission</b> |
|-------------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <u>Specs Ops – Advanced Technology Integration</u>                |                                                                     |                                                                                  |
| Is it a Special Operation?                                        | Yes                                                                 | Yes                                                                              |
| Does it use Advanced Technology?                                  | Yes                                                                 | Yes                                                                              |
| <u>Enabling Conditions</u>                                        |                                                                     |                                                                                  |
| Does this integration have a clear purpose?                       | No                                                                  | Not conclusive                                                                   |
| Is the technology compatibility with Special Operations?          | Not conclusive                                                      | Not conclusive                                                                   |
| Is there integration effort?                                      | Yes                                                                 | Yes                                                                              |
| <u>Outcome</u>                                                    |                                                                     |                                                                                  |
| Is it effective for the mission?                                  | No                                                                  | Not conclusive                                                                   |
| Does it reduce risk to mission/force?                             | No                                                                  | No                                                                               |
| <u>Overall synergistic relationship</u>                           |                                                                     |                                                                                  |
| What is the synergistic relationship for the emergent capability? | Negative                                                            | Neutral                                                                          |

### 1. Integration of Special Operations and Advanced Technology

OOS was assessed to have contributed to the reduction in piracy in Somali waters. While not every mission conducted in OOS was a SO, both the track-and-avoid and search-and-disable missions could qualify as SOs. Table 8 shows the missions that qualified as SO based on the tenets in Chapter II.

Table 8. Qualifying Operations Conducted by Task Force Barracuda as Special Operations<sup>258</sup>

| <b>Special Operations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition: “Small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.” |                                   |                                                                                                                                                                |
| <b>Key Tenets</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Demonstrated in Operation?</b> | <b>Elaboration</b>                                                                                                                                             |
| <b><u>Small scale</u></b> , clandestine, <b><u>covert</u></b> or overt operation                                                                                                                                                                                                                                                                                                                                                                                                                     | Yes                               | The tasks of tracking and disabling is done by a small team of frogmen, undetected by the pirates.                                                             |
| Unorthodox                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Yes                               | The use of specialized equipment such as a beacon to track pirate ships has never been used in conventional warfare.                                           |
| High-risk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Yes                               | Risk to the force is high operating in harsh sea conditions.                                                                                                   |
| <b><u>Significant political</u></b> or military objectives in support of foreign policy                                                                                                                                                                                                                                                                                                                                                                                                              | Yes                               | The objective for Operation Ocean Shield was to keep the sea lane free from piracy and the desired outcome of the mission is aligned to achieve the objective. |
| Oversight at the highest level                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Yes                               | Approval needs to be given by higher headquarters before the tasks force can execute the mission.                                                              |
| Use of military and non-military resources, including intelligence assets.                                                                                                                                                                                                                                                                                                                                                                                                                           | Yes                               | Maritime SOF units were supported by other assets, including boats and helicopters.                                                                            |

In terms of advanced technology, while there was a list of technologies used in the SO, only two items fell into the category of advanced technology according to the model (see Table 9). Four out of six technologies that were used are commercially available, and no modification was required. Three out of six technologies existed in the frogmen’s inventories before OOS. These technologies could not be considered as advanced as they did not provide a capability breakthrough. For analysis of this operation, the advanced technologies that integrated with SO will thus be narrowed to both the payloads, i.e., improvised beacon for tracking vessels and command-detonated explosive for disabling vessels.

<sup>258</sup> Tugwell and Charters, “Special Operations and the Threats to United States Interests in the 1980s,” 35.

Table 9. Qualifying Technology Used by Task Force Barracuda as Advanced Technology

| Type of technology          | Available commercially? | Modification? | Existing frogmen's technology? | Purpose                                                                                   | Advanced technology |
|-----------------------------|-------------------------|---------------|--------------------------------|-------------------------------------------------------------------------------------------|---------------------|
| Improvised beacon           | No                      | Yes           | No                             | To track pirate motherships' location from command ship                                   | Yes                 |
| Command-detonated explosive | No                      | Yes           | No                             | To provide flexibility on the time to detonate, so as to reduce risk of collateral damage | Yes                 |
| Shark shield                | Yes                     | No            | No                             | To repel shark                                                                            | No                  |
| GPS-enabled radio           | Yes                     | No            | Yes                            | To enable communication with HQ and to locate divers and track progress of mission        | No                  |
| Night vision goggles        | Yes                     | No            | Yes                            | To see target vessel as well as enemy in darkness                                         | No                  |
| Diver propulsion systems    | Yes                     | No            | Yes                            | To assist divers in navigation in harsh sea conditions                                    | No                  |

## 2. Enabling Conditions

### a. Purpose

#### (1) Improvised Beacon

While there was a clear intent for OOS—to reduce the number of piracy attacks in Somali waters—it was unclear how that intent translated to the purpose of frogmen and the HQ. The frogmen believed that the development of a maritime-capable beacon to track the vessel was useful for tracking the motherships. HQ thought otherwise, however. The misalignment of expectations of the frogmen and HQ resulted in the underutilization of the technology. Hence, the purpose for integrating the improvised beacon with the frogmen for the track-and-avoid operation was not clear.

## (2) Command-Detonated Explosive

The purpose for the time-delayed explosive that was used in the initial phase of OOS was clear to both HQ and the ground units. Five missions were executed successfully until HQ wanted more control over the detonation to prevent collateral damage. With this change of intent, the purpose of the integration between explosive and frogmen also adapted. While the purpose was clear to HQ, the same could not be said for the frogmen. Due to the change in purpose, the frogmen's mission risk increased and mission confidence decreased due to the reduced reliability of the command-detonated explosive. Again, there was misalignment in the purpose between HQ and frogmen. Hence, the purpose for integrating command-detonated explosive with frogmen for search-and-disable mission was not clear.

### ***b. Integration Effort***

#### (1) Improvised Beacon

The frogmen dedicated significant effort to integrating and enhancing the beacon in order to accomplish the challenging track-and-avoid mission. Initially, during the onset of the operation, there was no viable solution for effectively monitoring the ship to fulfill the mission of tracking and locating the pirates' mothership. The frogmen discovered a similar solution being utilized by the police from their home country and resolved to adapt it for their purposes, however.

As mentioned earlier, the beacon posed limitations, lacking waterproofing and being too conspicuous for use as a reliable tracking device on target vessels. Additionally, finding a suitable method of mounting the beacon proved to be a challenge. After several months of discussions and trial runs with the beacon, the necessary modifications were successfully implemented for the operation.

#### (2) Command-Detonated Explosive

Likewise, the frogmen faced the task of reconfiguring the detonation mechanism for the explosives to suit the intent of HQ. The rigor to go to army counterparts and

manufacturers to confirm the details indicate the strong integration effort spent to ensure the system's reliability and performance.

