A Historical Primer of Espionage
within the U.S. Department of the Navy

TREASONOUS TIDES

Stephen C. Ruder

TREASONOUS TIDES

TREASONOUS TIDES

A Historical Primer of Espionage within the U.S. Department of the Navy

Stephen C. Ruder

MCUP
MARINE CORPS UNIVERSITY PRESS
Quantico, Virginia
2025

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA
Names: Ruder, Stephen C., author. | Marine Corps University (U.S.). Press, issuing body.
Title: Treasonous tides: a historical primer of espionage within the U.S. Department of the Navy / Stephen C. Ruder.
Other titles: Historical primer of espionage within the U.S. Department of the Navy
Description: Quantico, Virginia: Marine Corps University Press, [2025] | In scope of the U.S. Government Publishing Office Cataloging and Indexing Program (C&I); Federal Depository Library Program (FDLP) distribution status to be determined upon publication. | Includes bibliographical references. | Summary: "Treasonous Tides looks at more than a century of espionage against and within the U.S. Department of the Navy (DON) to discern the trends that will illuminate the future of U.S. naval counterintelligence. Based on the principles of war, the book suggests a new way to interpret naval counterintelligence that emphasizes the merger of intelligence and law enforcement to ensure that the DON wins the war at sea. Including more than 50 espionage cases that impacted the DON from 1898 to 2010, the book places each case into historical perspective, provides a brief overview, and draws out the significance and lessons learned for each. The book highlights trends that remain applicable today while also revealing how the DON's past apathy and lack of investment in counterintelligence led to strategic surprise on several occasions. The book also provides unique insight into the motivations and methods of those who spied against the DON, most of which remained remarkably consistent for more than 100 years. At the strategic level, the book clarifies the relative significance of each case and uses that information to suggest an operational prioritization for the future. Everyone involved in resourcing, planning, executing, and benefiting from U.S. naval counterintelligence will profit from the history and analysis presented here"— Provided by publisher.
Identifiers: LCCN 2024055921 (print) | LCCN 2024055922 (ebook) | ISBN 9798987336229 (paperback) | ISBN 9798987336236 (epub)
Subjects: LCSH: United States. Department of the Navy—History. | Intelligence service—United States—History. | Law enforcement—United States—History. | Spies—United States—History. | Espionage, American—History.
Classification: LCC JK468.I6 (print) | LCC JK468.I6 (ebook) | DDC 327.1273009—dc23/eng/20241029 | SUDOC D 214.513:ES 6
LC record available at https://lccn.loc.gov/2024055921
LC ebook record available at https://lccn.loc.gov/2024055922

DISCLAIMER
The views expressed in this publication are solely those of the author(s). They do not necessarily reflect the opinion of Marine Corps University, the U.S. Marine Corps, the U.S. Navy, the U.S. Army, the U.S. Air Force, or the U.S. government. The information contained in this book was accurate at the time of printing. Every effort has been made to secure copyright permission on excerpts and artworks reproduced in this volume. Please contact the editors to rectify inadvertent errors or omissions.

Copyright for all works—journals and monographs—is retained by the author(s). Some works of authorship from Marine Corps University Press (MCUP) are created by U.S. government employees as part of their official duties and are now eligible for copyright protection in the United States; further, some of MCUP's works available on a publicly accessible website may be subject to copyright or other intellectual property rights owned by non-Department of Defense (DOD) parties. Regardless of whether the works are marked with a copyright notice or other indication of non-DOD ownership or interests, any use of MCUP works may subject the user to legal liability, including liability to such non-DOD owners of intellectual property or other protectable legal interests.

MCUP makes every effort to ensure that no generative AI was used in the creation of its works. MCUP products are published under a Creative Commons NonCommercial-NoDerivatives 4.0 International (CC BY - NC-ND 4.0) license.

Published by
Marine Corps University Press
2044 Broadway Street
Quantico, VA 22134

1st Printing, 2025
ISBN: 979-8-9873362-2-9
DOI: 10.56686/9798987336229

THIS VOLUME IS FREELY AVAILABLE AT WWW.USMCU.EDU/MCUPRESS

Contents

Foreword

When one thinks of a military spy, images often flash of a mysterious man in a tuxedo speeding away in a sleek sports car, shadowy figures meeting in a dimly lit foreign café, or intense brawls with hulking henchmen. If only those fantasies were real. Or perhaps one thinks of true villains, such as Aldrich H. Ames or Robert P. Hanssen. But the reality is neither romantic nor dramatic—it is far more mundane and, in many ways, far more sobering. While the U.S. Department of the Navy (DON) has had its share of high-profile cases, more often than not, the villain is a cash-strapped, lonely young man willing to sell his last shred of dignity to the highest bidder. This book offers a stark, unfiltered look at the real espionage cases that have plagued the U.S. Navy and Marine Corps for more than a century, examining the impact on the DON's combat effectiveness and how to contend with these threats in the years to come.

Nearly a decade ago, when I reported for duty as the assistant special agent in charge of the Naval Criminal Investigative Service (NCIS) Southeast Asia Field Office in Singapore, I met the author of this book, Steve Ruder, then the senior intelligence analyst for the field office. Though I had a background in criminal investigations, my knowledge of counterintelligence was relatively limited. Steve, however, was a seasoned counterintelligence analyst with more than 20 years of experience. He offered to mentor me, drawing from a trove of historical material he had amassed over the years but never had a chance to fully explore. So, every Friday afternoon for several months, we went through the history of naval espionage, examining each case in depth.

The insights that Steve shared with me were eye-opening, underscoring the severe consequences that peacetime espionage can have during times of conflict. I carried those lessons with me throughout my career, and I relied on them for our counterintelligence activities while serving as the special agent in charge of the NCIS Hawaii Field Office and later as the NCIS executive assistant director for Pacific operations. Given the heightened tension in the Indo-Pacific—something I was acutely aware of—these lessons remain both timely and essential.

For Steve, a former Marine Corps intelligence officer, mentoring future leaders was simply a duty he felt compelled to fulfill. His decades of experience lent exceptional credibility to his analysis. Since 1989, Steve has studied the espionage activities of every major adversary the United States has faced, from the Soviet Union to Serbia, from al-Qaeda to Iraq, and from Russia to China. Steve has applied his knowledge and expertise to countless espionage investigations, threat analyses, and other counterintelligence operations. Along the way, he has been individually or collaboratively honored with three Defense Counterintelligence Awards, two National Counterintelligence and Security Awards, NCIS Civilian of the Year, and the U.S. Army Commander's Award for Public Service. He is the most knowledgeable counterintelligence expert I have ever met. Now, just as he did with me a decade ago, Steve has written this book as a selfless effort to pass on the insights he has gained from more than 30 years of naval counterintelligence.

While no organization enjoys scrutinizing the negative aspects of its personnel, understanding why and how espionage occurs is essential for addressing these problems and implementing sustainable solutions. Unlike most crimes, espionage has the potential to impact thousands of lives—lives that may be lost on the battlefield. This book explores that reality, using historical examples to illustrate long-term patterns in how and why sailors, Marines, and civilians have under-

mined or attempted to undermine U.S. naval operations through acts of espionage. It also examines how, over time, the DON has attempted—and often struggled—to address these issues with workable, resourced long-term solutions.

