Maritime Sabotage: Lessons Learned and Implications for Strategic Competition

Alexander Powell, Elizabeth Yang, Annaleah Westerhaug, and Kaia Haney

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
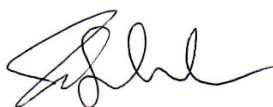
DRM-2021-U-030772-Final

Abstract

Warring sides have undertaken sabotage operations throughout history to generate battlefield effects, with varying degrees of success. In many cases, the forces conducting these operations have been special operations forces, their predecessors, or intelligence agencies. CNA initiated a quick-look study to examine past instances of sabotage in order to derive lessons and best practices for the future conduct of such operations. To increase the utility of the study for US Navy and US Marine Corps organizations, and because of the dearth of prior research on the topic, we focused our efforts on examining sabotage in the maritime domain. We generated a dataset of maritime sabotage instances dating back to World War II and analyzed this dataset according to a set of coding variables. These coding variables allowed us to perform both descriptive analysis of the dataset, as well as exploratory analysis.

Approved by: **October 2021**

Jonathan Schroden, Research Program Director
Countering Threats and Challenges Program
CNA Strategy, Policy, Plans, and Programs Division

Request additional copies of this document through inquiries@cna.org.

Executive Summary

Warring sides have undertaken sabotage operations throughout history to generate battlefield effects, with varying degrees of success. In many cases, the forces conducting these operations have been special operations forces (SOF), their predecessors, or intelligence agencies. During World War II, for example, the US Office of Strategic Services built a reputation for conducting sabotage across several theaters of operation and in multiple domains. However, over the past 20 years, SOF have focused heavily on counterterrorism and counterinsurgency operations, resulting in a current dearth of experience with sabotage against nation-state targets.

In light of SOF's history with sabotage and recent renewed interest in the subject, CNA initiated a quick-look study to examine past instances of sabotage in order to derive lessons and best practices for the future conduct of such operations. To increase the utility of the study for US Navy and US Marine Corps organizations, and because of the dearth of prior research on the topic, we focused our efforts on examining sabotage in the maritime domain. To conduct this study, we employed a five-step methodological process, as follows: (1) define key terms, (2) conduct a literature review of analytical works on sabotage, (3) build a maritime sabotage dataset, (4) code that dataset to derive analytic findings, and (5) distill implications for the future.

Upon review of existing US military doctrine and literature on sabotage, we were unable to find a common definition for this term. As such, we propose the following definition: sabotage is **a mission (conducted via individual act or as part of a campaign) to secretly disarm, obstruct, or destroy enemy war materiel or infrastructure for military advantage.** Using this definition and a thorough review of existing literature, we built a dataset consisting of 21 examples of maritime sabotage. We then coded these examples according to a set of variables that we identified as being of interest through our review of historical literature.

Using the results of the coding process, we conducted two sets of analyses. The first, which was descriptive in nature, explored trends in the conduct of maritime sabotage according to variables such as the type of military operation, the force conducting the sabotage act, and the overall success of an operation in achieving its desired objectives. Among the findings from this descriptive analysis are the following:

- World War II appears to have been a heyday for maritime sabotage; almost half of the identified instances in our dataset occurred during that conflict.
- More broadly, most instances of maritime sabotage occurred during periods of large-scale combat operations (LSCO) (Figure 1).

- In more than half of the maritime sabotage instances in our dataset, the force employed for sabotage was composed of SOF or SOF-like personnel.
- Of the instances examined, 85 percent were successful in achieving their desired tactical objective (Figure 1).

Figure 1.   Results of descriptive analysis of maritime sabotage dataset
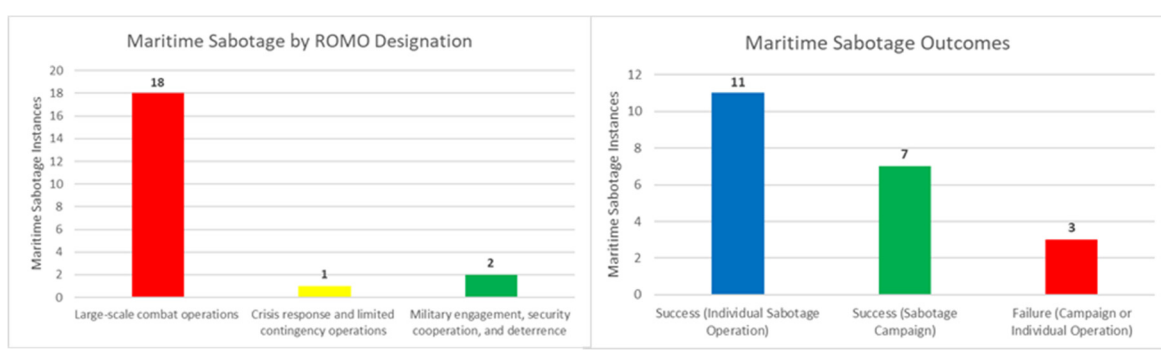
Source: CNA.

The second set of analyses, which was exploratory in nature, sought to identify and analyze cross-cutting themes present in our maritime sabotage dataset. To facilitate this analysis, we developed and tested four hypotheses focused on the interaction of coding variables. The hypotheses chosen, along with our findings related to those hypotheses, are as follows:

- **Hypothesis 1: Preplanned sabotage operations are more successful than spontaneous ones.**
  - *Finding: We were not able to make a determination on this hypothesis because of a lack of data.* Specifically, we found that the vast majority of the individual maritime sabotage cases we examined were not spontaneous but rather involved preplanning or rehearsal. We were not able to identify enough cases of spontaneous sabotage to make a meaningful comparison.
- **Hypothesis 2: Sabotage missions incurring third-party collateral damage have significantly negative political consequences.**
  - *Finding: The evidence gathered through analysis of our dataset suggests that this hypothesis may be true.* We identified two cases of maritime sabotage resulting in third-party collateral damage (the Central Intelligence Agency mining campaign in Nicaragua and the French sabotage of the *Rainbow Warrior* vessel). In both cases, the perpetrator of the maritime sabotage faced withering political backlash.

- **Hypothesis 3: Sabotage operations in which the element of surprise is lost are more likely to fail.**
  - *Finding: The results of our coding and analysis suggest that this hypothesis may be false.* Of the individual sabotage operations we examined in which the element of surprise was lost, approximately half still succeeded in achieving their desired tactical objective. Although this finding is not definitive, if this hypothesis were true, we would expect to see a greater fail rate associated with operations in which the sabotage force lost the element of surprise.
- **Hypothesis 4: Complex sabotage operations are more likely to fail.**
  - *Finding: The evidence collected through analysis of our maritime sabotage dataset suggests that this hypothesis may be true.* The sabotage operations that we considered to be the most complex tended to be associated with a greater rate of failure to achieve desired objectives or led to significant negative consequences (such as friendly casualties).

From this analysis, we identified a set of implications for both the Department of Defense (DOD) as well as the specific forces that may be directed to conduct maritime sabotage moving forward. We framed these implications in the context of questions DOD should seek to answer when thinking about the future of maritime sabotage in several areas:

- **Defining and describing sabotage**
  - How should DOD define sabotage in today's strategic environment?
  - What are the essential characteristics required for successful sabotage operations?
  - Should there be a distinct theory of sabotage akin to Admiral (Ret.) McRaven's theory of raiding?
- **Campaigning versus individual operations**
  - When might the United States benefit from a sustained campaign of sabotage operations?
  - When might the United States be better served by individual sabotage operations?
  - What are the benefits, drawbacks, and risks associated with each approach?
- **Maritime sabotage in competition below armed conflict (CBAC)**
  - What additional military or political benefits and risks might sabotage operations conducted in the CBAC or military engagement portions of the range of military operations (ROMO) entail?
  - For which portion(s) of the ROMO are sabotage operations most advantageous or least risky?

o What additional authorities might be needed to effectively conduct sabotage outside of LSCO? What should oversight and approval processes be for such operations?

o How do DOD leaders think about sabotage in the context of evolving concepts of deterrence and escalation? Specifically, if deterrence has an inherently overt characteristic, how does the secret nature of sabotage operations fit into this concept?

- **Multi-domain sabotage**

o How might DOD leverage maritime assets in support of sabotage in other domains or vice versa?

o What are the relative benefits, drawbacks, and risks of multi-domain sabotage operations as they relate to historical examples of complex sabotage?

o How should DOD leaders think about sabotage in the context of future warfighting concepts that span all domains?

o What additional authorities might be needed to conduct multi-domain sabotage operations? What should oversight and approval processes be for such operations?

This quick-look project examined an old concept (sabotage) in an attempt to distill new insights to inform future DOD decisions regarding sabotage and its potential use. In doing so, we sought to shed light on an underexplored aspect—sabotage conducted in the maritime domain. Our findings raise as many questions as they answer, and our analysis represents a jumping-off point and a way to energize DOD thinking on the benefits, drawbacks, and risks associated with maritime sabotage.

Contents

Introduction

Toward the end of the American Civil War, Thomas Courtenay of the Confederate Secret Service invented a new weapon meant to facilitate sabotage operations targeting Union steamships. The device consisted of an explosive charge hidden in a casing designed to look like a piece of coal (the explosive was covered in resinous pitch and rolled in coal dust). The idea was that Union steamship crews would unknowingly toss the disguised explosive into a vessel's furnace, triggering an explosion that would incapacitate the ship. Despite the inventiveness of the "coal torpedo," there is scant evidence of the weapon's success. Some historians have speculated that it led to the destruction of several vessels, including a ship serving as a floating headquarters for a Union general, although this has not been confirmed.[1] What appears certain, however, is that the negligible to modest results did not live up to the creator's vision at scale.

Warring sides have undertaken sabotage operations throughout history to secretly disarm, obstruct, or destroy enemy war materiel or infrastructure to generate battlefield effects, with varying degrees of success. In many cases, the forces conducting sabotage operations have been special operations forces (SOF), their predecessors, or intelligence agencies. For example, during World War II, the British Long-Range Desert Group (comprising what would become the Special Air Service (SAS)) pursued a campaign of sabotage operations targeting German airfields and other infrastructure.[2] Sabotage has not been limited to state actors, either. In some cases, the forces employing sabotage have been insurgent or terrorist groups. For example, the Liberation Tigers of Tamil Eelam (LTTE) employed frogmen divers to secretly place limpet mines on Sri Lankan Navy vessels.[3]

The United States has extensive experience conducting sabotage operations. During World War II, the US Office of Strategic Services (OSS) built a reputation for conducting sabotage across theaters of operation and in multiple domains. US Special Operations Command traces its lineage back to the OSS, demonstrating the historical significance of sabotage as a mission for the SOF community (although it is worth noting that the OSS was also the predecessor to

---

[1] Chris McNab, "Weapons Check: Coal Torpedo," *MHQ—The Quarterly Journal of Military History* 32, no. 3 (Spring 2020).