*c. Compatibility*

To recap, compatibility between systems refers to the technical feasibility of integrating individual components. The willingness displayed in their efforts, including engaging with the army counterpart to understand the command-detonated explosive on land and manufacturer to verify crucial details to ensure it was suitable for maritime usage, exemplified the level of integration invested to be assured of the system's performance.

(1) Improvised Beacon

Despite modifying the improvised beacon to facilitate transportation by the frogmen during the infiltration phase, it still fell short of addressing the need for the frogmen to surface during deployment. The technical challenge lay in the fact that the signal transmission could only occur through the medium of air. Consequently, the frogmen were compelled to resurface and affix the improvised beacon above the waterline on the ship's side.

One argument could suggest that the duration of exposure during resurfacing was relatively brief, and the frogmen operated under the cover of darkness in close proximity to the ship, thus mitigating the incompatibility. Regardless, this approach still introduced a higher level of risk compared to conducting the entire mission underwater, which was the fundamental purpose of employing frogmen. Consequently, the improvised beacon was evaluated as incompatible with the frogmen's operational requirements.

(2) Command-Detonated Explosive

Likewise, the command-detonated explosive could be transported by frogmen underwater for prolonged duration and retain its functionality. The frogmen would need to break the surface at the target, however, to set up the floating canister that contained the detonation circuitry and the receiver unit to receive signals back to HQ. This process also posed a risk of water entry into the canister, which could potentially short circuit and render it inoperable, posing a risk to the mission. Hence, the compatibility for command-detonated

explosive was assessed to be incompatible with the frogmen for search-and-disable mission.

### **3. Outcomes**

Chapter II discusses how the performance of a system against intended objectives can be evaluated retrospectively through the synergistic outcomes of system integration. In the case of OOS, however, both the improvised beacon and the command-detonated explosive technologies were not used enough to provide an accurate assessment of their effectiveness. Based on the limited findings from OOS, it was determined that integrating the improvised beacon with frogmen into the track-and-avoid mission had a negative outcome, while integrating the command-detonated explosive with frogmen in the search-and-disable mission was neutral. Nevertheless, subsequent paragraphs will explore and predict the potential effectiveness of integrating these technologies with frogmen if more opportunities for deployment are available. This would be done using a predictive and speculative lens rather than basing on actual operational data.

#### ***a. Risk***

The utilization of advanced technology generally aims to minimize the risk to both the mission and the force. Nonetheless, this did not hold true for the missions assigned to TF Barracuda. The harsh operating environment for frogmen already poses significant uncertainty in technology performance. Moreover, the introduction of advanced technology, i.e., improvised beacon and command-detonated explosive, to achieve the desired outcome of tracking and destroying, respectively, a mothership increases risk due to the necessity for frogmen to surface during the mission's final stages, which in turn increases the probability of detection by adversaries.

##### **(1) Improvised Beacon**

Specific to the improvised beacon, there was no plan to remove the improvised beacon after its deployment. Hence, the chance of pirates returning to shore and discovering the beacon was high. Once the device had been discovered, the pirates will

understand TF Barracuda's tactics and may design a countermeasure to prevent the other motherships from being tracked.

(2) Command-Detonated Explosive

For the command-detonated explosive, the main critique lies in the reliability of the system. Once water enters the canister containing the circuitry, the HQ would not be able to trigger the detonation and the mission would fail. Hence, for this reason, the risk to the mission is significant.

*b. Effectiveness*

(1) Improvised Beacon

Evaluating effectiveness based on only one failed tagging mission is difficult. Conceptually, it is a good idea to be able to locate the positions of motherships at any time. Besides providing advance warning to merchant ships to avoid the area, it could also allow the ships involved in OOS to pre-position themselves, such that they could react to any situation more readily. There was a critique on the battery life of the improvised beacon, however. It would only last one month. For an operation that lasted many years, and with consideration of the risk undertaken by frogmen to place the beacon, the duration of one month does not seem to justify the risk. Therefore, even if more improvised beacons were deployed in OOS, the integration for improvised beacons for the tracking mission would remain ineffective.

(2) Command-Detonated Explosive

Using explosives to disable motherships was assessed to be highly effective to eliminate the piracy threat temporarily as seen from the success of using time-delay detonation explosives. Damage caused to certain parts of the motherships would render them out of action for an extended period. The absence of motherships, therefore, mitigated piracy threats and kept the merchant vessels safe. Command-detonated explosives further enhanced the effectiveness by allowing decision makers to select the time for detonation. This capability could eradicate the public backlash from any accidental collateral damage

from using the time-delayed detonation. Hence, the command-detonated explosive was assessed to be effective if more opportunities were given.

## **E. CONCLUSION**

During both missions to track and disable the pirates' motherships under OOS, advanced technology in the form of improvised beacons and command-detonated explosives were integrated with the frogmen to deliver these technologies to the targets. According to the model used in Chapter II, the integration of advanced technology and SO did not achieve a synergistic outcome in OOS. This does not necessarily mean that the advanced technology is not useful, however. Rather, it highlights the importance of understanding and aligning the mission's purpose with the capabilities of the technology, as the same technology can have different outcomes in different missions, even under similar conditions.

Furthermore, this case study revealed that it may not always be feasible to reduce risk and increase effectiveness when integrating advanced technology with SO. When the benefits outweigh the risks, however, the integration can still achieve a synergistic outcome, as demonstrated by HQ's decision to deploy command-detonated explosives over time-delayed explosive.

## **VI. CONCLUSIONS AND RECOMMENDATIONS**

Today, global conflicts have shifted from traditional warfare to the gray zone that exists between peace and war and employs hybrid warfare tactics. In this ever-changing environment, SO remain crucial. The ability to use a small force to achieve strategic effects, especially in peacetime, offers policymakers a wider range of strategic options in the gray zone conflict.<sup>259</sup> Furthermore, the rapid advancement of technology—particularly in the commercial sector—has created unprecedented opportunities to gain advantage over adversaries. As a result, policymakers and military commanders must remain vigilant in their efforts to keep pace with these developments in order to maintain a competitive edge.

There has not been sufficient discussion and research done in this field to consider the possible outcomes that arise from the integration between SO and advanced technology and the conditions that enable this integration, however. This research aims to provide insights into those gaps by developing a conceptual model that identifies the relationship between SO and advanced technology—specifically, the outcomes one should expect from the integration of SO and advanced technology and the conditions that are required to enable this integration.

### **A. SUMMARY OF KEY FINDINGS**

While a conclusion could not be definite using simply three case studies, there are strong indications that the abovementioned integration could be elaborated using the conceptual model that was modified from system theory. This claim is supported by the following summary of key findings from this research, with relevant examples highlighted for emphasis.