Given that sweeping remit, this book operates on multiple levels. First, it stands as the most comprehensive compilation of U.S. naval espionage cases in existence. Second, through historical case studies, it weaves a narrative that not only chronicles more than 50 espionage cases spanning more than a century but also assesses the impact of each case on naval warfare. Finally, the analysis throughout the book offers valuable insights for investigators, a policy road map for the future, and, for today's sailors and Marines, a deeper understanding of how espionage and counterespionage play a crucial role in the larger framework of naval operations and warfighting.

For readers such as myself—law enforcement officers and their leaders—this book serves as an essential guide, filled with historical examples of counterintelligence investigative techniques highlighting both successes and, perhaps more valuably, failures. For military leaders, this book provides a window into the world of naval counterintelligence, underscoring its critical relevance and importance to warfighters. For policymakers, the cases in this book showcase counterintelligence capabilities that have proven indispensable for more than a century, despite frequently being left to wither unfunded. This book critiques shortsighted decisions and offers a path forward to prevent a repeat of the most serious espionage-driven strategic surprises that have challenged the DON during the past century. For all the above reasons, I consider Steve's book a must-read for anyone who serves as or supports the U.S. warfighter.

Nayda Mannle
Former Executive Assistant Director of Pacific Operations
U.S. Naval Criminal Investigative Service
Kailua, Hawaii

Preface and Acknowledgments

The origin of this study lies in a training session taken more than a decade ago. Using case studies, the training walked a class of naval counterintelligence personnel through an array of high-profile espionage cases. What the course developer overlooked was that few, if any, of the students in the class would ever investigate espionage with the strategic significance of the case studies presented. Instead, like most naval counterintelligence personnel, they would investigate the more routine cases typical of the U.S. Department of the Navy. This work, begun as a quick attempt to rectify that problem, eventually expanded into this study.

I would like to thank my friend and colleague, retired Marine Corps colonel Fred Hudson, for his invaluable thoughts, encouragement, and assistance with this work. Without him, it would never have been finished. Likewise, I would like to thank my family for their patience with the many hours I spent working on this book and for their assistance—particularly my son Frederick for reading the book and suggesting changes. Without their understanding, this work never would have been completed. Finally, I would like to recognize U.S. Naval Criminal Investigative Service public affairs officer Ed Buice, who sadly passed away recently. Without his assistance and encouragement more than a decade ago, I never would have attempted to write several espionage history articles that led me to attempt this study.

While several authors have written books about U.S. naval espionage, particularly during the past 40 years, most have focused largely on individual cases vice the continuum of naval espionage and the risk it poses to warfighting. This book illuminates the world of naval counterintelligence by detailing its successes and failures and their impact on the U.S. national maritime strategy and combat.

This study shows that several times during the past century, the Department of the Navy was unwittingly a victim of strategic surprise largely because it failed to address counterintelligence as a strategic imperative. The cases considered here indicate that only the repeated theft of new construction plans in the early twentieth century drove the department to create a counterintelligence arm at all. Later cases suggest that between World Wars I and II, naval counterintelligence remained weak and isolated from the other Services and the Federal Bureau of Investigation. This study demonstrates that the result of this lack of emphasis on counterintelligence was strategic surprise across the Pacific and what could have been a crippling defeat at Pearl Harbor, Hawaii, in December 1941. This study shows that as the United States entered the atomic age and developed the modern nuclear triad, unproductive background investigations swamped naval counterintelligence. The study links that problem to the John A. Walker Jr. espionage ring and describes how the Walker case could have impaired the United States' submarine-launched nuclear missile capability. Finally, this study attests to the challenges faced by the department as it entered the information age and suggests that its contractors left data networks undersecured, which resulted in the massive loss of sensitive but unclassified technical information, reportedly allowing adversaries to bypass years of research and development in the fielding of weapons and combat systems.

This study argues that the root of each of those strategic surprises was a lack of naval counterintelligence operational prioritization and that the evolution of U.S. naval counterintelligence was fraught with missteps, inconsistencies, and neglect. It demonstrates that its forma-

tion in the face of World War I and then abandonment until World War II as well as a continuously rotating series of relatively inexperienced line officers, sailors, and contract civilian investigators hamstrung naval counterintelligence well into the Cold War. This study shows that the situation changed dramatically with the implementation of new U.S. counterintelligence policies in 1979–80 and the beginnings of a truly professionalized naval counterintelligence capability. The cases considered here reveal that with expanded investigative authority, within a decade the Naval Criminal Investigative Service had effectively reduced the threat of espionage from a critical concern for the Department of the Navy's leadership to an irritant that required little investment. This examination of the past several decades of espionage proves that after 1986, no U.S. naval espionage case concluded without a full reckoning of the damage caused by the compromise of classified information. Finally, this study suggests that throughout the past century, the department's counterintelligence efforts were hampered by a lack of focus on critical warfighting capabilities as a means to prioritize strategic counterintelligence resource allocation, operational fleet counterintelligence integration, and tactical counterespionage investigative activities.

This study presents a historical trend analysis of most U.S. naval espionage cases during the past century, which illustrates four bedrock principles about strategically countering espionage and resourcing naval counterintelligence:

- The employment of limited naval counterintelligence assets worked best when tied to an enduring operational prioritization that was both predictive and focused on warfighting. Inadvisedly prioritizing background investigations during the early Cold War left the Department of the Navy open to a shift in Soviet espionage that contributed to rapid Soviet advances in undersea warfare. Once shed of the background investigation mission, naval counterintelligence quickly regained the initiative.

- Espionage investigations required extensive physical and technical surveillance. The surveillance personnel were skilled technical specialists who were expensive to train and retain but critical to ensuring militarily effective resolutions to espionage. Lack of surveillance capacity within naval counterintelligence left the Department of the Navy largely blind to Japanese intelligence collection on Oahu, Hawaii, just prior to World War II and contributed to the intelligence failure at Pearl Harbor in December 1941.
- Espionage investigations were, at their heart, criminal investigations. The most successful naval counterintelligence investigators were well-versed and experienced in criminal and intelligence procedures, rules of evidence, and the law. The lack of criminal investigative experience within naval counterintelligence in the 1930s compromised several espionage investigations and left the Department of the Navy with little understanding of the damage done.
- Interagency, allied, and partner collaboration was routinely a key enabler for naval counterintelligence. Facilitating that sharing by experienced and aggressive liaison within the United States and at naval concentration areas around the world was an expensive but critical requirement. The discreet sharing of extremely sensitive counterintelligence information alerted the Department of the Navy to more than half of the traitors in their midst during the period of this study.

In any future environment of pressure to reduce expenditures, Department of the Navy leaders must be aware that shortchanging counterintelligence is a false economy, and the department must formulate enduring strategies for prioritizing its counterintelligence resources to maximize their efficiency.

TREASONOUS TIDES

Introduction

At the most strategic level, the U.S. Secretary of the Navy defines *counterintelligence* as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, assassinations conducted for or on behalf of foreign powers, organizations, persons, or their agents, or international terrorist organizations or activities."[1] This definition suggests that if naval counterintelligence identified, deceived, exploited, disrupted, or protected against espionage, then it was militarily effective. However, the cases considered in this study demonstrate that this was not necessarily the case.