[2] See Ben Macintyre, *Rogue Heroes: The History of the SAS, Britain's Secret Special Forces Unit that Sabotaged the Nazis and Changed the Nature of War* (New York: Broadway Books, 2016).

[3] See Admiral J. Colombage, "Maritime Security and Theories of Naval Warfare: Way Ahead for a Professional Navy," in *Proceedings of 8th International Research Conference, KDU*, published Nov. 2015.

the Central Intelligence Agency (CIA), demonstrating the shared historical experience between SOF and intelligence agencies in this space). However, over the past 20 years, SOF have focused heavily on counterterrorism (CT) and counterinsurgency operations, resulting in a current dearth of experience with sabotage against nation-state targets.

In accordance with the directed shift in priorities from CT to strategic competition articulated in the 2018 National Defense Strategy, SOF have begun to shift their focus from mostly CT to a more balanced focus of CT and competition with peer and near-peer actors. Accompanying that shift has been a renewed interest in the potential utility of sabotage. In its fiscal year (FY) 2021 list of desired research areas, for example, the Joint Special Operations University (JSOU) listed *strategic sabotage* as a priority topic.[4] Yet, perhaps in part because of the lack of emphasis on this type of operation in the recent past, there remains some confusion in the Department of Defense (DOD) today about what exactly constitutes sabotage, much less strategic sabotage. Definitional challenges, discussed in greater detail below, may have heretofore hindered in-depth analysis of sabotage as a mission.

In light of SOF's history with sabotage and recent renewed interest in the subject, CNA initiated a quick-look study to examine past instances of sabotage in order to derive lessons learned and best practices for the future conduct of such operations. To increase the utility of the study for US Navy and US Marine Corps (USMC) organizations, and because of the dearth of prior research on the topic, we focused our efforts on examining sabotage in the maritime domain. Specific questions that we sought to address in this study included the following:

- What historical cases of maritime sabotage have been conducted and how are they relevant for strategic competition?
- How effective were maritime sabotage operations? Under what conditions were such operations successful or unsuccessful? How was success defined?
- How were maritime sabotage operations related to broader operations? Were they conducted as individual operations or as campaigns? Were there unforeseen consequences, and if so, what were they and what can we learn from them?
- What forms of maritime sabotage carry the greatest risk? Is there a taxonomy of conditions under which maritime sabotage is conducted, and associated risk, that could be useful for Navy and USMC SOF as they compete with state adversaries in the years to come?

---

[4] Joint Special Operations University, *Special Operations Research Topics 2020 Revised Edition for Academic Year 2021*, (Florida: JSOU Press, 2020), p. 1.

Methodology

To answer these questions, we used a five-part methodological approach consisting of the following steps:

1. **Define key terms.** Given the definitional challenges we encountered (discussed in more detail below), we elected to create our own definitions for the key terms of interest, specifically *sabotage* and *maritime sabotage*.

2. **Conduct a literature review.** Despite a relative dearth of literature on the subject, we identified and examined several works that critically examine the historical and contemporary use of sabotage. We focused on the definitions these works used, the case studies they selected, and the conclusions they reached to inform our own work (i.e., this step and step 1 were conducted iteratively).

3. **Build a dataset**. We originally intended to take a historical case study approach to this project, selecting three or four cases to examine in depth. However, we found that the data available were not well suited to that approach. We decided instead to build a representative dataset of instances of US and foreign maritime sabotage dating back to World War II.

4. **Code cases to derive findings.** We coded our dataset using a variety of variables organized into thematic categories to derive crosscutting findings that are relevant to US SOF as well as Navy and Marine Corps organizations. We used the coding process to conduct both descriptive and exploratory analysis.

5. **Identify implications for the future.** We leveraged the results of our analysis, as well as reviews of existing DOD operating concepts and discussions with Naval Special Warfare Command (NAVSPECWARCOM) and US Marine Corps Forces Special Operations Command (MARSOC), to identify implications of our analysis (e.g., lessons and best practices) for the future conduct of sabotage operations.

Organization

The rest of this report is organized according to the methodology outlined above. We begin by presenting the definitions we adopted for this analysis, explaining their origins and why we selected them. Next, we review key literature focused on sabotage to identify pertinent themes and implications for our study. We then present the dataset of maritime sabotage cases we identified, which provides basic background information for each instance. Next, we analyze our dataset using the set of coding variables we identified. We split this analysis into two sections. First, we conduct descriptive analysis of our sabotage dataset, which focuses on

presenting visual depictions of our data according to the coding variables. Second, we use our coded dataset to test a number of hypotheses related to the success and failure of maritime sabotage through exploratory analysis. We also highlight other relevant insights or findings from this analytic process. Finally, we discuss our findings in the context of implications and recommendations.

Caveats

Before proceeding, it is worth noting several caveats regarding our analysis. First, we limited our search to only unclassified instances of maritime sabotage. We did so mainly because we wanted to produce a document that would be distributable to the widest possible audience, given this study is (to our knowledge) the only analytic effort focused on the subject of maritime sabotage. In addition, because of the limited time and resources associated with a quick-look study, we decided it would be best to focus on unclassified instances of sabotage with an understanding that a comprehensive future study could include classified instances as well. As such, we acknowledge that our sabotage dataset is likely missing instances that remain classified.

Our second caveat relates to the balance of successful and failed sabotage acts in our dataset. While conducting background research for this project, we found it difficult to uncover failed acts of maritime sabotage. This finding is not surprising, given that successful instances are more likely to be documented and eventually made known whereas unsuccessful attempts are less so. Therefore, we acknowledge that our dataset may be skewed toward successful acts, which may affect the analytic conclusions we reached.

One final caveat surrounding our sabotage dataset involves the provenance of sabotage acts. Most of the maritime sabotage instances we were able to uncover were conducted by Western nations (specifically the United States and European powers). We do not mean to imply that only Western nations have undertaken sabotage. However, we lacked access to historical accounts written in foreign languages (such as Russian and Chinese) that may have allowed us to better diversify our dataset. As such, we had to rely on English-language publications, which tend to focus on Western military history.

Defining Maritime Sabotage

The term *sabotage* is not defined in the most current version of the DOD *Dictionary of Military and Associated Terms*, which discusses the term only in the context of preventing acts of sabotage through means such as counterintelligence.[5] Interestingly, however, the term has not always been excluded. As recently as 2016, *sabotage* was defined by DOD as "an act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources."[6] It is not clear why DOD removed *sabotage* from its dictionary, although the Joint Staff periodically adds and removes terms from this document. More broadly, sabotage as a defined concept has appeared sporadically in other publications as well, including a US Army publication dating to the 1960s.[7]

Given the ambiguous nature of sabotage as a formally defined concept within DOD, we created our own definition based on our research. We decided not to use the 2016 DOD definition for two reasons. First, that definition makes no mention of secrecy, which our research indicated is a key element of sabotage. Second, the 2016 definition appears to include the killing of select enemy personnel as acts of sabotage. Although we acknowledge that sabotage often results in enemy deaths, we distinguish it from acts such as targeted killings.

We define *sabotage* as **a mission (conducted via individual act or as part of a campaign) to secretly disarm, obstruct, or destroy enemy war materiel or infrastructure for military advantage**. This definition includes several important details. First, sabotage is defined as a mission, not a tactic. Similar to a CT mission, sabotage can involve a range of different tactics, but the term *sabotage* refers to the purpose of a given act. Second, our definition requires an intent of secrecy on the part of the saboteur.[8] That is, the perpetrator

---

[5] US Department of Defense, *Dictionary of Military and Associated Terms*, updated Jan. 2021.

[6] US Department of Defense, *Joint Publication 1-02: Dictionary of Military and Associated Terms*, Nov. 8, 2010 (as amended through Feb. 15, 2016), p. 209.

[7] Headquarters, Department of the Army, *US Department of the Army Pamphlet 550-104: Human Factors Considerations of Undergrounds in Insurgencies*, Sep. 1966.

[8] We use the term *secret* here purposefully to distinguish our definition from those using *covert* and *clandestine*. We explain this issue in greater detail in the literature review section.

must intend to leverage secrecy in the execution of the act.[9] This element was missing from the DOD definitions we found and was a common component of other definitions found in our literature review, as discussed in the next section. Third, our definition excludes acts of terrorism, such as the suicide attack by members of al-Qaeda targeting the USS *Cole* in 2000.

Finally, to maximize utility for US Navy and US Marine Corps organizations, this project focuses exclusively on *maritime sabotage*, by which we mean sabotage acts that occur in blue water and the littorals (both surface and subsurface), target ports and port infrastructure, or are conducted on land but require access from the sea.

---

[9] There are two ways to incorporate the notion of secrecy: (1) secrecy in the intent of a sabotage operation, and (2) maintaining secrecy throughout the course of a sabotage operation. Our definition hews to the first option. Our definition would thus include an act of sabotage in which the force was discovered during the execution phase. In other words, the loss of secrecy does not disqualify an act from being considered as sabotage.

Literature Review

After settling on definitions for the terms in question, our next step was to survey available literature on sabotage. In general, we found few studies that met our qualifications. We did not seek to examine every piece of literature that discussed any act of sabotage conducted throughout history. Rather, we sought to focus on those works that critically examined sabotage as a military concept, exploring its utility and potential pitfalls through an analytic methodology such as historical case study analysis. Although there are many books and articles devoted to describing historical instances of sabotage (which we used to populate our maritime sabotage dataset), there has been less emphasis on studying sabotage itself as a military mission. Furthermore, we were not able to find a single study that examined sabotage in the maritime domain specifically.

The relevant literature we were able to find is quite recent, indicative of DOD's shift to strategic competition with nation-states and renewed interest in sabotage missions. It is also comprised almost entirely of theses completed by active duty military members, some in response to the FY 2021 JSOU research topics list mentioned above. We collected these studies and summarized them according to a number of variables, including scope, methodology, and findings. We then examined them for common themes, including areas of agreement and contention.