#### **1. Integration between Special Operations and Advanced Technology**

This research suggests that SO are suitable for integration with advanced technology due to its unique characteristics. For most instances, SO are small-scale,

---

<sup>259</sup> Gray, “Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?”

unorthodox tactical actions generating high-end strategic effects. Such nimbleness creates opportunities for advanced technology to be introduced and integrated. The importance and criticality of SO is usually accompanied by direct support from policymakers, which ensures the availability of resources. In addition, due to the nature of being small scale and unorthodox, the units conducting the operations are highly adaptable and there is no need to mass produce, which strains resources and results in longer lead time.

## **2. Enabling Conditions**

This research emphasizes that three uniquely independent enabling conditions—purpose, integration effort, and compatibility—are critical to successful integration.

### ***a. Purpose***

Every SO is planned and executed for a different purpose. Past success of an integration of technology may not be applicable to subsequent missions. As such, the purpose of every mission should be carefully examined and clearly understood before the search for advanced technology to enhance the operation. One example can be seen from the case study of OOS. The frogmen went through the rigor to design and integrate the tracking beacon as their capability without fully understanding the purpose of the mission. Therefore, while the beacon used for tracking ships is compatible with the underwater operation, and the frogmen successfully validated their TTPs, the outcome was ineffective, mostly due to the lack of deployment opportunities, because the purpose of the mission was understood differently in the first place.

### ***b. Integration Effort***

To recap, integration effort refers to the willingness to produce a successful integration. It requires commitment of resources, including manpower, time, and money. Successful integration usually requires support from high-ranking personnel and strong inter-agency coordination because SO units do not generally own or maintain advanced technology. All three case studies demonstrated the need for a substantial degree of integration effort to fulfill the operation. Usually, when the outcome of the SO is of strategic implication, the support comes from heads of state. For example, President Bush

and President Obama directly approved Operation Olympic Games, and multiple entities, including intelligence, scientists, and engineers, supplied the coders with the critical information to build the code.

*c.       Compatibility*

It is fundamental that SO and advanced technology be compatible before any integration commences. To be compatible means the two components are able to overcome any technicality in the integration. One example that clearly showed the value of compatibility was the EW system that was used in Operation Orchard. Due to the limited range of the EW system, it had to be deployed by the planes involved in the operation, i.e., F-15s or F-16s, in order to manipulate the Syrian IADS. If the systems had not been compatible in the first place, the option of the airstrike would have been too risky and alternatives might have had to be considered.

**3.       Outcomes**

This research asserts that integration of SO and advanced technology under the right enabling conditions has potential to produce a positive emergent capability, which would produce a synergistic outcome. To qualify as a synergistic outcome, the risk of the SO is reduced and/or the effectiveness of the SO is enhanced. To be clear, there could also be exceptions that the integration between advanced technology and SO attain a synergistic outcome when the increase in effectiveness outweighs the increase in risk. In such a situation, the policymakers and the military leaders generally accept that undertaking risk is necessary to generate an effective outcome. An example was shown in OOS where HQ decide to deploy command-detonated explosives knowing that the risk to the frogmen would increase.

*a.       Risk*

To recap, risk to SO consists of two components: risk to mission and risk to force. The integration of technology with SO shall generally not introduce greater risk but reduce it in one or both components. Again, in the case of Operation Orchard, the manipulation of Syria's IADS enabled Israeli planes to fly into al-Kibar undetected and unimpeded. The

pilots could focus solely on dropping munitions on the target, undistracted by SAMs, which critically reduced both the risk to the mission and the risk to the force.

***b. Effectiveness***

After examination of the case studies, this research supports the position that enhancing the effectiveness of SO should not be undertaken simply to achieve mission objectives but more importantly, it should improve the quality of the outcome. Using Operation Olympic Games for elaboration, the main objective was to delay Iran's nuclear program. The Stuxnet worm was seen as effective not primarily due to its ability to destroy centrifuges, however, but to its ability to propagate while remaining concealed, thereby persistently causing issues and creating confusion among the Iranian scientists.

**B. IMPLICATIONS AND RECOMMENDATIONS**

This thesis has provided a conceptual model to capture the findings from the research. The purpose of the conceptual model is to improve decision making when faced with the need to integrate advanced technology with SO. The conceptual model has provided insights to two key questions:

- When would integration between advanced technology and SO be successful?
- What are the expected outcomes from a successful integration between advanced technology and SO?

Based on this research, three recommendations are proposed in the areas, namely conceptual, organizational, and doctrinal:

**1. Conceptual**

Policymakers and military commanders should consider the employment of SO as an instrument of statecraft from a systems perspective. Undertaking this perspective would allow them to view forces, including conventional and non-conventional, military and non-military, and capabilities, such as advanced technology and state-of-the-art equipment, as mere components for selection, rather than considering SOF as the dominant tools to fulfill

SO. This perspective offers the policymakers and military commanders the further expansion of strategic choices as compared to solely relying on narrow SOF capabilities.

## **2. Organizational**

Policymakers and military commanders should consider the implementation of an adaptive TF structure for SO. This approach involves establishing temporary TFs that can be deployed to achieve specific strategic objectives. As demonstrated in the case studies, the application of advanced technologies in SO often requires capabilities that may not be organically possessed by SOF, and not all SO are exclusively conducted by SOF. By organizing as operational TFs, decision makers can select the most suitable forces and capabilities for each mission, ensuring optimal effectiveness and adaptability. This method also unshackled the burden for SOFs to conduct all SO and sustained all requisite capabilities and technologies.

## **3. Doctrinal**

Policymakers, military commanders, and technological partners responsible for strategy development, operational planning, tactical execution, and capability development in SO should consider integrating the conceptual model into their doctrines. This conceptual model serves as a valuable framework, guiding the effective integration of advanced technology with SO. It offers insights into crucial aspects such as force and capability selection, the conditions for successful integration, and the evaluation of effectiveness and risk. By incorporating this model, decision makers can enhance their decision-making processes and improve the overall outcomes of SO.

## **C. AREAS FOR FUTURE RESEARCH**

This research, which explores integration between SO and advanced technology, is one of the first and, hopefully, one of many to come. Due to the constraint of time and the nature of the classification, the scope of the research is intended to be general but informative and applicable. Hopefully, it provokes readers' inquisitive minds to conduct deeper research by considering the following questions:

- Is advanced technology for SO only used once? How could a competitive advantage be sustained using advanced technology with SO?
- How can advanced technology be integrated with the conventional forces?  
Can the conceptual model be applied to conventional forces?

Following from these questions, future research could focus on identifying new theories to sustain competitive advantage using advanced technology for SO and examining conventional military case studies to validate the model for integration of advanced technology for military operations.