This definition of counterintelligence does not describe how it supports naval operations. However, the principles of war discussed in *Naval Warfare*, Naval Doctrine Publication (NDP) 1, may provide clues.[2] Based on centuries of lessons learned, the nine principles of war do not directly mention counterintelligence, but three of these sweeping military principles (figure 1), form the foundation of the counterintelligence contribution to victory at sea: security, mass, and surprise.

The principle of security states that the commander must "never permit the enemy to acquire an unexpected advantage."[3] One can be certain that the adversary will gain an advantage but, as implied in the

[1] *Secretary of the Navy Instruction 3850.2E, Counterintelligence* (Washington, DC: Department of the Navy, 3 January 2017), Encl. 2, 1.
[2] *Naval Warfare*, Naval Doctrine Publication 1 (Norfolk, VA: Naval Warfare Development Center, 2020), 57.
[3] *Naval Warfare*, 57.

Figure 1. The nine principles of war

- Objective. Direct every military operation toward a clearly defined, decisive, and attainable objective.
- **Mass. Concentrate combat power at the decisive time and place.**
- Maneuver. Place the enemy in a position of disadvantage through the feasible application of combat power.
- Offensive. Seize, retain, and exploit the initiative.
- Economy of Force. Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary efforts.
- Unity of Command. Ensure unity of effort for every objective under one responsible commander.
- Simplicity. Avoid unnecessary complexity in preparing, planning, and conducting military operations.
- **Surprise. Strike the enemy at a time or place or in a manner for which he is unprepared.**
- **Security. Never permit the enemy to acquire unexpected advantage.**

Source: *Naval Warfare*, Naval Doctrine Publication 1 (Washington, DC: Department of the Navy, 1994), adapted by MCUP.

This study will demonstrate that mass, surprise, and security are the principles of war most applicable to counterintelligence.

principle of security, a commander that is aware of the adversary's advantage can adjust the plan. This study suggests that to have been militarily effective, naval counterintelligence should have ensured that any enemy advantage was ***not unexpected*** so that plans could be adjusted.

The principle of mass tells one's enemy to concentrate combat power at the decisive time and place. Similarly, the principle of surprise tells the enemy to strike at a time or place or in a manner for

which one is unprepared. Both mass and surprise focus on gaining a *time and place advantage*. Surprise also encompasses another concept, "*a manner for which he is unprepared*," which alludes to weapons and tactics.[4] The principles of security, mass, and surprise guide naval counterintelligence toward a fundamental mission of ensuring that enemy knowledge of three basic categories of information is *not unexpected*:

- Where forces will be.
- When forces will be there.
- How forces will fight.

This study demonstrates that throughout its history, U.S. naval counterintelligence was often militarily ineffective because it either failed to achieve that fundamental mission or the intervention came too late to be militarily effective. The principles of security, mass, and surprise suggest that the objective of espionage prosecutions is to ensure full disclosure of all the information compromised. The legal framework surrounding espionage provides the leverage to do so. However, this study suggests that naval counterintelligence was historically a limited resource in need of operational prioritization. The degree to which U.S. Department of the Navy (DON) and counterintelligence practitioners agreed on the relative sensitivity of information was unclear throughout the period of this study. Both classification and myriad warfighting effects appear to have driven counterintelligence priorities.

However, naval history suggests that a militarily effective U.S. naval counterintelligence operational prioritization should not have been based solely on classification or diffused among myriad warfighting effects, but that it should have instead striven to quickly identify the loss of the type of information that could result in the loss of an

[4] *Naval Warfare*, 57.

entire naval campaign: command and control information.[5] Because this had the potential to be campaign-altering, the DON should have considered command and control espionage the most critical element of a naval counterintelligence strategy. The DON should also have considered weapons and sensors secondary naval counterintelligence priorities because throughout the course of naval history, their compromise often resulted in tactical defeats but generally did not affect the outcome of a campaign once addressed. The cycle of sensor/weapon and countermeasure development was generally a slow process, but occasionally the cycle caught one side or the other off guard and resulted in tactical defeats that were overcome through improved tactics or rapid countermeasure development. Finally, the DON should have considered shore establishments a tertiary naval counterintelligence priority and always assumed that observation was ongoing.

This work addresses the lack of widely available data-driven analytic studies to form the basis for an enduring U.S. naval counterintelligence operational prioritization. It breaks new ground in the DON leadership's understanding of the military effectiveness of counterintelligence within the context of naval warfighting; provides a basis for suggesting future counterintelligence priorities; and, at a more granular level, forms the nucleus of a naval counterintelligence lessons learned repository.

Because this work seeks a broad audience, stretching from DON leadership to warfighters and counterintelligence practitioners, secondary sources that provide concise summaries of complex historical topics form the bulk of the background information about naval campaigns and other historical events. Those sources provide the necessary context for those with only general knowledge of world and military history.

[5] See appendix E for a discussion of the historical events behind this statement.

This study describes espionage operations that were conducted by a wide chronological and geographic breadth of intelligence adversaries of the United States, from late-nineteenth-century Spanish naval intelligence, to mid-twentieth-century Imperial Japanese Navy intelligence, to late-twentieth-century Soviet KGB and early twenty-first-century People's Republic of China military intelligence. Comparing and contrasting the histories, motivations, and successes of the many foreign intelligence services that have targeted the DON would have made this study more complete. However, that level of academic scrutiny lies beyond the scope of a historical primer intended to familiarize a broad audience. Hopefully, this study inspires additional research and study to fill that gap.

Much of the previous literature about naval counterintelligence appears as either organizational histories about the activities of naval counterintelligence agencies and personnel such as *A Century of U.S. Naval Intelligence* by Captain Wyman H. Packard or memoirs such as *Secret Missions* by Ellis M. Zacharias and *Special Agent, Vietnam* by Douglass H. Hubbard Jr.[6] However, this study is not a history of naval counterintelligence. Rather, it details and analyzes the espionage cases that those organizations and personnel were charged to investigate and neutralize.

This study is not the first to detail and analyze naval espionage cases. Some previous literature has touched on many aspects of a selection of individual espionage cases in discreet and isolated ways, but none address them holistically or in the context of warfighting. Those studies form two categories: narrow, deep studies of individual case histories; and wide, shallow studies of U.S. Department of Defense

[6] Capt Wyman H. Packard, USN (Ret), *A Century of U.S. Naval Intelligence* (Washington, DC: Department of the Navy, 1996), 248–99; RAdm Ellis M. Zacharias, USN, *Secret Missions: The Story of an Intelligence Officer* (Annapolis, MD: Naval Institute Press, 1946); and Douglass H. Hubbard Jr., *Special Agent, Vietnam: A Naval Intelligence Memoir* (Washington, DC: Potomac Books, 2006).