Rather than individually summarizing each study, we elected to synthesize the studies into a number of themes noted below. The following studies were examined as part of this literature review:[10]

- Howard L. Douthit III, "The Use and Effectiveness of Sabotage as a Means of Unconventional Warfare - An Historical Perspective from World War I through Viet Nam," Master's thesis presented to the Air Force Institute of Technology, September 1987

---

[10] We chose to exclude several operational works on sabotage completed during World War II, including the OSS *Simple Sabotage Field Manual* and select documents from the British Special Operations Executive (SOE). These field manuals provide detailed instructions on the process of conducting sabotage and are effectively "how-to" guides. However, they do not critically examine sabotage as a concept or military mission. As such, they provide useful background information but do not represent the literature we sought. See Office of Strategic Services, *Simple Sabotage Field Manual*, Strategic Services Field Manual No. 3, Jan. 17, 1944; *How to be a Spy: The World War II SOE Training Manual* (Toronto: The Dundurn Group, 2001).

- Andrew Gaab, "Strategic Sabotage: Historical Analysis meets Future Application," Master's thesis presented to the National Defense University, 2020
- Jarod Hahn, "Strategic Sabotage: Historical Lessons and Future Potential," Master's thesis presented to the National Defense University, 2020
- Daniel Meegan, "Breaking Other People's Toys: Sabotage in a Multipolar World," Master's thesis presented to the Naval Postgraduate School, December 2020
- Daniel Miller, "On Strategic Sabotage," Master's thesis presented to the National Defense University, 2020

The value of concealment

The studies we examined all use slightly different definitions for *sabotage* and *strategic sabotage*. This lack of consensus likely stems from the lack of current official DOD definitions for these terms. However, one common feature of these studies is the inclusion of secrecy as a critical component of sabotage. Even when the authors do not explicitly include secrecy in their definitions, the secret nature of sabotage is highlighted throughout their works. For example, authors Gaab, Miller, and Hahn all note that maintaining secrecy is a key element of successful sabotage,[11] which is interesting, especially in light of the fact that previous DOD definitions did not mention secrecy as a necessary aspect of sabotage.

The descriptions of sabotage in the literature differed in how the authors explained the concept of secrecy and the terms ascribed to it. Authors Miller, Meegan, and Gaab invoked the term *covert*, whereas Douthit and Hahn used *clandestine* when discussing sabotage operations. However, these terms are distinct and are associated with specific conditions regarding attribution. A *covert operation* is one conducted in such a way as to conceal the party responsible for the operation or at least create plausible deniability.[12] A *clandestine operation*, on the other hand, is one in which the effects of the operation itself are concealed in addition to the responsible party.[13] Even so, all of the studies we examined appeared to agree that, at the very least, an ideal sabotage operation should conceal the identity of the responsible party.

---

[11] Andrew Gaab, "Strategic Sabotage: Historical Analysis Meets Future Application," (Master's thesis, National Defense University, 2020); Daniel Miller, "On Strategic Sabotage," (Master's thesis, National Defense University, 2020); Jarod Hahn, "Strategic Sabotage: Historical Lessons and Future Potential," (Master's thesis, National Defense University, 2020).

[12] US Department of Defense, *Dictionary of Military and Associated Terms*, updated Jan. 2021, p. 53.

[13] US Department of Defense, *Dictionary of Military and Associated Terms*, p. 35.

As explained above, we agree that secrecy is a key component of sabotage, although in our definition we prefer not to restrict the term only to cases of obscured identity.

Consensus on utility of sabotage

Every study we examined as part of the body of literature finds sabotage to be a potentially useful tool, pointing to different aspects of the concept as evidence. Meegan, for instance, points to the benefits of sabotage as an economy of force operation, requiring little in the way of personnel.[14] Sabotage operations thus have the potential to achieve effects without the dedication of large amounts of resources. Douthit, through his case study analysis, concludes that historically there is no effective countermeasure to sabotage.[15] Even the most useful countersabotage method employed (physically hunting down saboteurs) often resulted in the enemy foregoing other parts of its defense, a situation saboteurs could use to their advantage to launch other operations.

Even so, some of the studies we examined offer caveats to this finding. Gaab, for instance, highlights the importance of balancing achieving effects with maintaining some level of secrecy. He argues that planners must weigh the short-term impact of a sabotage act against the potential long-term effects of the responsible party being discovered.[16] Hahn, meanwhile, argues that sabotage has led to some tactical successes in the past but has had little impact at the strategic level, despite the objectives of the perpetrators.[17] This lack of strategic impact could serve as an appetite suppressant for those expecting to achieve strategic results in the future. Although Miller finds that sabotage can serve as a low-cost, high-return tactic, he also highlights that sabotage acts can develop in unpredictable ways.[18] Once an act is carried out, it is impossible to "undo," and the perpetrator may be unable to contain spillover effects.

---

[14] Daniel Meegan, "Breaking Other People's Toys: Sabotage in a Multipolar World," (Master's thesis, Naval Postgraduate School, 2020), pp. 86–89.

[15] Howard L. Douthit III, "The Use and Effectiveness of Sabotage as a Means of Unconventional Warfare - An Historical Perspective from World War I through Viet Nam," (Master's thesis, Air Force Institute of Technology, 1987), p. 109.

[16] Gaab, "Strategic Sabotage: Historical Analysis Meets Future Application," p. 57.

[17] Hahn, "Strategic Sabotage: Historical Lessons and Future Potential," pp. 50–51.

[18] Miller, "On Strategic Sabotage," p. 59.

Primacy of historical case study analysis

All of the studies we examined use historical case studies to inform their understanding of the use of sabotage and generate findings on its utility. Rather than building a dataset for quantitative analysis, they relied on in-depth examinations of individual sabotage acts and campaigns to generate qualitative analytic insights. From a methodology standpoint, there is little variation across the studies. This similarity in approach leads to potential gaps in understanding and provides an opportunity to take another approach to analyzing historical acts of sabotage.

Furthermore, although the studies generally examined a wide variety of sabotage acts, three trends are notable, all of which have consequences for the present study. First, the literature focuses on sabotage in the land domain. This focus makes sense; it is likely easier to carry out sabotage on land (because there are fewer environmental variables), so there may be more historical examples to choose from. However, the lack of exploration of maritime sabotage is noteworthy and is in some ways the genesis of this report. Second, many of the sabotage cases examined in the literature occurred during World War II. It appears as though sabotage in other contexts has not been studied as closely. Third, the studies tend to rely on a few well-known instances of sabotage. These include the World War II Allied sabotage of the German heavy water facility at Vemok, Norway; the World War I German sabotage of Black Tom Island in New York; and the actions of British forces (both the Special Operations Executive (SOE) and the SAS) against the Axis powers during World War II in multiple theaters. To expand the literature on this important topic, we focused this study on sabotage in the maritime domain and employed a different analytic methodology.

Sabotage as an understudied area

The final theme we identified from existing analytic reports centers on the notion of sabotage as an understudied area, which is not surprising given the dearth of literature on the topic and the fact that DOD entities such as JSOU have expressed an interest in more analysis on the subject. However, it is worth noting that all of the studies we examined echo this theme. Furthermore, most offer specific areas ripe for additional examination. Meegan, for example, suggests examining the potential for sabotage against transportation assets in the maritime

domain.[19] Meanwhile, both Douthit and Hahn recommend studying sabotage operations conducted in the cyber domain.[20]

---

[19] Meegan, "Breaking Other People's Toys," pp. 93–97.

[20] Hahn, "Strategic Sabotage: Historical Lessons and Future Potential," pp. 54; and Douthit III, "The Use and Effectiveness of Sabotage as a Means of Unconventional Warfare," p. 111.

Maritime Sabotage Dataset

Upon completing our literature review of previous efforts to analyze instances of sabotage, we created a dataset of maritime sabotage acts to foster our own analysis of the topic. We leveraged a diverse set of resources in compiling this dataset. They include the documents examined as part of the literature review, scholarly accounts of military campaigns, and discussions with both internal and external subject matter experts. As stated in the methodology section, we adopted a dataset approach because of our inability to identify enough detailed information about instances of maritime sabotage to produce in-depth case studies. Therefore, rather than recount each sabotage instance we collected in prose, we present an overview of our maritime sabotage dataset in Table 1 on the next page.

Table 1.   Maritime sabotage dataset

Year	Description	Perpetrator	Method	Tactical Target	Location	Target Country	Conflict
1941	Italian attack on Alexandria	Italian navy	Submarines, torpedos	Royal Navy vessels	Alexandria, Egypt	UK	WWII
1942	SOE sabotage campaign	UK SOE	Timed bombs, commandos, etc.	Port of St. Nazaire, SF *Hydro*, others	St. Nazaire, France; Norway	Germany	WWII
1942	German attempts at sabotaging US homeland	Germany	Landing saboteurs via sub	US industry	New York, Florida	US	WWII
1942	SBS Mediterranean sabotage campaign	UK SBS	Sub/raft infil, satchel charges	Aircraft/airfields	Crete, Rhodes, elsewhere	Axis powers	WWII
1942	Operation Frankton	UK Royal Marines	Kayaks launched from subs, limpet mines	German vessels at Bordeaux	Bordeaux	Occupied France	WWII
1943	Operation Jaywick	Z Special Unit (UK and Australia)	Canoes, limpet mines	Japanese shipping in Singapore Harbor	Singapore Harbor	Japan	WWII
1944	Operations Ginny I and II	OSS/US Navy	Explosives	Railway communication tunnels	Framura, central Italy	Italy (German occupied)	WWII
1944	Skorzeny's attack on the Waal River (part of broader sabotage campaign)	German Special Forces	Frogmen, underwater demolition	US forces	Bridges over the Waal River near Nijmegan, Netherlands	Allied powers	WWII
1944	OSS Maritime Unit Southeast Asia UW campaign	US OSS Maritime Unit/UK forces	Sub infiltration	Axis forces in Southeast Asia	Burma and throughout Southeast Asia	Axis powers	WWII