#### **D. CONCLUSION**

While this research is intended to provide valuable insights for anyone interested in the relationship between SO and advanced technology, its primary audience is composed of three groups: policymakers, military commanders, and technological partners. Often, these three groups have different interests and concerns, and failure to understand each other would naturally lead to a failure of integration. This conceptual model could bridge the gap by aligning all three parties to view integration from the same starting point. In other words, establishing unity of effort. This alignment would hopefully bring about consensus in decision making, leading to successful integration. While it is not a guide that prescribes detailed steps to fulfill the integration, the conceptual model serves as a useful framework to consult during planning for integration in an increasingly complex world.

In this way, the model could enhance SO through the integration of advanced technology to produce higher quality outcomes.

## **APPENDIX A. INTERVIEW PROTOCOL**

The content of this interview will only be solely for academic purpose and would not be published without the consent from the interviewees. The classification of the interview is limited to unclassified information. The anonymity of the interviewees shall be maintained in the transcript or thesis.

### **Introduction. (About yourself)**

Could you share your appointment during the Operation Ocean Shield and what was your role in it? Can you share some of your responsibilities?

### **Question 1. (Overview of the Operation)**

Could you describe on the organization structure of Task Force Barracuda? Could you elaborate on what was your mission? How did your mission impact the overall success of Operation Ocean Shield?

### **Question 2. (Overview of the technology)**

In the context of the special operation, how were some technologies that were used during Operation Ocean Shield? Can you explain to me how the technology works, in terms of where it came from, how did work, what is it operations envelope and limitation? Will you be able to walk me through the Tactics, Techniques and Procedures (TTPs) that were used by the Task Force?

### **Question 3. (Understanding the effort behind employing the technology)**

Can you describe the enabling conditions in terms of compatibility and integration that were present to enable the use of technology in Operation Ocean Shied? In other words, was there anything that the Task Force did to integrate the technology with the SOFs teams? Were there any challenges faced and how it was overcome?

(Note: In my thesis, I would be using the concept of enabling condition to analyze understand the effort required to integrate the technology with special operation. The three enabling conditions are purpose, compatibility and integration effort. Purpose refers to the intent, objectives and desired outcome of the mission. Compatibility refers to the technical

feasibility for a technology to be used in special operations. E.g., Can the technology work in the environment? Can it communicate with the operators? Integration effort refers to the willingness of management to employ the technology. E.g. Education/training required to use the technology? Using technology that belong to some other agencies that could be helpful? Modification of the technology to suit your operation.)

**Question 4. (Effectiveness of the technology)**

Is the use of technology effective? Why? Is the mission high-risk? Is it worth the risk?

(Note: I define effectiveness as the quality of the outcome. It is not limited to the efficient use of resource. Risk refers to both risks to force and risk to mission. Risk to force is the likelihood of casualties, risk to mission Is the likelihood the mission would fail.)

**Question 5. (Importance of the technology and its alternatives)**

If the technology was not available, how would it impact the mission? Were there alternatives? Were there better ideas that did not get implemented?

## APPENDIX B. LIST OF INTERVIEWEES

The following is a list of interviewees from Operation Ocean Shield–Task Force Barracuda.

| Position              | Rank           | Reference Number |
|-----------------------|----------------|------------------|
| On-Scene Commander    | Major          | R1               |
| Assistant Team Leader | Staff Sergeant | R2               |
| Team member           | Sergeant       | R3               |

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX C. SAMPLE INTERVIEW TRANSCRIPT

The following is a sample interview transcript of Respondent #1:

### **Coded interview of Respondent #1**

#### Legend

Red = Fact

Blue = Opinion/Beliefs

Yellow = Sentiments – Positive [+], Negative [-], Neutral [N]

March 8, 2023

On-scene commander of Task Force Barracuda

Lieutenant Colonel

**Please give an introduction about yourself and describe the position and role you play during Operation Ocean Shield.**

I was the on-scene commander of the Task Force Barracuda. In our organization, it means that I was the tactical leadership on the ground, in this case, on the sea. In our structure, there was a commanding officer at the Navy Frigate with a small HQ (Headquarter) element. We were stationed on the boat. The task force on the boats were commanded by one team commander and I had also helicopters and airplanes under my tactical command.

**Could you explain the mission of the Task Force?**

The piracy numbers were very high in the Somali waters. On top of my head, there were about 10–20 ships and 750 hostages being taken. Along the coast of Somalia, there were pirate hotspots and there were maybe 4–5 big merchant vessels in every pirate hotspot. What we want to do with many European navies at least was to reduce piracy. We, as a task force, have two tasks. The first was to immobilize the mothership of the pirates. The pirates used these motherships to go out to the ocean and then they use smaller boats to get close to the merchant vessels, hijack it, hold the crew hostage and steer the ship back to Somali coast.

The second task was if we could not immobilize the ship, we would tag it with beacon.

### **How did the task force immobilize the ship?**

We used explosives. I can't tell you how in detail. The amount of explosive use would not sink the ship, it is a surgical use of explosive to stop the pirates from driving the ship.

### **What about the beacons? How was it used?**

The concept for placing the beacon was to see and avoid. The whole thinking was that all the navies would know where the (pirates) motherships were and then they could warn the merchant vessels that the pirates are there. They will then take another route.

### **What kind of beacons were used? Is it an innovation or commercially off the shelf product?**

These are self-made because we were looking for watertight product. The beacons also have to be camouflaged for many months. These are items not available on the market. We work together with other units and build our own product essentially.

### **What is the developmental process of the product?**

I don't think this is a secret. We worked together with the police units who are very experience with beacon. [+] We had a lot of exchanges with them on how to beacon work. They shared their methods and we shared ours. For us, when you are in the water, it is very difficult to work on a ship, even more so for the hull of the ship. [-] We can't use a boat and drive to the mothership in the Somali water. We thought of another method to work from the water to get the beacon to the ship. We tested the range from a distance. It is really important to incorporate their technical knowledge with our diving knowledge and experience. It takes many months of trial and error to arrive at a working solution.

### **How did the mission impact the overall success of Operation Ocean Shield? Did the use of technology reduce the risk to the mission and/or force?**

At the start of the mission, we thought that we would put many beacons on ships. But actually the top leadership wanted immobilization more than tagging. So we only did one tagging operation. To your question, did it contribute to the overall success? I would say no. [-] We anticipated that it would, but when we were there, they asked why tag when you can just immobilize? Our response was, "sure we can." And they said "do it." Our SOF unit thought that this (tagging) was something they wanted, but the assessment was wrong.

### **Was the use of technology effective?**

We did a lot of trial and error at different places in the world but not in Somalia.[+] We tested using screw and we tested using glues, many different types of glues. We found screwdrivers that work in the water, we also found glue that worked. But in Somalia nothing worked. So this was one of the lesson learnt. You think sea water is sea water, but there is a very big difference in sea water in one place and at the other. While many things went wrong in the tagging operation, we eventually manage to place a beacon on the ship. There was only glue on it. We didn't get a signal from the beacon. We suspected that it was due to the rocking of the ship that cause the beacon to fall off again. However, we can't be sure. We had many lessons learnt from that operation and we have continued to innovate and improve on the product and procedures. But that mission was not a successful operation. [-]

Due to monsoon in that area, there are only a two-month windows that the mission can be executed. So, for most of the year, there was a heavy current and strong wind. The sea state was 4–5 and the waves were big. The condition was worsened when the current and wind are going different directions.