(DOD) espionage writ large. Examples of the former include Ronald J. Olive's *Capturing Jonathan Pollard*, Pete Earley's *Family of Spies*, and Ronald Kessler's *The Spy in the Russian Club*.[7] Olive, a former Naval Investigative Service special agent, was directly involved in the Pollard case and so his book serves as a primary reference. His insights into the case are invaluable. Earley and Kessler are journalists, so their accounts, while very useful, do not have the same direct insights as Olive's, but their works remain excellent secondary sources. For the purposes of academic study of naval espionage, all three are superb resources on each individual case, but none address the wider trends and implications of espionage that targets the DON.

The most prominent example of this is the Defense Personnel and Security Research Center (PERSEREC). PERSEREC is a DOD entity established in Monterey, California, in 1986 as a response to the John A. Walker Jr. espionage case. The Walker case involved the U.S. Navy and is included in brief in this study. PERSEREC broadly works to improve the DOD's security clearance program but is also a principal source of unclassified information on espionage for the U.S. security community. PERSEREC maintains an unclassified database of more than 200 espionage and security cases from across the U.S. government. Since 1992, PERSEREC has published five reports containing espionage case summaries and analyses of the perpetrators of espionage in the United States from 1945 to 2015. For DON purposes, however, PERSEREC research focused on the entire DOD, did not include espionage prior to 1945, examined a limited number of elements for comparison, and did not address the wider implications of espionage for warfighting. Not including World War II-era cases is particularly pertinent to the immediate future of U.S. naval counterintelligence because the DON

[7] Ronald J. Olive, *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice* (Annapolis, MD: Naval Institute Press, 2006); Pete Earley, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1988); and Ronald Kessler, *The Spy in the Russian Club* (New York: Charles Scribner's Sons, 1990).

is potentially facing another Pacific War as it did during 1941–45. As with the books on individual cases, while the PERSEREC studies are valuable research tools, they are not unique to the DON and do not study the problem in sufficient depth and breadth to discern trends across multiple adversaries and periods as well as evaluating the military effectiveness of the response.[8]

To expand on the individual case history books and PERSEREC research, this study uses a case brief approach to compile a data set of DON-specific espionage incidents. A survey of the five PERSEREC publications contained references to all post-1945 DON cases. A wide range of other sources, cited in the case briefs in the following chapters, identified the pre-1945 cases. The selection criteria for cases between 1898 and 1930 was simply available information. However, from 1930 onward the selection criteria limited inclusion to cases prosecuted under the Espionage Statute, the law passed in 1917 that forms the basis of espionage prosecutions today.[9] The study totals 57 case briefs, which form the bulk—if not entirety—of espionage cases within the DON between 1898 and 2010. Those 57 cases totaled 63 espionage subjects in 54 of the cases. In three additional cases—USS *Pennsylvania* (BB 38), USS *Hull* (D 7), and the unidentified chief—the perpetrator either was not identified or the case was unsolved. Four other cases—Kurt A. Jahnke, George Roenitz, Christian F. Danielsen, and Gustav E. Guellich—have been cast in histories as espionage, but the record is unclear. Finally, one case—Michael S. Schwartz—began

[8] Suzanne Wood and Martin F. Wiskoff, *Americans Who Spied against Their Country since World War II* (Monterey CA: Defense Personnel Security Research Center, 1992); Katherine L. Herbig and Martin F. Wiskoff, *Espionage against the United States by American Citizens, 1947–2001* (Monterey CA: Defense Personnel Security Research Center, 2002); Katherine L. Herbig, *Changes in Espionage by Americans: 1947–2007* (Monterey CA: Defense Personnel Security Research Center, 2008); *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008* (Monterey, CA: Defense Personnel Security Research Center, 2009); and Katherine L. Herbig, *The Expanding Spectrum of Espionage by Americans, 1947–2015* (Monterey, CA: Defense Personnel Security Research Center, 2017).

[9] Espionage Act of 1917, Pub. L. No. 65–24, 40 Stat. 217 (1917).

as an espionage case but ended with the subject pleading guilty to a lesser charge. All eight of those cases are described in case briefs but have been excluded from statistical analysis, leaving 49 cases totaling 58 espionage subjects.

The case briefs that form the data set for this study are not full descriptions of each case. Often a much larger body of information exists, but the data was extraneous to the requirements of this study. The case briefs are instead short narratives intended to identify the following 21 discreet variables in four sections:

Background

- Age
- Marital status
- Clearance level
- Access
- Motivation
- Financial considerations
- Substance abuse considerations

Recruitment and Espionage

- Espionage country
- Recruitment type
- Espionage success
- First contact method
- First contact location
- Tradecraft employed

Investigation and Punishment

- U.S. counterintelligence detection method
- Espionage duration
- Legal issues
- Incarceration

Significance

- Strategic significance
- Military effectiveness of the investigation
- Warfighting lessons learned
- Counterintelligence lessons learned

This study includes a comparison of the data set derived from each of these 21 variables that result from examining the 58 subjects identified herein as bonafide espionage subjects across the 112-year span of the study to determine trends and derive lessons learned. Additionally, to better understand the warfighting and counterintelligence lessons learned, a short description of the historical context in which the espionage occurred precedes each case brief.

Due to the sensitive nature of counterintelligence activities, much of this work is based on publicly available information. Wherever possible, primary sources provide pertinent details. However, much of the information remains classified or, for older cases, the files are no longer available. For cases that occurred before 1935, data is based largely on secondhand information documented in press coverage, an official history, a historical investigation, and one surviving original investigative document recovered from the National Archives. Much of the 1935–45 data is based on Federal Bureau of Investigation case files acquired through the Freedom of Information Act (FOIA). However, the Germany-related data largely relied on primary source information from British Security Service (MI5) archival files.

The 1945–2010 data is based primarily on press reporting of the court proceedings acquired through a commercially available online newspaper database. Secondary sources such as these are not preferable, but they were the only means available for cases that were not already released through the lengthy FOIA process. For example, the author's first-time FOIA request for the 1962 Nelson C. Drummond investigation took several years to process and resulted in 563 pages

of an FBI jury panel investigation in preparation for Drummond's espionage trial but no case details.[10] Most other cases remain ineligible for access by researchers through FOIA because the subject of the investigation is still alive or died during the writing of final drafts of this study, and FOIA restricts the provision of information about a living second party without their consent.

While individual military personnel records would be a useful primary source for information about individuals discussed in each case brief, the Privacy Act of 1974's "No Disclosure without Consent" rule requires the consent of the individual or, at their death, the consent of their next-of-kin to release those records.[11] However, military personnel records are open to the public 62 years after a servicemember leaves the military. The National Archives and Records Administration notes that FOIA and the Privacy Act provide balance between the right of the public to obtain information from military service records and the right of the former military servicemember to protect their privacy.