Year	Description	Perpetrator	Method	Tactical Target	Location	Target Country	Conflict
1945	USS *Barb* sabotage against Japan	US Navy	Sub-launched saboteurs armed with bombs	Train on a vital railway line	East coast of Japan (now Russia)	Japan	WWII
1950	SOG/UDT campaign in coastal Korea	US Navy UDTs/UK/UN	Frogmen, explosives	Railways, bridges, port facilities	Coastal Korea, Pusan coast	North Korea	Korean War
1951	Spontaneous cutting of Chinese cable	US Air Force member	Individual destruction via axe	Chinese telecomm cable	Island in Yellow Sea	China	Korean War
1954	Viet Minh mining waterways	Viet Minh	Blocking free navigation or mines	French forces	Tonkin area	Vietnam	French in Indochina
1964	Attack on USNS *Card* (part of broader sabotage campaign)	VC Special Ops	Combat swimmer, explosives	USNS *Card*	Saigon	US	Vietnam War
1970	Stop Our Ship (SOS) movement sabotage campaign	SOS personnel (some US civilians and military pax)	Deliberate engine damage, arson, oil spillage	US Navy aircraft carriers	At port/at sea	US	Vietnam War
1982	Attempted Argentine sabotage in Gibraltar	Argentine SOF	Frogmen, limpet mines	Royal Navy warship	Gibraltar	UK	Falklands War
1982	SAS sabotage against Argentine aircraft	UK SAS	Man-laid charges	Argentine aircraft	Pebble Island	Argentina	Falklands War
1984	CIA mining of Nicaraguan harbors	US CIA	Mining using speedboats	Nicaraguan harbors	Corinto, Puerto Sandino, El Bluff	Nicaragua	Iran-Contra
1985	French sabotage of the *Rainbow Warrior*	French SOF	Limpet mines	*Rainbow Warrior* ship	New Zealand	Nonstate actor (Greenpeace)	N/A

Year	Description	Perpetrator	Method	Tactical Target	Location	Target Country	Conflict
1989	SEAL sabotage during Operation Just Cause	US Navy SEALs	Combat swimmers, explosives	Manuel Noriega's personal transportation	Panama City	Panama	Invasion of Panama
1983–2009	LTTE sea unit sabotage campaign	LTTE Sea Tigers	Frogmen, limpet mines	Sri Lankan Navy vessels	Sri Lanka	Sri Lanka	Sri Lankan civil war

Source: CNA.

Note: N/A = not applicable; SBS = Special Boat Service; SOG = special operations group; UDT = underwater demolition team; VC = Viet Cong; UW = unconventional warfare.

Analyzing Maritime Sabotage

Coding variables

The coding variables we selected represent the units of analysis for this effort. We used them to derive relevant findings and implications from our maritime sabotage dataset.[21] We identified these variables through the process of building our dataset (by identifying characteristics during our research that we deemed important) as well as through internal discussions focused on how to elicit the best results from our analysis. The variables are organized according to four categories: context, planning, execution, and aftermath/consequences. These categories correspond to specific aspects of a sabotage operation. We present our coding variables in Table 2.

Table 2.   Sabotage coding variables

Context	Planning	Execution	Aftermath/Consequences
Year	Target type	Location	Desired effect achieved (Y/N)
Conflict	Desired effect	Tactics	Casualties
Nature of perpetrator (state/nonstate actor)	Individual act or campaign	Forces employed	Collateral damage or additional damage
Nature of target (state/nonstate actor)	Preplanned or spontaneous[22]	Notable equipment	Strategic effects[23]
Strategic environment (according to range of military operations)	Joint operation (Y/N)	Duration	Unintended consequences

---

[21] We relied on a large array of documents to provide the necessary background information to code the maritime sabotage instances. We created a separate section within our references section to list all of the documents we used for this portion of the analysis.

[22] By spontaneous sabotage operations, we mean operations that did not seem to have been planned far in advance or ones in which the details of the operation (the time, force employed, etc.) shifted just before execution. We contrast spontaneous sabotage with operations for which it appears there was planning or advance rehearsal. Admittedly, it was at times difficult to code this variable with the data we had available.

[23] We coded strategic-level effects as sabotage that targets an adversary's national-level defense infrastructure or is intended to influence national-level politics.

Context	Planning	Execution	Aftermath/Consequences
N/A	Combined operation (Y/N)	Use of explosives (Y/N)	N/A
N/A	Desired concealment	Problems encountered	N/A
N/A	N/A	Characterization of operation as a raid (Y/N)	N/A

Source: CNA. N/A = not applicable.

Descriptive analysis

After coding our sabotage dataset against the variables introduced above, we found that we could display the data in visually engaging ways to elucidate trends across variables. We introduce these depictions here. However, we emphasize that our dataset is limited so it is difficult to derive conclusive findings, especially given the lack of recent operations (or possibly the lack of available data on them).

Maritime sabotage over time

The first trend we sought to visualize was the distribution of maritime sabotage operations in our dataset over time. Figure 2 displays the results of this exploration in the form of a Gantt chart. The most noticeable aspect of this figure is the concentration of maritime sabotage instances from 1940 to 1950. World War II stands out for its multitude of maritime sabotage operations conducted by both Allied and Axis powers throughout the course of the conflict.

Another interesting aspect of these data is the relative dearth of publicly available information about maritime sabotage cases since 1990. With the exception of the LTTE maritime sabotage campaign, we were unable to identify any recent examples. A cursory examination of these data may lead some to conclude that maritime sabotage has diminished in importance over the years. However, we note that our dataset is likely incomplete owing to our reliance on open source information. We therefore caution against drawing sweeping conclusions about the use of sabotage over time from this visualization.

**Figure 2.   Maritime sabotage over time (Gantt chart)**
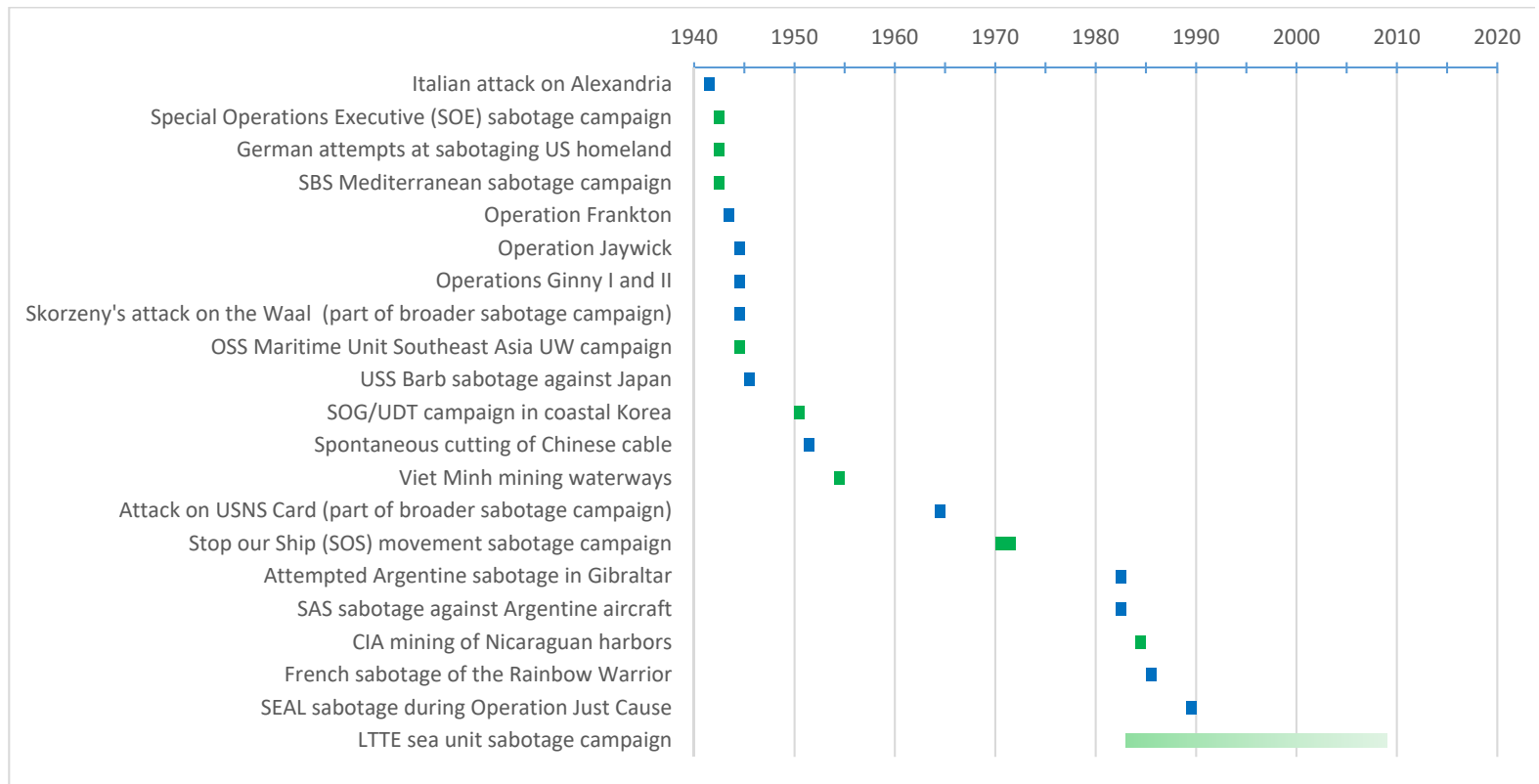
Source: CNA. Maritime sabotage campaigns are shaded in green, whereas isolated instances are shaded in blue. The LTTE sea unit campaign extends over several decades because that was the length of time of the formation's existence. It is not known whether maritime sabotage was conducted regularly throughout the entire period, hence the gradient in shading.

Maritime sabotage across the range of military operations

As alluded to above, one theme to emerge from the coding process was that the vast majority of maritime sabotage instances we examined occurred during what we would consider large-scale combat operations (LSCO) (Figure 3). This finding is to some extent unsurprising. World War II, for example, was the closest modern conflict to what would be characterized as "total war." In such periods of open armed conflict with seemingly existential consequences, one would expect military forces to undertake any operation they believe will increase their chances of gaining a military advantage—including sabotage.

On the other hand, during times of crisis response/limited contingency or military engagement/deterrence, acts of maritime sabotage may be considered overly provocative if the actor is discovered. We identified only three instances of maritime sabotage that occurred during these aspects of the range of military operations (ROMO): the CIA mining of Nicaraguan harbors, the French sabotage of the *Rainbow Warrior* vessel, and the US Navy SEAL sabotage of Panamanian leader Manuel Noriega's transportation. We note, however, that this analytic finding may be skewed because of available data. Acts of maritime sabotage conducted during LSCO may become known to the public more readily because of the difficulty of hiding military activity during open conflict, whereas operations conducted in other stages of the ROMO may be more likely to remain secret.