#### **Is the mission worth the risk? How was the risk managed?**

This was the question that the top leaders have as well. We did a lot of testing. Whether it is worth the risk depends on the context. It depends on how high the hull of the ship, how many people are on the ship? How many people are awake on the ship? How aggressive they are? How on the ball they are? For the Somali pirates, they are awake the whole night eating drugs and they carry their AK-47 around.

We need to operate in hour of darkness. We need to find out what is the current? With all the above factors taken into consideration, we will then assess if we can do the mission. It is not math, but it also depend on the feeling that we have based on experience. I will looked around the room, looking every team leaders in his eyes and ask, are you happy to do this? Yes or no? No, why not? This is the conversation we had every operation.

In general, I would say it is worth the risk, but there is a lot of nuance in this question. There is always strategic risk in the mission we do. Then the question is, are we able to do it? We may receive a lot of pressure to do it, but in the end, we are the ones in the water. We want to do the mission, but we don't want to die or be taken hostage by Somalis. It is also our culture that if we can't do it, we will say no to our leaders because of these reasons. There was one occasion where they were not happy, but they understood it and in all the other operations we were successful. So, we build the trust and accept our answer.

#### **Do you have any other points to add to this interview?**

While our discussion was focused on the beacon, we also used other technology for the operation. For example, the divers have propulsion device on the hips that assist us in swimming in the water with strong current. We also dive with night vision goggles. It supported us in finding the ship. We also wear shark shield on our ankle. It is something that send out electric pulse to repel sharks. We haven't tested it. We will also have radio with GPS signals. For communication, the divers communicate with hand signals. The radios are for them diver to speak to the boats.

We have a lot of technology to keep the diver safe in order to put a small piece of equipment on the ship. So, I would say you need the whole combination of technology to eventually put the beacon on ship.

The biggest challenge of these equipment is not with the acquisitions but with the maintenance.[N] The equipment will break down frequently in salty water.[-] I think the maintenance was the biggest thing in keeping the technology up.

## APPENDIX D. CONTENT ANALYSIS

The following content analysis is done on the transcript of Respondent #1:

| Special Operations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Technology                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Enabling Condition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                              | Outcomes                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Integration Effort                                                                                                                                                                                                                                                                                                                                                                                                                                   | Compatibility                                                                                                                                                | Effectiveness                                                                                                                                                                                                                                                                                                   | Risk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>What we want to do with many European navies at least was to reduce piracy. We, as a task force, have two tasks. The first was to immobilize the mothership of the pirates. The pirates used these motherships to go out to the ocean and then they use smaller boats to get close to the merchant vessels, hijack it, hold the crew hostage and steer the ship back to Somali coast.</p> <p>We were stationed on the boat. The task force on the boats were commanded by one team commander and I had also helicopters and airplanes under my tactical command.</p> <p>The piracy numbers were</p> | <p>These are self-made because we were looking for watertight product. The beacons also have to be camouflaged for many months. These are items not available on the market. We work together with other units and build our own product essentially.</p> <p>For example, the divers have propulsion device on the hips that assist us in swimming in the water with strong current. We also dive with night vision goggles. It supported us in finding the ship. We also wear shark shield on our ankle. It is something that send out electric pulse to repel sharks. We haven't tested</p> | <p>We anticipated that it would, but when we were there, they asked why tag when you can just immobilize? Our response was, "sure we can." And they said "do it." Our SOF unit thought that this (tagging) was something they wanted, but the assessment was wrong.</p> <p>There is always strategic risk in the mission we do. Then the question is, are we able to do it? We may receive a lot of pressure to do it, but in the end, we are the ones in the water. We want to do the mission, but we don't want to die or be taken hostage by Somalis. It is also our culture that if</p> | <p>We worked together with the police units who are very experienced with beacon. [+] We had a lot of exchanges with them on how to beacon work. They shared their methods and we shared ours.</p> <p>The biggest challenge of these equipment is not with the acquisitions but with the maintenance.[N] The equipment will break down frequently in salty water.[-] I think the maintenance was the biggest thing in keeping the technology up.</p> | <p>So this was one of the lesson learnt. You think sea water is sea water, but there is a very big difference in sea water in one place and at the other</p> | <p>To your question, did it contribute to the overall success? I would say no.[-]</p> <p>But that mission was not a successful operation. [-]</p> <p>However, we can't be sure. We had many lessons learnt from that operation and we have continued to innovate and improve on the product and procedures.</p> | <p>This was the question that the top leaders have as well. We did a lot of testing. Whether it is worth the risk depends on the context. It depends on how high the hull of the ship, how many people are on the ship? How many people are awake on the ship? How aggressive they are? How on the ball they are? For the Somali pirates, they are awake the whole night eating drugs and they carry their AK-47 around.</p> <p>We need to operate in hour of darkness. We need to find out what is the current? With all the above factors taken into consideration, we will then assess if we can do the mission. It is</p> |

| Special Operations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Technology                                                                                                                                                             | Enabling Condition                                                                                                                                                                                                                                        |                    |               | Outcomes      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                   | Integration Effort | Compatibility | Effectiveness | Risk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>very high in the Somali waters. On top of my head, there were about 10–20 ships and 750 hostages being taken. Along the coast of Somalia, there were pirate hotspots and there were maybe 4–5 big merchant vessels in every pirate hotspot.</p> <p>We used explosives. I can't tell you how in detail. The amount of explosive use would not sink the ship, it is a surgical use of explosive to stop the pirates from driving the ship.</p> <p>Due to monsoon in that area, there are only a two-month windows that the mission can be executed. So, for most of the year, there was a heavy current and strong wind. The sea state was 4–5 and the waves were big. The</p> | <p>it. We will also have radio with GPS signals. For communication, the divers communicate with hand signals. The radios are for them diver to speak to the boats.</p> | <p>we can't do it, we will say no to our leaders because of these reasons. There was one occasion where they were not happy, but they understood it and in all the other operations we were successful. So, we build the trust and accept our answer.</p> |                    |               |               | <p>not math, but it also depend on the feeling that we have based on experience. I will looked around the room, looking every team leaders in his eyes and ask, are you happy to do this? Yes or no? No, why not? This is the conversation we had every operation.</p> <p>We have a lot of technology to keep the diver safe in order to put a small piece of equipment on the ship. So, I would say you need the whole combination of technology to eventually put the beacon on ship.</p> |