For the research presented here, 75 percent of the cases reviewed fall within the Privacy Act and FOIA restrictions and required consent from the individual or next-of-kin. Due to the circumstances of these individuals' legal histories, consent was not sought from the living or from the next-of-kin of the deceased, and background information made available by publicly available sources was deemed suitable for the scope of the research.[12]

Although it may seem counterintuitive, despite the highly secretive nature of counterintelligence, press reporting about prosecutions often provided information about the 21 discreet variables needed for

[10] Federal Bureau of Investigation, "FOIPA Request No.: 1158292-002, Subject: Drummond, Nelson Cornelious," letter to the author, 22 February 2017.
[11] Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat. 1896 (1974).
[12] "Veteran's Service Records," National Archives and Records Administration, accessed 7 July 2023.

this study because those variables were often the same information presented in court by the prosecutors to prove the elements of the Espionage Act. By studying those discreet variables across 58 espionage subjects spanning more than a century, this work lays the foundation for strategic thought about counterintelligence within the DON to better define the mission of naval counterintelligence, suggests enduring naval counterintelligence priorities, and realizes a common understanding of the strategic imperative of naval counterintelligence.

Chapter 1
Early Modern-era Case Briefs, 1898–1918

At the end of the American Civil War in 1865, the U.S. Navy included hundreds of ships and tens of thousands of men. However, it was almost entirely a green-water navy, organized and equipped for riverine and coastal combat. With no domestic enemies left to fight and an isolationist government, the Navy quickly deteriorated. Then, in the 1880s, as the last of the Civil War-era officers were retiring, the United States elected a more internationally focused series of presidential administrations. As a result, the Navy began to rebuild.[1]

Far outstripped by the European navies, the U.S. Navy embarked on a massive technology collection operation to buy or copy the newest naval armaments and designs from Europe. At first, the effort was haphazard, but eventually the Department of the Navy (DON) focused the activities into one office, the Office of Naval Intelligence (ONI). ONI had only a foreign intelligence collection responsibility from 1882 until 1916. Because the Navy was only building its force, it was

[1] See *Report of the Secretary of the Navy, Being Part of the Message and Documents Communicated to the Two Houses of Congress at the Beginning of the Second Session of the Forty-Seventh Congress, in Three Volumes*, vol. 1 (Washington, DC: Government Printing Office, 1882), 6. This indicates the need for the U.S. Navy to move from wooden ships to steel ships. See also William S. Peterson, "Congressional Politics: Building the New Navy, 1876–86," *Armed Forces & Society* 14, no. 4 (Summer 1988): 489–509; and David Colamaria, "The Story of the New Steel Navy," Sailor's Life in the New Steel Navy (website), 2010.

not much of a target for foreign espionage. As such, the DON did not devote any effort to counterintelligence.[2]

Even if the DON had a counterintelligence capability, the lack of appropriate legislation would have hamstrung it. As late as 1916, when World War I raged in Europe, the United States had no workable law against committing espionage. Beginning in 1898, Congress passed two laws intended to protect defense information. However, these laws focused primarily on protecting fixed installations from sabotage and collection of information by outsiders during wartime. The laws did not address the concept of an insider compromising a wide range of defense information during peacetime.[3] Counterintelligence agencies, if they had existed, would have had limited legal authority to act. Congress solved the problems in 1917 by passing the Espionage Act, a version of which is still used today.[4]

Additionally, the relative sensitivity of the material was a problem. While the U.S. military recognized a need to keep some information "confidential," there were no classification markings. For example, Navy General Order No. 36 of 20 August 1909 stipulated, "It is desired that all features of the present system of training [target practice and engineering] be held as confidential, and therefore it is directed that foreigners or persons not directly connected with the naval service be given as little information as is consistent with professional etiquette."[5]

Then, realizing a need to define terms, the U.S. military struggled for a decade with meanings for the markings used on classified materials. The Navy first defined *confidential* in 1909. In 1917, the Ameri-

[2] Capt Wyman H. Packard, USN (Ret), *A Century of U.S. Naval Intelligence* (Washington, DC: Department of the Navy, 1996), 1–2, 12–13.
[3] Harbor Defenses Act of 1898, 55th Cong., § 575–576 (1898); and Defense Secrets Act of 1911, 61st Cong., § 224–226 (1911).
[4] Espionage Act of 1917, Pub. L. No. 65–24, 40 Stat. 217 (1917).
[5] "Changes in Naval Regulations and Naval Instructions No. 7, 1916, and Navy General Order No. 36, 1909," National Archives Staff Information Paper, Origin of Defense-Information Markings in the Army and Former War Department (Washington, DC: National Archives and Records Service, 1972), annexes R and S.

can Expeditionary Forces, deployed to France to fight in World War I, copied the classification regulations of the British and French armies and created the system in use today.[6]

So, before World War I, U.S. counterintelligence had no legal authority and no legal way to determine what information was sensitive. By the end of World War I in 1918, Congress and the U.S. military had created the basic framework still used today.

By April 1898, a war with Spain loomed and the transition from wooden to steel ships begun in the 1880s was complete. As the Secretary of Navy John D. Long noted, "When I entered upon my duties in March 1897, the Navy, though not large compared with the navies of one or two foreign powers, was well equipped and well prepared."[7]

Unfortunately, the counterintelligence and security assets of the Navy lagged far behind the progress of its steel ships. As the United States moved toward war with Spain, the legal and investigative basis for effective counterintelligence was far from ready, and there was no way for the DON to ensure that any advantage gained by Spain was *not unexpected*. The DON had no organic investigative capability, and the nation had only the Secret Service, an element of the Treasury Department, as its sole federal law enforcement agency. Moreover, unless war was declared, the United States had no law against espionage. The first quasi-espionage law was not enacted until July 1898, just as hostilities with Spain ended.[8] Against this backdrop of naivete about the realities of espionage and foreign intelligence, the DON embarked on its first

---

[6] *Executive Classification of Information—Security Classification Problems Involving Exemption (b) (1) of the Freedom of Information Act (5 U.S.C. 552): Third Report by the Committee on Government Operations* (Washington, DC: Government Printing Office, 1973), 4–5; and Arvin S. Quist, *Security Classification of Information*, vol. 1, *Introduction, History, and Adverse Impacts* (Oak Ridge, TN: Oak Ridge Classification Associates, 2002), 22, 25–26.

[7] *The American-Spanish War: A History by War Leaders* (Norwich, CT: Chas. C. Haskell & Son, 1899), 339.

[8] Samuel J. Barrows, *New Legislation Concerning Crimes, Misdemeanors, and Penalties: Compiled from the Laws of the Fifty-fifth Congress and from the Session Laws of the States and Territories for 1897 and 1898* (Washington, DC: Government Printing Office, 1900), 4.

war in the modern era. Fortunately, the Secret Service was prepared and took action to protect the department from a disgruntled former sailor.

The First Navy Spy

The first known spy event within the DON was a short-lived attempt at the start of the Spanish-American War. In 1898, Cuba had been a Spanish colony for more than two centuries, and for more than 70 years rebels sought to overthrow the Spanish government, often with U.S. support. In the United States, public sentiment in support of the rebels grew and peaked in February 1898, when the Navy ship USS *Maine* (1889) exploded and sank in Havana Harbor. Despite being militarily unprepared for war, Congress took the drastic step of voting to recognize an independent Cuba, and Spain declared war on the United States on 21 April 1898. At the time, the U.S. Army numbered only 27,500 active troops and the Spanish Navy appeared to be the equal of the U.S. Navy. However, the United States achieved quick victories in the war, defeating Spanish fleets and armies in Cuba and the Philippines.[9]

As Congress deliberated recognizing Cuba during the last two weeks of April 1898, the Secret Service organized an "auxiliary secret service" to conduct counterespionage investigations in the event of war. The Secret Service, the only federal investigative agency in the U.S. government, hired several Spanish-speaking detectives and put them to work surveilling the Spanish diplomatic delegation. On 21 April, when Spain declared war on the United States, the Spanish ambassador, Luis Polo de Bernabé, accompanied by the Spanish naval attaché, Lieutenant Don Ramón de Carranza y Fernández Reguera, left Washington, DC, to return to Spain via Canada.