Figure 3.   Maritime sabotage operations according to the ROMO
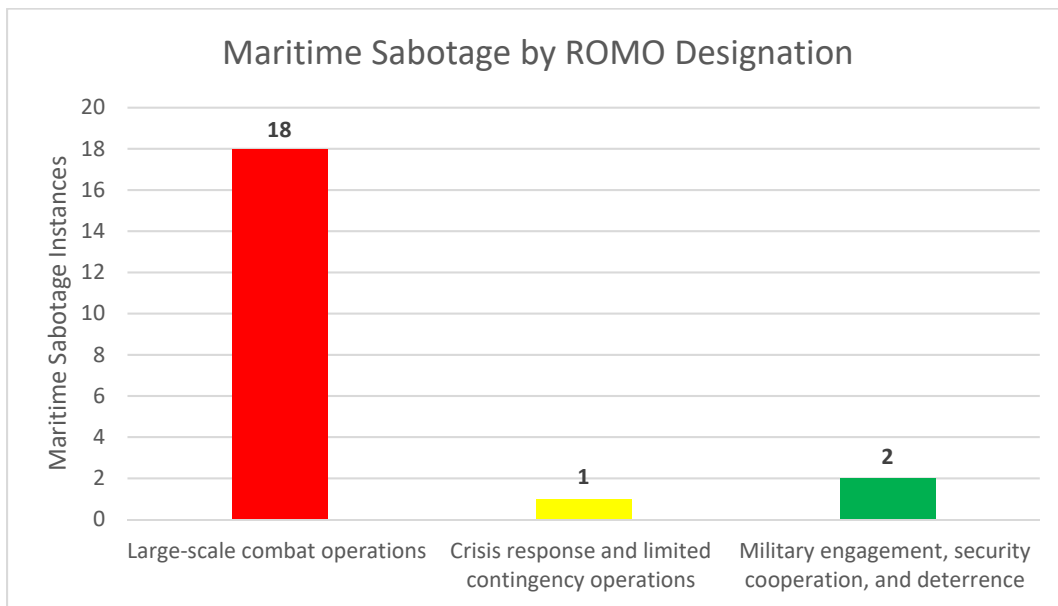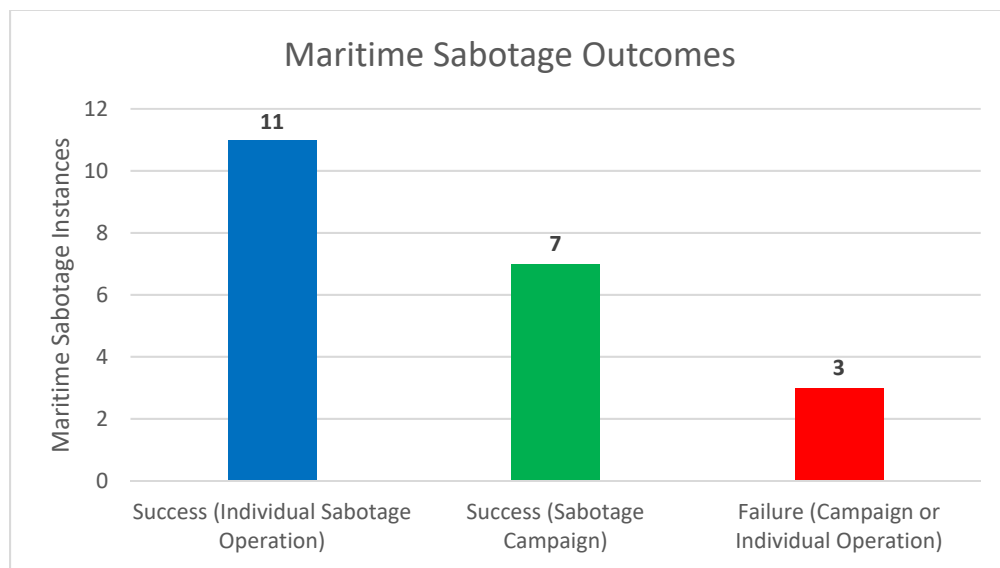

Source: CNA.

Success of maritime sabotage

Another dynamic we sought to explore was the success or failure of the maritime sabotage instances in our dataset. To examine this variable, we evaluated the tactical success of individual sabotage instances and the overall success of maritime sabotage campaigns.

We discovered that nearly all of the sabotage campaigns we examined were either successful or mostly successful in achieving their desired results. Although there may have been individual examples of failure within each campaign, most campaigns as a whole were successful. The only maritime sabotage campaign that decisively failed was the German attempt to infiltrate specially trained saboteurs into the United States during World War II. It is worth mentioning that the tactical objectives of each of the campaigns varied, with some being more ambitious than others. The failed German campaign, for example, was among the most ambitious, which could have contributed to its failure. We explore these dynamics more in the exploratory analysis section of the paper.

The trend for individual examples of maritime sabotage was similar. The vast majority of individual sabotage operations in our limited dataset were tactically successful in achieving their objectives. Only two failed: the disastrous Operations Ginny I and II carried out by OSS forces targeting railroad tunnels in Italy during World War II and the Argentine attempt to sabotage a British Royal Navy ship in Gibraltar during the Falklands War. Figure 4 presents the distribution of maritime sabotage instances according to success and failure.

**Figure 4.   Outcomes of maritime sabotage campaigns and individual operations**

Source: CNA.

Prevalence of SOF in conducting maritime sabotage

Another variable we examined during the coding process that merits further analysis was the nature of the forces employed to conduct maritime sabotage. We were interested in discerning whether any patterns existed regarding who has conducted maritime sabotage over the years. We framed this coding variable in the context of SOF or SOF-like versus non-SOF. By "SOF-like" we mean forces considered to be SOF predecessors (such as Navy underwater demolition teams), intelligence agencies (such as the OSS and the British SOE), or groups of personnel specially trained for the mission in question.

We found that in more than half of the maritime sabotage cases we examined, the forces that carried out the operation were what we would define as either SOF or SOF-like in nature (Figure 5). Given that the maritime sabotage operations we examined often involved the use of combat divers to emplace explosives or a small set of highly trained personnel to infiltrate a target on land, it makes sense that SOF were involved because these skill sets are typically associated with SOF versus conventional forces.

Figure 5. Forces executing maritime sabotage
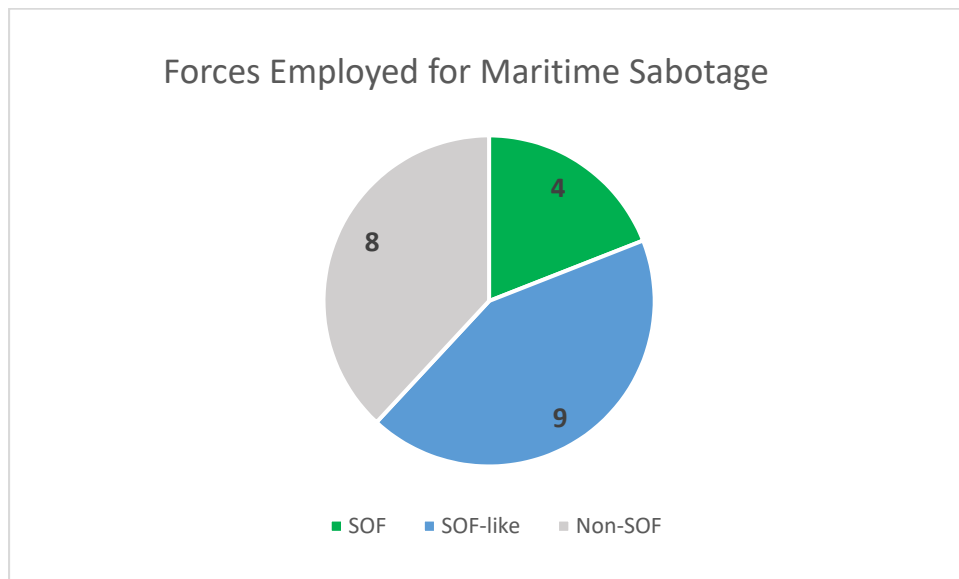
Source: CNA.

Exploratory analysis

In addition to the descriptive analysis presented above, the coding process allowed for more in-depth exploratory analysis of cross-cutting themes present in this limited maritime sabotage dataset. To facilitate this analysis, we identified several hypotheses regarding how our coding variables may be linked to one another. These hypotheses were derived from the background research we conducted as well as from internal project team discussions. In this section, we explore these hypotheses as well as other trends to emerge from the data.[24]

Hypothesis 1: Preplanned sabotage operations are more successful than spontaneous ones

The first hypothesis we sought to explore centered on the idea that preplanned or well-rehearsed maritime sabotage operations would be more successful in achieving their desired objectives than spontaneous operations. As noted in the coding variable section above, by spontaneous sabotage operations, we mean operations that did not seem to have been planned far in advance or ones in which the details of the operations (the time, force employed, etc.) shifted just before execution.

We were not able to make a determination on this hypothesis because of a lack of data. Specifically, we found that the vast majority of the individual maritime sabotage cases we examined were not spontaneous but rather involved preplanning or rehearsal. Furthermore, the only instance of spontaneous maritime sabotage we examined was successful (running counter to our hypothesis). In 1951, a member of the US Air Force stationed on an island overheard a Korean speaking about a Chinese sea cable. He then of his own accord severed the cable, depriving the Chinese of secure surface telephone communications and allowing the US military to eavesdrop. It may be tempting to conclude from analysis of this hypothesis that maritime sabotage is rarely conducted spontaneously. However, this conclusion may reflect only the data we could find. With access to classified examples of maritime sabotage, we may have been able to make a more definitive determination.

Although it stands to reason that preplanning or rehearsal would improve the chances of a sabotage operation being successful, we cannot rule out the possibility that emerging targets

---

[24] We note that our exploratory analysis is just that: exploratory. We do not pretend to have definitively proven causality in this project. Rather, we hope that this analysis can act as a stepping stone to further research in this area.

of opportunity for sabotage may arise wherein planning is not strictly necessary.[25] In particular, tactically simpler operations requiring less complicated equipment and methods, such as the cable cutting example noted above, may not need such planning. Maritime sabotage campaigns, on the other hand (which by their very nature we coded as preplanned), appear to be an effective way of thinking about sabotage in a holistic, long-term way. Nearly all the sabotage campaigns we examined were successful in achieving their desired results—and all of them appear to have been planned in advance. This finding would appear to support the notion that preplanned sabotage operations are more successful than spontaneous ones. However, it is not clear that the historical instances of failed sabotage campaigns were accurately represented in the data, underscoring the need for additional study. Furthermore, the dataset of individual maritime sabotage operations was also weighted toward successful examples, making it difficult to definitively state that campaigns are more likely to succeed than individual operations. Nonetheless, it is worth noting that, within our limited dataset, the vast majority of examples were both successful and involved advance planning.