| Special Operations                                                                                                                                                                                                                                                                                                                                              | Technology | Enabling Condition |                    |               | Outcomes      |      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------------|--------------------|---------------|---------------|------|
|                                                                                                                                                                                                                                                                                                                                                                 |            | Purpose            | Integration Effort | Compatibility | Effectiveness | Risk |
| <p>condition was worsened when the current and wind are going different directions.</p> <p>The concept for placing the beacon was to see and avoid. The whole thinking was that all the navies would know where the (pirates) motherships were and then they could warn the merchant vessels that the pirates are there. They will then take another route.</p> |            |                    |                    |               |               |      |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- Adee, Sally. "The Hunt for The Kill Switch." *IEEE Spectrum*, May 1, 2008. <https://spectrum.ieee.org/the-hunt-for-the-kill-switch>.
- Albright, David, Paul Brannan, Andrea Stricker, Christina Walrond, and Houston Wood. *Preventing Iran from Getting Nuclear Weapons: Constraining Its Future Nuclear Options*. Washington, D.C.: Institute for Science and International Security, 2012. [https://www.researchgate.net/profile/David-Albright-2/publication/267689515\\_Preventing\\_Iran\\_from\\_getting\\_nuclear\\_weapons\\_constraining\\_its\\_future\\_nuclear\\_options\\_p\\_10\\_5\\_March\\_2012/links/56f2884608ace034d8c635a5/Preventing-Iran-from-getting-nuclear-weapons-constraining-its-future-nuclear-options-p-10-5-March-2012.pdf](https://www.researchgate.net/profile/David-Albright-2/publication/267689515_Preventing_Iran_from_getting_nuclear_weapons_constraining_its_future_nuclear_options_p_10_5_March_2012/links/56f2884608ace034d8c635a5/Preventing-Iran-from-getting-nuclear-weapons-constraining-its-future-nuclear-options-p-10-5-March-2012.pdf).
- Albright, David, and Andrea Stricker. "Iran's Nuclear Setbacks: A Key for U.S. Diplomacy." *PBS*, January 19, 2011. <http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2011/01/irans-nuclear-setbacks-a-key-for-us-diplomacy.html>.
- Albright, David, and Christina Walrond. *Iran's Gas Centrifuge Program: Taking Stock*. Iran Reports. Washington, D.C.: ISIS, 2010. <https://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock/8>.
- Arnold, Zachary. "What Investment Trends Reveal about the Global AI Landscape." *Brookings* (blog), September 29, 2020. <https://www.brookings.edu/techstream/what-investment-trends-reveal-about-the-global-ai-landscape/>.
- Arquilla, John. *From Troy to Entebbe: Special Operations in Ancient and Modern Times*. Lanham, Md: University Press of America, 1996.
- BBC News*. "Israel Admits Striking Suspected Syrian Nuclear Reactor in 2007." March 21, 2018. <https://www.bbc.com/news/world-middle-east-43481803>.
- Bertalanffy, Ludwig von. *General System Theory: Foundations, Development, Applications*. New York, NY: Braziller, 1984.
- Black, Ian. "Iran and Iraq Remember War That Cost More than a Million Lives." *The Guardian*, September 23, 2010. ProQuest.
- Bridger, James M. "Safe Seas at What Price? The Costs, Benefits and Future of NATO's Operation Ocean Shield." *NATO*, no. 95 (September 2013). [https://www.files.ethz.ch/isn/169344/rp\\_95.pdf](https://www.files.ethz.ch/isn/169344/rp_95.pdf).
- Britannica*, s.v. "military technology." Accessed March 17, 2023. <https://www.britannica.com/technology/military-technology/Prehistory#ref57563>.

- Broad, William J., John Markoff, and David E. Sanger. "Israel Tests Called Crucial In Iran Nuclear Setback." *New York Times*, January 16, 2011. ProQuest.
- Bush, George W. *Decision Points*. New York: Crown Publishers, 2010.
- Churchman, C. West. *The Design of Inquiring Systems: Basic Concepts of Systems and Organization*. New York: Basic Books, 1971.
- CMSadmin. "The Israeli 'E-Tack' on Syria – Part I." *Airforce Technology*, March 9, 2008. <https://www.airforce-technology.com/features/feature1625/>.
- CMSadmin. "The Israeli 'E-Tack' on Syria – Part II." *Airforce Technology*, March 10, 2008. <https://www.airforce-technology.com/features/feature1669/>.
- Cronin, Audrey K. *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists*. New York, NY: Oxford University Press, 2020.
- Cronin, Audrey K. "Technology and Strategic Surprise: Adapting to an Era of Open Innovation." *The U.S. Army War College Quarterly: Parameters* 50, no. 3 (August 2020): 71–84. <https://doi.org/10.55540/0031-1723.2675>.
- Davenport, Kelsey. *UN Security Council Resolutions on Iran*. Washington, D.C.: Arms Control Association, 2022. <https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran>.
- Falliere, Nicolas, Liam O Murchu, and Eric Chien. *W32. Stuxnet Dossier*. Version 1.3. Cupertino, CA: Symantec Security Response, 2011. [https://www.wired.com/images\\_blogs/threatlevel/2010/11/w32\\_stuxnet\\_dossier.pdf](https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf).
- Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (February 2011): 23–40. <https://doi.org/10.1080/00396338.2011.555586>.
- Follath, Erich, and Holger Stark. "The Birth of a Bomb: A History of Iran's Nuclear Ambitions." *Der Spiegel*, June 17, 2010. <https://www.spiegel.de/international/world/the-birth-of-a-bomb-a-history-of-iran-s-nuclear-ambitions-a-701109.html>.
- Follath, Erich, and Holger Stark. "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor." *Der Spiegel*, November 2, 2009. <https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html>.
- Fulghum, David A., and Douglas Barrie. "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target." *ABC News*, October 8, 2007. <https://abcnews.go.com/Technology/story?id=3702807&page=1>.