[9] *The American-Spanish War*, 3–13, 17–92, 289–317.

Figure 2. Ramon de Carranza y Reguera

Source: Don Ramón de Carranza y Reguera, *La Ilustración española y americana* [The Spanish and American Enlightenment] 13 (8 April 1898).

Spanish Navy lieutenant Ramon de Carranza y Reguera, 1898.

Two Secret Service agents accompanied the delegation, ostensibly for their protection. Carranza made headlines as the delegation departed by challenging two senior U.S. officers to a duel over their testimony that Spain was responsible for the sinking of USS *Maine* in Havana.[10] After the delegation's arrival in Canada, they lingered in Toronto, where Carranza organized an espionage operation. Two additional Secret Service agents maintained the surveillance.[11] As they watched the Spanish delegation, a recently discharged sailor from the armored cruiser USS *Brooklyn* (CA 3), seeking revenge and a payout, stumbled into the Secret Service net.

1898: George A. Downing

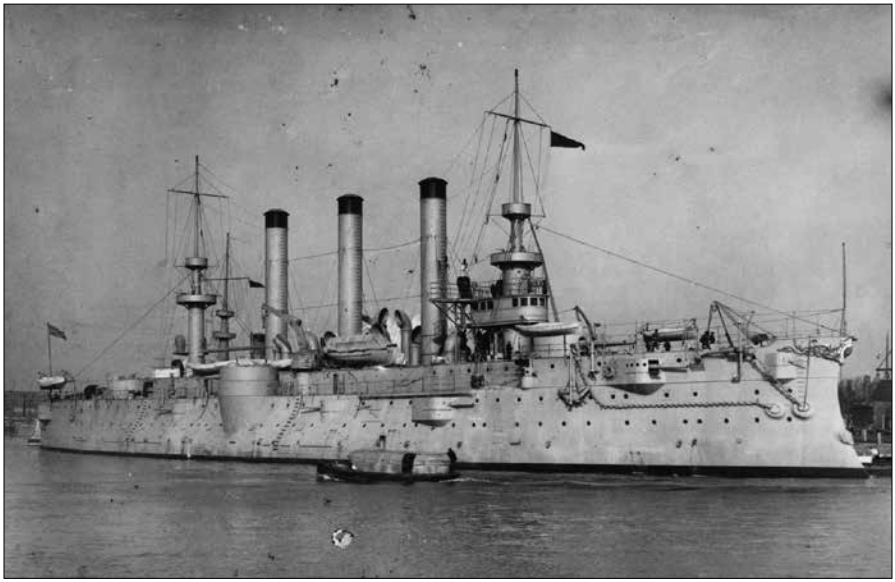
Background

In April 1898, George A. Downing was a recently discharged 33-year-old commissary yeoman, a rate specific to running the consolidated mess, like a modern logistics specialist. Downing was a naturalized former British citizen who had reportedly previously been a merchant sailor with the British shipping company Peninsular and Oriental and crewed a yacht owned by a wealthy New Yorker. Other accounts suggest that Downing had settled earlier in southern Placer County, California, for a time and had been in the Navy for approximately seven years, first aboard the steam sloop of war USS *Mohican* (1883) in California and later aboard *Brooklyn* in New York. After his arrest, an alleged contemporary in California described Downing as "addicted to drink" and someone who "is liable to get himself into any

[10] "Challenged to a Duel," *New York Times*, 16 April 1898.

[11] *The American-Spanish War*, 425–28, 433–36; Don Ramón de Carranza y Reguera, *La Ilustración española y americana* [The Spanish and American Enlightenment] 13 (8 April 1898): 212; and "Letter from U.S. Secretary of the Treasury Lyman J. Gage to U.S. Secretary of State John Sherman regarding surveillance of Carranza, 6 July 1898," Record Group (RG) 59: General Records of the Department of State, Series: Letters Received, File Unit: M179–Miscellaneous Letters of the Department of State, 1789–1906, Item, 1–11 July 1898, NAID: 153522163, National Archives and Records Administration (NARA), College Park, MD, 165.

Figure 3. USS *Brooklyn* (CA 3)



Source: Naval History and Heritage Command, Washington, DC.
USS *Brooklyn* (CA 3) at the New York Navy Yard, Brooklyn, NY, 1898.

scrape." In late April 1898, Downing left the Navy with an honorable discharge but was not recommended for reenlistment, a snub that reportedly enraged him.[12]

Initiation and Espionage

After leaving the Navy, Downing moved from New York to Washington, DC, intent on seeking a job at the Washington Naval Yard. In Washington, he allegedly brooded over the effect that his reenlistment status would have on his job prospects and was drinking heavily. Apparently having made the decision to commit espionage, on 6 May 1898, Downing appeared in Toronto, where he approached the

[12] "Our Military Secret Service," *New York Times*, 10 May 1898; "Suspected Spy, George Downing," *Evening Bee* (Sacramento, CA), 11 May 1898; "An Alleged Spy Suicides," *Evening Bee* (Sacramento, CA), 12 May 1898; and Lt Benton C. Decker, USN, "The Consolidated Mess of the Crew of the U.S.S. Indiana," U.S. Naval Institute *Proceedings* 23, no. 3 (July 1897).

decamped Spanish naval attaché Carranza at his room in the Queen's Hotel and volunteered as a spy for Spain.[13] Carranza interviewed Downing for more than an hour and, convinced that he was genuine, provided Downing with approximately $100 (more than $3,000 today), a code to use for letters, and an accommodation address to mail them to in Montreal. An *accommodation address* refers to an unobtrusive location at which an operative secretly holds routine-appearing mail for pickup by an intelligence service—a technique still used today.[14] Unbeknownst to them both, a Secret Service agent had rented the adjoining room and was able to monitor the entire conversation. When Downing left the Queen's Hotel, the Secret Service agent surveilled him back to his hotel and eventually back to Washington.

Investigation and Punishment

Under constant surveillance and within hours of his return to Washington, Downing visited the DON in what is now the Eisenhower Executive Office Building, where he picked up scraps of information about ship movements. Without using the code provided to him by Carranza, Downing wrote the information in a letter, along with a promise of more information from Norfolk, Virginia, and mailed it to the accommodation address in Montreal. The letter was immediately intercepted by the Secret Service, and military authorities arrested Downing later that same day. He was imprisoned at the Washington Barracks, now known as Fort Lesley J. McNair, in southwest Washington.