Hypothesis 2: Sabotage missions incurring third-party collateral damage have significant negative political consequences

The second hypothesis we explored sought to link unintended damage resulting from a maritime sabotage operation with negative consequences for the perpetrator. Essentially, we were interested in examining whether collateral damage had political ramifications for the saboteur. The evidence as derived from our coding suggests that there may be a link between third-party collateral damage and negative political consequences. By third-party collateral damage, we mean casualties or significant damage to the personnel, infrastructure, or economic interests of an entity that is not the target of the sabotage operations.

The evidence gathered through the coding of our dataset suggests that this hypothesis may be true. We identified two cases of maritime sabotage resulting in third-party collateral damage. In both cases, the perpetrator of the maritime sabotage faced withering political backlash. In 1984, the CIA undertook a campaign to mine several harbors in Nicaragua in an effort to block access to those harbors. Discovery of the campaign, along with the CIA's role in it, led to significant backlash and political embarrassment. Chief among those leading the outcry were nations angry about not being able to access the Nicaraguan harbors. One year later, in 1985, the French sought to sabotage and sink the *Rainbow Warrior*, a vessel belonging to the nonprofit group Greenpeace. During the operation, at least one civilian (a New Zealand

---

[25] Tied to the notion of sabotage targets of opportunity is the matter of authorities. To conduct any operation, the military must either rely on existing authorities or request authorities. For an actor to take advantage of emerging sabotage opportunities in a timely manner, authorities may already need to be in place. However, standing authorities permitting sabotage may incur additional risk.

national) was killed. Discovery of the details of the operation and the role of the French caused a public relations disaster for France. In both instances, the sabotage operation unintentionally affected entities other than the intended target, and those entities then levied heavy criticism against the perpetrator. We acknowledge here that we rely on a small number of cases to make a judgment on this hypothesis, so we cannot be definitive. However, the two cases that are pertinent to this discussion involved strong political backlash, an outcome worth noting by any future practitioners of sabotage operations.

Incidentally, both sabotage operations referenced above occurred outside of LSCO, which may suggest a broader point about the political danger associated with conducting sabotage operations in various security environments. As noted above, the vast majority of maritime sabotage operations we were able to identify occurred during LSCO. Although this finding may be tied to the fact that incidents occurring during LSCO are more likely to become public, it may also be that conducting sabotage during LSCO is considered more "acceptable" than conducting sabotage during other portions of the ROMO. If true, this finding would lend credence to the idea that sabotage conducted outside of LSCO entails greater risk of blowback for the perpetrator if it goes awry.

Hypothesis 3: Sabotage operations in which the element of surprise is lost are more likely to fail

The third hypothesis we examined centered on the importance of maintaining the element of surprise. As a concept, surprise is related to, but distinct from, secrecy. Secrecy can help with garnering surprise, yet surprise may also be generated through other means, such as constant repetition.[26] Given the fact that sabotage operations are often undertaken by small (albeit specially trained) forces, we hypothesized that losing the element of surprise would make a sabotage operation more likely to fail.

Interestingly, the results of the coding process suggest that this hypothesis may be false. At least, we were not able to confirm the hypothesis as being true. Of the individual sabotage operations we examined in which the element of surprise was lost (excluding the campaigns, which may contain multiple examples of successful and failed acts), approximately half still succeeded in achieving their desired tactical objective. Although this finding is not definitive, if this hypothesis were true, we would expect to see a greater fail rate associated with operations in which the sabotage force lost the element of surprise. Instead, although sabotage forces were fairly routinely exposed during the conduct of their missions (because of, in Clausewitzian terms, the friction of war), many were still able to achieve their tactical objective.

---

[26] William H. McRaven, "The Theory of Special Operations," (Master's thesis, Naval Postgraduate School, 1993), pp. 11-12.

More broadly, analysis of this hypothesis in the context of our limited dataset suggests that maritime sabotage operations appear to be difficult to conceal, as exemplified by the high rate of force exposure noted above. If true, this dynamic may give pause to policy-makers wishing to employ maritime sabotage operations in sensitive environments. However, given the unclassified nature of our project, we acknowledge the possibility that our dataset is skewed toward instances in which the force was exposed. In other words, it is possible that many more maritime sabotage cases in which the sabotage force was not exposed (thus preserving the secrecy of the mission) exist at the classified level. Furthermore, the available data include a sizable fraction of examples from World War II. Tactics and training for conducting operations have evolved since then, so sabotage operations conducted today may be more readily concealable.

Hypothesis 4: Complex sabotage operations are more likely to fail

The fourth and final hypothesis we explored examined the link between the complexity of a maritime sabotage operation and the success or failure of that operation. By complexity, we mean a holistic examination of the sabotage force (whether the operation was joint or combined), the equipment employed, and the relative ease or difficulty of the mission itself.[27] For example, the sabotage conducted as part of the Stop Our Ship (SOS) movement would be considered *simple sabotage* because it involved individual personnel doing whatever they could to disable ships in a rudimentary way (by using arson or throwing wrenches into engines).[28] Conversely, the US Navy SEAL sabotage operation targeting Panamanian dictator Manuel Noriega, which involved sabotaging transportation assets in multiple locations so that they would be disabled but not destroyed, would be considered a complex operation.

The evidence collected through coding our maritime sabotage dataset suggests that this hypothesis may be true. The sabotage operations that we considered to be the most complex tended to be associated with a greater rate of failure to achieve desired objectives or led to significant negative consequences (such as friendly casualties). One such example is the German attempts to sabotage the United States during World War II. This plan involved

---

[27] We acknowledge that distinguishing between simple and complex sabotage involved a judgment call on the part of the project team and that complexity is perhaps better considered along a spectrum. However, when examining our dataset using our selected criteria, we found that we were able to delineate between simple and complex with relative ease.

[28] *Simple sabotage* refers to uncomplicated acts of sabotage that may be carried out without advanced planning by ordinary citizens. It can include arson and the use of rudimentary explosives. It also can include simple acts of passive resistance by people under enemy occupation, such as deliberately working inefficiently in an occupied factory. See Office of Strategic Services, *Simple Sabotage Field Manual*, Strategic Services Field Manual No. 3, Jan. 17, 1944.

German saboteurs landing by submarine at various points along the East Coast and carrying out sabotage targeting US lines of communication (LOCs) and industry. The operation failed almost immediately, with all of the saboteurs being captured because of their suspicious behavior.

Another example is Operations Ginny I and II. These operations, both of which failed, involved OSS forces attempting to secretly infiltrate Italy from the sea and blow up railway tunnels comprising enemy LOCs. In both attempts, the sabotage force landed at the wrong location and the mission failed. Even complex maritime sabotage operations that did achieve their stated objectives were sometimes plagued by negative consequences. For example, the Navy SEAL sabotage of Noriega's transportation resulted in the deaths of four SEALs and the wounding of eight others when Noriega's airplane was not in the location they originally thought.

Related to this finding is a broader observation about the desired objectives of maritime sabotage operations. All three of the maritime sabotage operations referenced above (two of which failed and one of which incurred heavy friendly casualties) involved attempts to secretly infiltrate a force by sea to conduct a sabotage mission on land. This type of operation is in contrast to sabotage operations involving destroying a target at sea using explosives, let alone examples of simple sabotage such as the SOS movement. In all three of the above examples, the sabotage force was exposed during the operation. We thus may be able to draw a line between complex sabotage operations requiring infiltration from the sea and operations involving destruction of a target at sea. We explore this dynamic further in the next section in our juxtaposition between maritime sabotage operations and maritime raids.

Other analytic insights

Comparing maritime sabotage and Admiral (Ret.) McRaven's principles of special operations

In his seminal work "The Theory of Special Operations," retired Admiral William McRaven introduced six principles for conducting special operations: simplicity, security, repetition, surprise, speed, and purpose.[29] Although the title of McRaven's thesis was focused on special operations as a whole, his description of them and the case studies he examined essentially equate to direct action raids. By contrast, our study focuses on sabotage as an operation distinct from tactics like raids or ambushes (as described in greater detail in our definitions section). Nevertheless, a cursory comparison of McRaven's principles against our coding variables reveals overlap, specifically in the areas of simplicity, repetition, and

---

[29] McRaven, "The Theory of Special Operations," p. 11.

security/surprise. We thus examined the results of our analysis in the context of whether or not they support McRaven's findings.

The degree to which our findings support McRaven's principles varies. In one instance, simplicity, we are in agreement with McRaven that tactically less complex operations appear more likely to succeed than complex ones. In another instance, surprise/security, we diverge, as our analysis suggests that surprise/security may actually be less important than McRaven hypothesized in his thesis. The third instance of variable overlap is difficult to fully parse. The degree to which repetition or preplanning of an operation contributes to mission success is not clear from our analysis. However, what does appear to be clear is that maritime sabotage campaigns (which de facto were preplanned) were generally successful tactically, highlighting the potential benefit to be gained through taking a campaign-style approach to conducting sabotage operations. Even so, it may also be true that some one-off maritime sabotage operations do not require exquisite repetition.

Differentiating "types" of maritime sabotage

Analysis of our maritime sabotage dataset enabled us to group maritime sabotage instances according to their desired objectives and the tactics employed when carrying them out. In this way, we were able to identify a taxonomy of conditions characterizing maritime sabotage operations. Although not all-encompassing, they are representative of the vast majority of maritime sabotage cases we identified. These types are the following:

- **Small team amphibious raids to destroy a maritime target using man-portable explosives.** Many of the examples we identified in this project fell into this category. Use of combat swimmers to attach explosives to vessels appears to be a common method for conducting maritime sabotage.

- **Sea-borne infiltration raids to destroy enemy LOCs on land.** Some of the more complex maritime sabotage operations we identified fell into this category, including attempts to destroy enemy railroad lines via infiltration of small sabotage teams.

- **Platform-based ordnance delivery to destroy a maritime target.** This category of operations includes those focused on delivery of effects via platforms instead of small teams of people. The Italian midget submarine attack on British forces at Alexandria is an example of this category of operations.