- Fulghum, David A., and Robert Wall. "U.S. Electronic Surveillance Monitored Israeli Attack on Syria." *Aviation Week*, November 21, 2007. <https://www.worldsecuritynetwork.com/Israel-Palestine/AviationWeek.com/U.S.-Electronic-Surveillance-Monitored-Israeli-Attack-On-Syria>.
- Fulghum, David A., Robert Wall, and Amy Butler. "Israel Shows Electronic Prowess." *Aviation Week*, November 25, 2007. [http://www.aviationweek.com/aw/generic/story\\_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess](http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess).
- Garamone, Jim. "U.S. Drone Strike Kills al-Qaida Leader in Kabul." *DOD News*, August 2, 2022. <https://www.defense.gov/News/News-Stories/Article/Article/3114362/us-drone-strike-kills-al-qaida-leader-in-kabul/>.
- Gartner. "Definition of Advanced Technology." Gartner. Accessed May 1, 2023. <https://www.gartner.com/en/information-technology/glossary/advanced-technology>.
- Gault, Matthew. "Even the Pentagon Is Using ChatGPT Now." *Vice*, February 9, 2023. <https://www.vice.com/en/article/5d37y3/even-the-pentagon-is-using-chatgpt-now>.
- Geoghegan, Tom, and Sarah Shenker. "'Stealth Helicopters' Used in Bin Laden Raid." *BBC News*, May 6, 2011. <https://www.bbc.com/news/world-us-canada-13297846>.
- Gigova, Radina. "Who Vladimir Putin Thinks Will Rule the World." *CNN*, September 2, 2017. <https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>.
- Gray, Colin S. *Explorations in Strategy*. Westport, Conn: Greenwood Press, 1996.
- Gray, Colin S. "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?" *The U.S. Army War College Quarterly: Parameters* 29, no. 1 (October 1999): 2–24. <https://doi.org/10.55540/0031-1723.1916>.
- Hari, Johann. "You Are Being Lied to About Pirates." *The Independent*, January 5, 2009. <https://www.independent.co.uk/voices/commentators/johann-hari/johann-hari-you-are-being-lied-to-about-pirates-1225817.html>.
- House, White. "Maintaining Military Advantage Through Science & Technology Investment," 2019.
- Hughes, Alex. "ChatGPT: Everything You Need to Know about OpenAI's GPT-4 Tool." *BBC Science Focus Magazine*, March 16, 2023. <https://www.sciencefocus.com/future-technology/gpt-3/>.
- Issa-Salwe, Abdisalam M. *The Collapse of the Somali State: The Impact of the Colonial Legacy*. London: Haan, 1996.

- Jafarzadeh, Alireza. "Remarks by Alireza Jafarzadeh on New Information on Top Secret Projects of the Iranian Regime's Nuclear Program | Iran Watch," August 14, 2002. <https://www.iranwatch.org/library/ncri-new-information-top-secret-nuclear-projects-8-14-02>.
- Jewish Telegraphic Agency. "Turkey Puts Israeli Sortie behind It." November 6, 2007. <http://www.jta.org/cgi-bin/iowa/breaking/105120.html>.
- Jewish Virtual Library. "Sayeret Matkal." Accessed April 26, 2023. <https://www.jewishvirtuallibrary.org/sayeret-matkal>.
- Jonathan Bellish. "The Economic Cost of Somali Piracy 2012." One Earth Future Foundation, 2013. [https://oneearthfuture.org/sites/default/files/documents/publications/View%20Full%20Report\\_3.pdf](https://oneearthfuture.org/sites/default/files/documents/publications/View%20Full%20Report_3.pdf).
- Kamiński, Mariusz Antoni. "Operation 'Olympic Games.' Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Programme." *Security and Defence Quarterly* 29, no. 2 (2020): 63–71. <https://doi.org/10.35467/sdq/121974>.
- Katz, Yaakov. "And They Struck Them with Blindness." *The Jerusalem Post*, September 29, 2010. <https://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness>.
- Katz, Yaakov. *Shadow Strike: Inside Israel's Secret Mission to Eliminate Syrian Nuclear Power*. New York: St. Martin's Press, 2019.
- Kiras, James D. "Future Tasks: Threats and Missions for SOF." *Special Operations Journal* 5, no. 1 (January 2019): 6–24. <https://doi.org/10.1080/23296151.2019.1581424>.
- Klieger, Noah. "A Strike in the Desert." *Ynetnews*, November 2, 2009. <https://www.ynetnews.com/articles/0,7340,L-3799227,00.html>.
- Knops, Raymond. "The Challenge of Piracy: International Response and NATO's Role." NATO Parliamentary Assembly, November 2012.
- Lambakis, Steve. "Colin Gray on the Strategic Utility of Special Operations." *Comparative Strategy* 40, no. 2 (March 2021): 205–8. <https://doi.org/10.1080/01495933.2021.1880841>.
- Langner, Ralph. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Arlington, Hamburg, Munich: The Langner Group, 2013. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.
- Lesch, David W. *Syria: The Fall of the House of Assad*. New Haven, CT: Yale University Press, 2012.

- Lykke Jr, Arthur F. "Toward an Understanding of Military Strategy." In U.S. *Army War College Guide to Strategy*, Joseph R. Cerami and James F. Halcomb, eds. Cumberland County, VA: U.S. Army War College, 2001, 179–85.
- MacAskill, Ewen, and Chris McGreal. "George Bush's Memoirs Reveal How He Considered Attacks on Iran and Syria." *The Guardian*, November 8, 2010. ProQuest.
- Magen, Dan. *Operation Orchard: Israel's Strike On The Syrian Reactor*, 2016.
- Makovsky, David. "The Silent Strike." *The New Yorker*, September 10, 2012. <https://www.newyorker.com/magazine/2012/09/17/the-silent-strike>.
- Marshall, Michael. "Timeline: Weapons Technology." *New Scientist*, July 7, 2009. <https://www.newscientist.com/article/dn17423-timeline-weapons-technology/>.
- McConnell, Tristan. "Interview with a Pirate." *GlobalPost*, June 12, 2009. <https://theworld.org/stories/2009-06-12/interview-pirate>.
- McMillan, Robert. "Siemens: Stuxnet Worm Hit Industrial Systems." *Computerworld*, September 14, 2010. <https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html>.
- McRaven, William Harry. *Spec Ops: Case Studies in Special Operations Warfare : Theory and Practice*. Novato (CA): Presidio, 1996.
- Melman, Yossi. "Outgoing Mossad Chief: Iran Won't Have Nuclear Capability before 2015." *Haaretz*, January 7, 2011. <https://www.haaretz.com/2011-01-07/ty-article/outgoing-mossad-chief-iran-wont-have-nuclear-capability-before-2015/0000017f-e993-dea7-adff-f9fba1f80000>.
- Melman, Yossi. "Outside The Box: Israel's Strike on Syria's Nuclear Plant." *The Jerusalem Post*, April 6, 2018. <https://www.jpost.com/arab-israeli-conflict/outside-the-box-israels-strike-on-syrias-nuclear-plant-547870>.
- Merriam-Webster*, s.v. "system." Accessed May 12, 2023. <https://www.merriam-webster.com/dictionary/system>.
- Morris, Nigel, and Andrew Buncombe. "Libya Gives up Nuclear and Chemical Weapons." *The Independent*, December 20, 2003. <https://www.independent.co.uk/news/world/politics/libya-gives-up-nuclear-and-chemical-weapons-83350.html>.
- Nakashima, Ellen, and Joby Warrick. "Officials Say U.S., Israel Were behind Cyberattack on Iran." *The Washington Post*, June 2, 2012. ProQuest.