Because the United States was formally at war with Spain as of 21 April 1898, Downing was charged under Section 38 of the National Forces Act of 1863, which states: "All persons who, in time of war, or of rebellion against the supreme authority of the United States, shall be found lurking or acting as spies, in or about any of the fortifications,

[13] "Doings of Senor Polo," *Evening Star* (Toronto, ON), 25 April 1898.
[14] Col Mark L. Reagan, USA (Ret), ed., *Counterintelligence Glossary: Terms and Definitions of Interest for Counterintelligence Professionals* (Washington, DC: Department of Defense, 2014), 3.

posts, quarters, or encampments of any of the armies of the United States, or elsewhere, shall be triable by a general court-martial, or by a military commission, and shall, on conviction thereof, suffer death." Despondent, Downing committed suicide in his cell on 13 May 1898.[15]

Significance

Downing was a strategically insignificant, militarily effective financial volunteer because he never provided any information of value and was under constant surveillance throughout his short tenure as a Spanish intelligence asset. He exhibited hallmark indicators of a *financial volunteer*—he suffered from substance abuse, money problems, and vindictiveness. Downing also volunteered to the "threat" in the news and went to the nearest diplomatic establishment. These same traits were repeated throughout the 112 years covered in this study by financial volunteer spies.

Lessons Learned

The lack of a counterintelligence entity within the DON was tempered by the fact that Downing was no longer in the Navy, the rapid and effective wartime reorientation of the Secret Service from forgery crimes to counterintelligence, and the overall incompetence of the Spanish espionage effort. The Secret Service's coverage of Spanish espionage activity outside the United States was particularly noteworthy and was the key to solving the Downing case effectively. Downing is the only U.S. naval espionage case considered in this study to be intercepted through physical surveillance of an adversary's diplomatic presence.

[15] *Acts and Resolutions of the Third Session of the Thirty-Seventh Congress* (Washington, DC: Government Printing Office, 1863), 132; "Senor Carranza's Letter," *New York Times*, 5 June 1898; and "Letter from U.S. Secretary of War Russell A. Alger to U.S. Secretary of State John Sherman regarding disposition of personal effects of George Downing, 6 July 1898," RG 59: General Records of the Department of State, Series: Letters Received, File Unit: M179–Miscellaneous Letters of the Department of State, 1789–1906, NAID: 153522163, NARA, 166.

Tensions in the Pacific

Between 1884 and 1899, German colonialism spread across the Central Pacific, directly rivaling U.S. influence in the region. Germany established protectorates over northwest New Guinea and New Britain in 1884, and the Caroline, Palau, Marshall, and northern Solomon Islands were placed under German protection in 1886. In 1889, Germany, the United States, and the United Kingdom established a joint protectorate over Samoa, but later that year, amid a civil war, Germany and the United States divided Samoa east and west.[16]

In 1898, with the surrender of the Spanish to U.S. forces in the Philippines and on Guam, Germany rushed to fill the void, dispatching an Imperial German Navy squadron from China to Luzon just a few days later. Several days after the Battle of Manila Bay, the U.S. ambassador in London, John M. Hay, forwarded intelligence he had received that Germany "might seek to complicate the question with Samoa or Philippine Islands." To stave off the Germans, the United States claimed both the Philippines and Guam. The following year, in 1899, Germany purchased the Caroline, Mariana, and Palau Islands from Spain, theoretically placing German forces astride U.S. lines of communication between the Philippines and the West Coast of the United States.[17]

The sudden arrival of the United States in the Western Pacific in 1898 was a shock to the Germans. According to Vanderbilt University history professor Holger H. Herwig in 1976, "The United States was now regarded [by Germany] as a most dangerous competitor in the pursuit of colonial possessions and naval coaling stations." Germany's

[16] Kees van Dijk, *Pacific Strife* (The Netherlands: Amsterdam University Press, 2015), 122, 140, 143, 174.

[17] "Telegram from U.S. Ambassador to the United Kingdom John M. Hay to William Hay, 3 May 1898," RG 59: General Records of the Department of State Series: Despatches from Diplomatic Officers, File Unit: Despatches from U.S. Ministers to Great Britain, 1791–1906, Item: Volume 192: May 2–July 18, 1898, NAID: 188587078, NARA, 7; and Van Dijk, *Pacific Strife*, 389, 393, 409.

political and military leaders therefore turned their attention to the likelihood of an armed clash with this new rival. By the early 1900s, German naval planning included attacks on the U.S. East Coast and Puerto Rico as well as identifying forward naval bases called *stutzpunkte* that girdled the globe to facilitate their operations.[18] Officers from both sides agreed by 1903 that "the next war between great powers would be between the United States and Germany." While the consensus of both navies was that the war would be fought over German attempts to expand into the Caribbean and South America, the Pacific would continue to figure in the anticipated conflict.[19]

Within that tense German-American naval rivalry, a former German sailor appeared at a U.S. Marine Corps recruiting office in Detroit, Michigan, offering to enlist.

1909: Kurt Albert Jahnke

Background

Kurt Albert Jahnke was a 21- to 27-year-old German citizen who enlisted in the Marine Corps in Detroit in March 1909. His true date of birth remains a mystery. Jahnke completed basic training at the Marine Barracks aboard Mare Island Naval Shipyard in Vallejo, California. The Marines then assigned Jahnke to Naval Station Pearl Harbor, from where he deployed to the Philippines. In November 1909, he

[18] Holger H. Herwig, *Politics of Frustration: The United States in German Naval Planning, 1889–1941* (Boston, MA: Little, Brown, 1976), 29, 36–38, 42, 85–86. In an echo of history, the early 1900s German *stutzpunkte* or "base points" concept is similar to the People's Republic of China's early-2010s "strategic strong point" concept, as articulated in Conor M. Kennedy "Strategic Strong Points and Chinese Naval Strategy," Jamestown Foundation *China Brief* 19, no. 6 (22 March 2019).

[19] Alfred Vagts, "Hopes and Fears of an American-German War, 1870–1915," *Political Science Quarterly* 54, no. 4 (December 1939): 514–35, https://doi.org/10.2307/2143442.

Figure 4. Kurt Albert Jahnke

Source: Bain News Service Photograph Collection, Prints and Photographs Division, Library of Congress, Washington, DC.

Former Marine Corps private Kurt Albert Jahnke, ca. 1919.

contracted malaria, and the Marines discharged him in February 1910 after only 11 months of service.[20]

[20] "Albert Kurt Jahnke: Request for Marine Corp [*sic*] Records of," Bureau of Investigation, Department of Justice, 27 April 1923, 106 (author's records received per FBI Freedom of Information/Privacy Act request #240); and Henry Landau, *The Enemy Within: The Inside Story of German Sabotage in America* (New York: G. P. Putnam's Sons, 1937), 102.