- **Miscellaneous individual-driven sabotage.** Finally, some operations we examined primarily centered on individual-driven sabotage, by which we mean operations whose success depended on individual effort rather than platforms or complicated equipment. This category includes simple sabotage efforts such as the SOS campaign involving throwing wrenches into engine bays.

Besides the general benefit gained by simplifying our dataset via these categories, this process underscored another important takeaway from this work. Although many sabotage operations involved the use of raids as a tactic, others did not, which further illustrates the fact that sabotage is a distinct type of operation that can involve multiple tactics in its execution.

Implications and Areas for Further Study

As we acknowledged in the preceding discussion, the limited amount of data available on maritime sabotage operations at the unclassified level precluded our ability to draw firm conclusions regarding our hypotheses or to state definitively what does or does not contribute to a successful act of maritime sabotage. Nonetheless, our initial examination of maritime sabotage and the insights gained through our analysis still have a number of interesting implications for both DOD in general and the specific forces that may be directed to conduct maritime sabotage in the future. We raise these implications here in the form of additional questions DOD should ask relative to the future of maritime sabotage.

- **Defining and describing sabotage.** As noted in the definitions section, there is no current official DOD definition for *sabotage*. Yet sabotage is an area of renewed interest for DOD. To address this issue, our analysis suggests that DOD may want to consider the following questions:
  - How should DOD define sabotage in today's strategic environment? Should it be the same as DOD's prior (2016) definition? Or should that definition be updated and if so, how?
  - What are the essential characteristics required for successful sabotage operations?
  - Should there be a distinct theory of sabotage akin to Admiral (Ret.) McRaven's theory of raiding?
- **Campaigning versus individual operations.** This work has introduced the concepts of maritime sabotage campaigns and individual, one-off operations. In thinking about the future role of sabotage, DOD should take note of these two approaches in the context of the potential strategic environment in which sabotage operations may be conducted. Some questions DOD may want to consider are the following:
  - When might the United States benefit from a sustained campaign of sabotage operations?
  - When might the United States be better served by individual sabotage operations?
  - What are the benefits, drawbacks, and risks associated with each approach?
- **Maritime sabotage in competition below armed conflict (CBAC).** The vast majority of maritime sabotage operations in our limited dataset occurred during LSCO. We

explored the potential reasons for this trend, as well as some caveats as to why our data might be skewed in this fashion. The United States is not currently in a state of LSCO but rather an environment of day-to-day competition. DOD should therefore consider what role sabotage may play in the CBAC or military engagement portion of the ROMO. Some specific questions to explore include the following:

- o What additional military or political benefits and risks might sabotage operations conducted in the CBAC or military engagement portions entail?
- o For which portion(s) of the ROMO are sabotage operations most advantageous or least risky? CBAC? During LSCO? Just before LSCO?
- o What additional authorities might be needed to effectively conduct sabotage outside of LSCO? What should oversight and approval processes be for such operations?
- o How do DOD leaders think about sabotage in the context of evolving concepts of deterrence and escalation? Specifically, if deterrence has an inherently overt characteristic, how does the secret nature of sabotage operations fit into this concept?

- **Multi-domain sabotage.** The past two decades have witnessed the introduction of two new domains into the DOD lexicon (cyber and space). Our dataset, being historical in nature, did not identify or examine any instances of cross domain sabotage involving the maritime domain and these new domains. However, in the future, one could imagine such multi-domain operations being possible—for example, using a sea-based platform to enable a sabotage operation in the cyber domain that generates no physical damage but disarms, obstructs, or destroys adversary cyber capabilities. The following related questions may merit study:

- o How might DOD leverage maritime assets in support of sabotage in other domains or vice versa?
- o What are the relative benefits, drawbacks, and risks of multi-domain sabotage operations as they relate to historical examples of complex sabotage?
- o How should DOD leaders think about sabotage in the context of future warfighting concepts that span all domains?
- o What additional authorities might be needed to conduct multi-domain sabotage operations? What should oversight and approval processes be for such operations?

Conclusion

This quick-look project examined an old concept (sabotage) in an attempt to distill new insights to inform future DOD decisions regarding sabotage and its potential use. In doing so, we sought to shed light on an underexplored aspect—sabotage conducted in the maritime domain. Additionally, we employed a methodological approach hitherto unused in previous analyses of sabotage—a dataset that enabled simple numerical analyses. Our findings raise as many questions as they answer and require additional study using a broader array of data sources. Our analysis represents a jumping-off point and a way to energize DOD thinking on the benefits, drawbacks, and risks associated with maritime sabotage.

Figures

Tables

Abbreviations

CIA	Central Intelligence Agency
CT	counterterrorism
CBAC	competition below armed conflict
DOD	Department of Defense
FY	fiscal year
JSOU	Joint Special Operations University
LOC	line of communication
LSCO	large-scale combat operations
LTTE	Liberation Tigers of Tamil Eelam
MARSOC	US Marine Corps Forces Special Operations Command
NAVSPECWARCOM	Naval Special Warfare Command
OSS	US Office of Strategic Services
ROMO	range of military operations
SAS	Special Air Service
SOE	Special Operations Executive
SOF	special operations forces
SOS	Stop Our Ship
USMC	US Marine Corps

References

Colombage, Admiral J. "Maritime Security and Theories of Naval Warfare: Way Ahead for a Professional Navy." In *Proceedings of 8th International Research Conference*, *KDU,* Nov. 2015.

Douthit III, Howard L. "The Use and Effectiveness of Sabotage as a Means of Unconventional Warfare - An Historical Perspective from World War I through Viet Nam." Master's thesis, Air Force Institute of Technology, 1987.

Gaab, Andrew. "Strategic Sabotage: Historical Analysis Meets Future Application." Master's thesis, National Defense University, 2020.

Hahn, Jarod. "Strategic Sabotage: Historical Lessons and Future Potential." Master's thesis, National Defense University, 2020.

Headquarters, Department of the Army. *US Department of the Army Pamphlet 550-104: Human Factors Considerations of Undergrounds in Insurgencies*. Sep. 1966.

How to be a Spy: The World War II SOE Training Manual. Toronto: The Dundurn Group, 2001.

Joint Special Operations University. *Special Operations Research Topics 2020 Revised Edition for Academic Year 2021*. Florida: JSOU Press, 2020.

Macintyre, Ben. *Rogue Heroes: The History of the SAS, Britain's Secret Special Forces Unit that Sabotaged the Nazis and Changed the Nature of War.* New York: Broadway Books, 2016.

McNab, Chris. "Weapons Check: Coal Torpedo." *MHQ—The Quarterly Journal of Military History* 32, no. 3 (Spring 2020).

McRaven, William H. "The Theory of Special Operations." Master's thesis, Naval Postgraduate School, 1993.

Meegan, Daniel. "Breaking Other People's Toys: Sabotage in a Multipolar World." Master's thesis, Naval Postgraduate School, 2020.

Miller, Daniel. "On Strategic Sabotage." Master's thesis, National Defense University, 2020.

Office of Strategic Services. *Simple Sabotage Field Manual*. Strategic Services Field Manual No. 3. Jan. 17, 1944.

US Department of Defense. *Dictionary of Military and Associated Terms*. Updated Jan. 2021.

US Department of Defense. *Joint Publication 1-02: Dictionary of Military and Associated Terms.* Nov. 8, 2010 (as amended through Feb. 15, 2016).

Maritime sabotage dataset references

"30 Years on, French Agent Apologises for Sinking Rainbow Warrior." *France 24 [Online].* June 9, 2015; Modified July 9, 2015. Accessed June 22, 2021. https://www.france24.com/en/20150906-france-rainbow-warrior-dgse-sinking-greenpeace.

Atlamazoglou, Stavros. "UK SOF in the Falklands War: The SAS Strike at Pebble Island." *SOFREP*. Sept. 19, 2019. Accessed June 22, 2021. https://sofrep.com/news/uk-sof-in-the-falklands-war-the-sas-strike-at-pebble-island-3/.

Babas, Latifa. "In 1942, a US Navy Top-Secret Mission Swam in the Sebou River to Cut a Steel Cable." Yabiladi.com. Sept. 30, 2020. Accessed June 25, 2021. https://en.yabiladi.com/articles/details/99649/1942-navy-top-secret-mission-swam.html.

Barford, Vanessa. "Remembering the Secret Mission of Cockleshell Heroes." *BBC News [Online]*. Mar. 31, 2011. Accessed June 25, 2021. https://www.bbc.com/news/uk-12914628.

Beevor, Antony. *Crete: The Battle and the Resistance*. New York: Penguin Books, 2014.

Briscoe, Charles H. "Jack Operations & Activities: Korea, 1951-1953." *Veritas* 9, no. 1, 2013. Accessed June 28, 2021. https://arsof-history.org/articles/v9n1_jack_operations_page_1.html.

Cassan, Dave. "Target Gibraltar: Operation Algeciras." *Falklands 30: Untold Stories of the War in the South Atlantic*. 2012. https://archive.org/details/Falklands/page/n2/mode/1up?view=theater.

Chandradasa, LT Malaka. "Learning from our Enemies: Sri Lankan Naval Special Warfare Against the Sea Tigers." *Combatting Terror Exchange* 2, no. 2 (2012): 4-8. ISSN 2162-6421 (online).

Cloninger, James M., Jr. "Analysis of Communist Vietnamese Special Operations Forces During the Vietnam War and the Lessons That Can Be Applied to Current and Future U.S. Military Operations." Master's thesis, Naval Postgraduate School, 2005. DTIC. https://apps.dtic.mil/sti/pdfs/ADA435487.pdf.

Colombage, J. "Maritime Security and Theories of Naval Warfare : Way Ahead for a Professional Navy."*Proceedings of 8th International Research Conference, KDU, General Sir John Kotelawala Defence University,* 2015, 100-107. KDU IRC. http://ir.kdu.ac.lk/handle/345/1248.

Coulombe, David P. "Learning on the Move, OSS Detachment 101 Special Operations in Burma." Master's thesis, United States Military Academy, West Point, 2015. Accessed June 25, 2021. https://apps.dtic.mil/sti/pdfs/AD1041757.pdf.

Davidson, J. Scott. "The Rainbow Warrior Arbitration Concerning the Treatment of the French Agents Mafart and Prieur." *The International and Comparative Law Quarterly* 40, no. 2 (Apr. 1991): 446-457. http://www.jstor.org/stable/759734.