- NATO. "Counter-Piracy Operations (2008-2016)." Accessed April 10, 2023. [https://www.nato.int/cps/en/natohq/topics\\_48815.htm](https://www.nato.int/cps/en/natohq/topics_48815.htm).
- NATO. "NATO Concludes Successful Counter-Piracy Mission." December 15, 2016. [http://www.nato.int/cps/en/natohq/news\\_139420.htm](http://www.nato.int/cps/en/natohq/news_139420.htm).
- NATO. "Operation Ocean Shield." Accessed April 10, 2023. <https://mc.nato.int/missions/operation-ocean-shield.aspx>.
- Naylor, Hugh. "Syria Tells Journalists Israeli Raid Did Not Occur." *New York Times*, October 11, 2007. <https://www.nytimes.com/2007/10/11/world/middleeast/11syria.html?ref=world>.
- Nevo, Saggi, and Michael R. Wade. "The Formation and Value of IT-Enabled Resources: Antecedents and Consequences of Synergistic Relationships." *MIS Quarterly* 34, no. 1 (March 2010): 163–83. <https://doi.org/10.2307/20721419>.
- Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. JP 1. Washington, D.C.: Joint Chiefs of Staff Washington, 2010. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/Reference-Series/>.
- Office of the Press Secretary. "President Delivers State of the Union Address." The White House, January 29, 2002. <https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html>.
- O'Hanlon, Michael E. *Forecasting Change in Military Technology, 2020–2040*. Washington, DC: Brookings Institution Press, 2018. [https://www.brookings.edu/wp-content/uploads/2018/09/FP\\_20181218\\_defense\\_advances\\_pt2.pdf](https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf).
- O'Hara, Vincent P, and Enrico Cernuschi. "Frogmen against a Fleet: The Italian Attack on Alexandria 18/19 December 1941." *Naval War College Review* 68, no. 3 (2015): 119–37. <https://digital-commons.usnwc.edu/nwc-review/vol68/iss3/8>.
- Oleg, Kupreev, and Ulasen Sergey. "Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.Gen.2 Review." VirusBlokAda, July 2010. [https://archive.f-secure.com/weblog/archives/new\\_rootkit\\_en.pdf](https://archive.f-secure.com/weblog/archives/new_rootkit_en.pdf).
- Peters, Sara. "Stuxnet 'Patient Zero' Attack Targets Revealed." *Dark Reading*, November 11, 2014, sec. attacks-breaches. <https://www.darkreading.com/attacks-breaches/stuxnet-patient-zero-attack-targets-revealed>.
- Plaut, Martin. "Tsunami: Somalia's Slow Recovery." *BBC*, December 26, 2005. <http://news.bbc.co.uk/2/hi/africa/4560246.stm>.

- Porter, Gareth. "When the Ayatollah Said No to Nukes." *Foreign Policy*, October 16, 2014. <https://foreignpolicy.com/2014/10/16/when-the-ayatollah-said-no-to-nukes/>.
- Riedel, Bruce. "Lessons of the Syrian Reactor." *The National Interest*, no. 125 (June 2013): 39–46. <http://www.jstor.org/stable/42896512>.
- Rogers, Everett M. *Diffusion of Innovations*. 4th ed. New York: Free Press, 1995.
- Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012.
- Sanger, David E. "Obama Order Sped Up Wave Of Cyberattacks Against Iran." *New York Times*, June 1, 2012. ProQuest.
- Searle, Tom. *Outside the Box: A New General Theory of Special Operations*. JSOU Report 17–4. MacDill AFB, FL: Joint Special Operations University, 2017.
- Shachtman, Noah. "Exclusive Interview: Pirate on When to Negotiate, Kill Hostages." *Wired*, July 28, 2009.
- Sherwell, Philip. "Israel Launches Covert War against Iran." *The Daily Telegraph*, February 16, 2009. ProQuest.
- Spulak, Robert G. *A Theory of Special Operations: The Origin, Qualities, and Use of SOF*. JSOU Report 07–7. Hurlburt Field, FL: Joint Special Operations University, 2007. <https://apps.dtic.mil/sti/pdfs/ADA495521.pdf>.
- StartUs Insights. "Top 10 Military Technology Trends for 2023," November 5, 2021. <https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/>.
- Szoldra, Paul. "A New Film Gives a Frightening Look at How the U.S. Used Cyberwarfare to Destroy Nukes." *Business Insider*, July 7, 2016. <https://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016-7>.
- Traynor, Ian, and Julian Borger. "Iran Admits Secret Uranium Enrichment Plant." *The Guardian*, September 25, 2009. <https://www.theguardian.com/world/2009/sep/25/iran-admits-uranium-plant>.
- Trevithick, Joseph. "Israel Details Long Secret Raid On Syrian Nuclear Reactor, Says It's Willing To Do It Again." *The Drive*, June 30, 2019. <https://www.thedrive.com/the-war-zone/19492/israel-details-long-secret-raid-on-syrian-nuclear-reactor-says-its-willing-to-do-it-again>.

- Tugwell, Maurice, and David Charters. "Special Operations and the Threats to United States Interests in the 1980s." In *Special Operations in U.S. Strategy*, 28–43. National Defense University Press, 1984.
- United Nations Security Council. "Resolutions Adopted by the Security Council in 2008." Accessed April 10, 2023. <https://www.un.org/securitycouncil/content/resolutions-adopted-security-council-2008>.
- United Nations Security Council (UNSC). Resolution 1851, S/RES/1851 (2008).
- U.S. Virtual Embassy Iran. "Policy & History." U.S. Virtual Embassy Iran. Accessed April 6, 2023. <https://ir.usembassy.gov/our-relationship/policy-history/>.
- USSOCOM. "SOF Truths." Accessed April 6, 2023. <https://www.socom.mil/about/sof-truths>.
- Wagenseil, Paul. "Obama, Bush Behind Stuxnet Worm, Report Says." *NBC News*, June 1, 2012. <https://www.nbcnews.com/id/wbna47647550>.
- Wanjohi Kabukuru. "Somali Piracy: In Search of Remedies for a Global Malady." *Africa Renewal*, January 17, 2012. <https://www.un.org/africarenewal/web-features/somali-piracy-search-remedies-global-malady>.
- Warrick, Joby. "U.S. Displays Nuclear Parts Given by Libya; Abraham Calls Haul A 'Big, Big Victory.'" *The Washington Post*, March 16, 2004. ProQuest.
- Warrick, Joby. "U.S. Is Said to Expand Covert Operations in Iran; Plan Allows Up to \$400 Million for Activities Aimed at Destabilizing Government." *The Washington Post*, June 30, 2008. ProQuest.
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.

## INITIAL DISTRIBUTION LIST

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



## DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

[WWW.NPS.EDU](http://WWW.NPS.EDU)

---

WHERE SCIENCE MEETS THE ART OF WARFARE