Dimuro, Gina. "Operation Greif: When German Commandos Were Trained to Act American and Wreak Total Havoc Behind Enemy Lines." All That's Interesting. Mar. 11, 2019, Updated Mar. 15, 2019. Accessed June 25, 2021. https://allthatsinteresting.com/operation-greif.

Djokovic, Petar. "Krait and Operation JAYWICK." Royal Australian Navy. Accessed June 25, 2021. https://www.navy.gov.au/history/feature-histories/krait-and-operation-jaywick.

Dorfmann, Jessie. "You Can Never Sink a Rainbow: Anti-Nuclearism in the Pacific." *Harvard International Review* 37, no. 2 (2016): 4-7. https://www.proquest.com/scholarly-journals/you-can-never-sink-rainbow-anti-nuclearism/docview/1822077864/se-2?accountid=10186.

Dungigan, Molly, Dick Hoffman Hoffman, Peter Chalk, Brian Nichiporuk, and Paul Deluca. "Adversary Capabilities in Maritime Irregular Warfare." *Characterizing and Exploring the Implications of Maritime Irregular Warfare*, 69-86. Santa Monica, CA: RAND Corporation, 2012. JSTOR. http://www.jstor.org/stable/10.7249/mg1127navy.12.

Finlayson, Kenneth. "The OSS Maritime Unit on the Arakan Coast of Burma." *Veritas* 1, no. 2, 2005. Accessed June 25, 2021. https://arsof-history.org/articles/v1n2_oss_maritime_page_1.html.

Fluckey, Eugene B. *Thunder Below!: The USS *Barb* Revolutionizes Submarine Warfare in World War II.* USA: University of Illinois Press, 1992. ISBN: 9780252097447.

"German Espionage and Sabotage." Naval History and Heritage Command. Sept. 20, 2017. Accessed June 25, 2021. https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/g/german-espionage-and-sabotage.html.

Glass, Andrew. "Goldwater Condemns CIA Mining of Nicaraguan Harbors: April 10, 1984." *Politico [Online]*. Apr. 9, 2017. Accessed June 22, 2021. https://www.politico.com/story/2017/04/goldwater-condemns-cia-mining-of-nicaraguan-harbors-april-10-1984-237037.

Goldstein, Richard. "Eugene B. Flucky, Daring Submarine Skipper, Dies at 93." *New York Times*. July 1, 2007. https://www.nytimes.com/2007/07/01/obituaries/01cnd-fluckey.html?ex=1340942400&en=db46628c017e4fa5&ei=5088&partner=rssnyt&emc=rss.

Hersh, Seymour M. "Navy Acts to Halt Racial Violence and Alleged Sabotage on Ships." *New York Times*. Nov. 6, 1972. https://www.nytimes.com/1972/11/06/archives/navy-acts-to-halt-racial-violence-and-alleged-sabotage-on-ships.html.

Hiatt, Fred, and Joanne Omang. "CIA Helped to Mine Ports in Nicaragua." *The Washington Post*. Apr. 7, 1984. Accessed June 22, 2021. https://www.washingtonpost.com/archive/politics/1984/04/07/cia-helped-to-mine-ports-in-nicaragua/762f775f-6733-4dd4-b692-8f03c8a0aef8/.

Hollway, Don. "Bridge to Victory at Malmedy." *HistoryNet World War II [Online]*. Dec. 2018. Accessed June 25, 2021. https://www.historynet.com/bridge-victory-malmedy.htm.

———. "Operation Greif and Otto "Scarface" Skorzeny." Warfare History Network. Jan. 19, 2016. Accessed June 25, 2021. https://warfarehistorynetwork.com/2016/01/19/operation-greif-and-otto-scarface-skorzeny/.

Huard, Paul Richard. "Revealed: Viet Cong Commandos Sank Navy Aircraft Carrier." The National Interest. Feb. 13, 2018. https://nationalinterest.org/blog/the-buzz/revealed-viet-cong-commandos-sank-navy-aircraft-carrier-24483.

Jackson, Peter. "Falklands War: SAS Role in the Conflict." *BBC [Online]*. May 4, 2012. Accessed June 22, 2021. https://www.bbc.com/news/uk-17203398.

Knighton, Andrew. "Manned Torpedoes and Massive Ships – The Alexandria Raid of World War Two." War History Online. Mar. 16, 2017. Accessed June 25, 2021. https://www.warhistoryonline.com/world-war-ii/alexandria-raid-1941.html.

"Lankan Army Foils Tigers' Master Counter Stroke." *Outlook India [Online]*. Feb. 2, 2009. Accessed June 22, 2021. https://www.outlookindia.com/newswire/story/lankan-army-foils-tigers-master-counter-stroke/653172.

Linton, E.W. (Jake), and Hector Donohue. "The Swimmer/Sapper Attack at Vung Tau 23 May 1969." *Naval Historical Review*. Dec. 2016. Accessed June 28, 2021. https://www.navyhistory.org.au/the-swim.

McManus, Doyle, and Robert C. Toth. "Setback for Contras : CIA Mining of Harbors 'a Fiasco'." *Los Angeles Times*. Mar. 5, 1985. Accessed June 22, 2021. https://www.latimes.com/archives/la-xpm-1985-03-05-mn-12633-story.html.

Minorities at Risk Project. *Chronology for Sri Lankan Tamils in Sri Lanka.* 2004. Accessed June 22, 2021. https://www.refworld.org/docid/469f38e0c.html.

National Museum of the Navy. "Underwater Demolition: Korean War." *The Blast* 41, no. 4. UDT-SEAL Association. 2019. https://www.honor.org/wp-content/uploads/2020/03/126121_UDT_Blast4Q2019_Web-December.pdf.

Navy Seal Museum. "Operation JUST CAUSE: Navy SEALs in Panama." navysealmuseum.org. Aug. 2019. Accessed June 22, 2021. https://www.navysealmuseum.org/about-navy-seals/seal-history-the-naval-special-warfare-storyseal-history-the-naval-special-warfare-story/operation-just-cause-navy-seals-panama.

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, Article 8 (2015). https://digital-commons.usnwc.edu/nwc-review/vol68/iss3/8.

"Old Soldier Remembers Blowing Up Huge Warship." *Viet Nam News [Online]*. Updated May 17, 2015. Accessed June 28, 2021. https://vietnamnews.vn/english-through-the-news/270368/old-soldier-remembers-blowing-up-huge-.

"Operation Jaywick." Australian War Memorial. Last updated Dec. 7, 2020. Accessed June 25, 2021. https://www.awm.gov.au/articles/encyclopedia/operation_jaywick.

Sacquety, Troy J. "The OSS Arakan Field Unit (AFU)." *Veritas* 8, no. 1, 2012. Accessed June 25, 2021. https://arsof-history.org/articles/v8n1_avedon_sb_arakan.html.

Singlaub, John K. *Hazardous Duty: An American Soldier in the Twentieth Century*. New York: Summit Books, 1991.

Sobchak, Frank K. "The Raid on St. Nazaire: Special Operations Planning." *Infantry Magazine.* Sept-Dec. 1998. ProQuest Central. https://www.proquest.com/trade-journals/raid-on-st-nazaire-special-operations-planning/docview/219711976/se-2?accountid=10186.

SOFREP. "Operation Frankton, the Most Daring Raid of All Time?" *SOFREP*. Dec. 11, 2019. Accessed June 25, 2021. https://sofrep.com/news/operation-frankton-daring-raid-time-2/.

Steven. "GI Resistance in the Vietnam War." libcom.org. Sept. 3, 2006. Accessed June 28, 2021. http://libcom.org/history/vietnam-gi-resistance.

Surhone, Lambert M., Mariam T. Tennoe, and Susan F. Henssonow. *Operation Albumen*. Betascript Publishing, 2011. https://books.google.com/books?id=DLc7KQEACAAJ.

"S.O.S & Stop Our Ship." *Good Times* IV, no. 30. Nov. 12, 1971. Accessed June 28, 2021. https://www.foundsf.org/index.php?title=S.O.S_%26_Stop_Our_Ship.

Taylor, David A. "The Inside Story of How a Nazi Plot to Sabotage the U.S. War Effort Was Foiled." *Smithsonian*. June 28, 2016; Updated June 26, 2017. Accessed June 25, 2021. https://www.smithsonianmag.com/history/inside-story-how-nazi-plot-sabotage-us-war-effort-was-foiled-180959594/.

This U.S. Sub Launched an Attack on a Japanese Train. Smithsonian Channel. 2018. YouTube. Accessed June 28, 2021. https://www.youtube.com/watch?v=Y6Ed7EQiLXU.

Tremlett, Giles. "Falklands War Almost Spread to Gibraltar." *The Guardian [Online]*. July 23, 2004. Accessed June 22, 2021. https://www.theguardian.com/world/2004/jul/24/gibraltar.falklands.

"Trial of Sailor Opens in Sabotage of Carrier Ranger." *New York Times*. June 10, 1973. https://www.nytimes.com/1973/06/10/archives/trial-of-sailor-opens-in-sabotage-of-carrier-ranger-in-prison-since.html.

Tuck, Howard. "The Pebble Island Raid." *Defense Media Network [Online]*. October 14, 2016. Accessed June 22, 2021. https://www.defensemedianetwork.com/stories/the-sas-raid-on-pebble-island/.

US Congress. House. Committee on Armed Forces. *Report by the Special Subcommittee on Disciplinary Problems in the US Navy*. 92nd Cong., 2d sess., 1973, H.A.S.C. 92-81. Washington, DC: Government Printing Office, 1973. https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/r/report-by-special-subcommittee-disciplinary-problems-us-navy.html

Walker, David A. "OSS and Operation Torch." *Journal of Contemporary History* 22, no. 4 (Oct. 1987): 667-679. Accessed June 25, 2021. JSTOR. https://www.jstor.org/stable/260815.

Warfare History Network. "Operation Ginny: Why America's Secret Raid Against Nazi Germany Failed." The National Interest. May 8, 2020. https://nationalinterest.org/blog/buzz/operation-ginny-why-americas-secret-raid-against-nazi-germany-failed-152376.

Yates, Lawrence A. *The U.S. Military Intervention in Panama: Operation Just Cause December 1989–January 1990*. Contingency Operations Series. Washington DC: Center of Military History, United States Army. CMH Pub 55–3–1. https://history.army.mil/html/books/055/55-3-1/cmhPub_55-3-1.pdf.

This page intentionally left blank.

CNA

Dedicated to the Safety and Security of the Nation