Apparently an experienced maritime Pacific hand, Jahnke had previously served in either the Imperial German Navy or merchant marine, and in 1903 he reportedly worked for the Imperial Maritime Customs Service, an international organization that managed Chinese ports from 1861 to 1949.[21]

Initiation and Espionage

In 1996, Richard B. Spence, an associate professor of history and department chair at the University of Idaho, wrote, "It is highly unlikely that Jahnke's emigration to the United States and his enlistment in the Marine Corps were personal decisions. Probably he was acting, formally or informally, as an agent of German naval intelligence, the Marine *Nachrichtenstelle* or 'N-Stelle,' which had a vital interest in American naval activities in the Pacific. The suspicion that Jahnke was on an intelligence-gathering mission is strengthened by his immediate return to Germany following his discharge, likely for debriefing."[22]

Investigation and Punishment

There was no known investigation of Jahnke's potential espionage during his service in the Marine Corps. If Spence is correct, Jahnke would be the first example of what can be termed *patriotic penetrations*. A mixture of patriotism and self-interest generally motivated this type of espionage. An agent's native country's intelligence service generally recruited the agent and assigned them the task of penetrating a specific foreign organization by joining that institution. Almost universally among the cases considered in this study, patriotic penetration agents held low-level positions with little or no access to classi-

[21] Richard B. Spence, "K. A. Jahnke and the German Sabotage Campaign in the United States and Mexico, 1914–1918," *Historian* 59, no. 1 (Fall 1996): 89–112; and Immanuel C. Y. Hsu, *The Rise of Modern China* (London: Oxford University Press, 1970), 329–31.

[22] Spence, "K. A. Jahnke and German Sabotage Campaign in the United States and Mexico," 89–112.

fied information. They also tended to have had life experiences rather than enlisting or applying for employment immediately after completing their initial education.

Significance

If Spence's assessment is correct, Jahnke was a strategically insignificant, militarily ineffective patriotic penetration of the DON. Unfortunately, there is no record of any investigation into Jahnke by the department to confirm Spence's assessment.

Lessons Learned

The most important aspect of the Jahnke case is that the lack of a counterintelligence entity within the DON left it wide open to espionage.

Stolen Ship Plans

The second early modern case brief shows the timelessness of certain types of espionage. In the early twentieth century, as the U.S. Navy became technologically comparable to its European counterparts, it also became an espionage target for countries seeking an *unexpected manner advantage*. In the early twenty-first century, it is the military/naval wing of the Chinese Communist Party (CCP), the People's Liberation Army Navy, that has sought to become technologically comparable to the U.S. Navy. In 2018, hackers from the CCP's Ministry of State Security pursued the same *unexpected manner advantage* and compromised gigabytes of data about U.S. Navy submarines.[23]

One hundred and five years earlier, another espionage case presaged modern-day concerns about the theft of sensitive technological

[23] *Military Power of the People's Republic of China 2009: Annual Report to Congress* (Washington, DC: Department of Defense, 2009), 52; and Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, 8 June 2018.

Figure 5. USS *Pennsylvania* (BB 38)

Source: Bain News Service Photograph Collection, Prints and Photographs Division, Library of Congress, Washington, DC.

USS *Pennsylvania* (BB 38) was launched at the Newport News Shipbuilding Company, VA, in March 1915, two years after its design was compromised by an unidentified spy.

information. While the two cases employed vastly different methods, the same basic premise applies, in that adversaries will steal sensitive technology left inadequately protected. This was true in 1913 and in 2018, and it will be true in the future.

However, naval counterintelligence improved immensely in the 105 years between 1913 and 2018. In 2018, naval counterintelligence identified the perpetrator and the information stolen and negated any *unexpected manner advantage*. In 1913, the DON never identified the perpetrator, and the leadership contemplated the need for counter-intelligence.

1913: USS Pennsylvania *Blueprints*

Background

In 1913, the U.S. Navy was building one of the largest warships in its history, the battleship USS *Pennsylvania* (BB 38). Draughtsmen in the Navy's Bureau of Steam Engineering and Bureau of Construction and Repair were in the final stages of the ship's design. The plans were stored in the Navy building, now the Eisenhower Executive Office Building, next to the White House.[24]

Initiation and Espionage

The first theft occurred on the night of 4 March 1913, the day of newly elected President T. Woodrow Wilson's inauguration. The room where the DON stored the *Pennsylvania* blueprints offered a view of the fireworks that evening, and the department allowed employees to bring their families into the building to watch the display. The plans, which a worker had left on a drafting table, were gone the next morning.[25]

Investigation

The DON immediately suspected an insider, and further missing documents confirmed these suspicions. Without an organic investigative capability, the department hired a private detective company, the Burns Detective Agency, and called in detectives from the Bureau of Investigation. The department kept the thefts secret to aid the investigation, but the news broke two months later. The thefts stopped, and the DON never identified the perpetrator.[26]

---

[24] *Hearings on the Proposed Reorganization of the Navy Department before the Committee on Naval Affairs of the House of Representatives* (Washington, DC: Government Printing Office, 1910), 61, 67; and "Thief Gets Vital Battleship Plans," *New York Times*, 14 May 1913, 1.
[25] "Battleship Plans Were Taken," *Hartford (CT) Courant*, 14 May 1913, 1.
[26] "Many Thefts of U.S. Navy Plans," *Perry County (PA) Times*, 22 May 1913, 2; and "Thief Gets Vital Battleship Plans."

The DON required that the draughtsmen file the *Pennsylvania* blueprints in a "confidential design locker."[27] However, while the department first stipulated the handling of information termed *confidential* in 1909, officials used the word in its common sense, not as a prescribed protective marking.[28] Moreover, the United States would have no workable espionage law for another five years. Consequently, a naval counterintelligence agency, if one had existed, would have had limited legal authority to react to the thefts.

Significance

This case may have been strategically significant and militarily ineffective because an unknown adversary may have gained an *unexpected advantage*. Fortunately, the perpetrators stole the original blueprints vice making surreptitious copies, so the advantage was discovered and was not unexpected.

Lessons Learned

As with the Jahnke case, the most important aspect of this case was the lack of a naval counterintelligence entity. Because this case highlighted the theft of information that the DON desired to remain confidential, the case also highlighted that any counterintelligence entity would need a system of security classifications and legal authorities to be effective.

Stolen Code Book

The third case brief during this period occurred just before the United States entered World War I. The war began in Europe in 1914, primar-

---

[27] "Preliminary Design No. 102: Pennsylvania," 21 November 1913 (photo no. S-584-41, Naval History and Heritage Command, Washington, DC).
[28] Dallas Irvine, *Origin of Defense-Information Markings in the Army and Former War Department* (Washington, DC: National Archives and Records Service, 1972), 43.

ily pitting France, the United Kingdom, and Russia against Germany and Austria-Hungary. While vehemently neutral, the United States sold weapons to both sides, but increasingly to the British, French, and Russians. One month after this case began in 1915, the British ocean liner RMS *Lusitania* (1906) was sunk by a German submarine, killing 120 Americans. The attack solidified U.S. public opinion against Germany and started the United States on the path to a declaration of war in 1917.[29]

This case brief deals with communications security. This is largely invisible today, but the theft of codes and the machines used to encode communications is a constant across this study. Due to the *time and place advantage* that it provided to the Soviet Union during the Cold War, the most damaging espionage case in U.S. Navy history was that of the John A. Walker Jr. spy ring, which nearly exclusively compromised communications security information.[30] Today, the codes are software called electronic keys; in Walker's time, they were punch cards; in World War II, they were set into machines with dials; and from the Civil War through World War I, codebooks substituted letter for letter in a system known as manual or offline encryption.[31]

The theft of one of the thousands of codebooks issued across the U.S. Navy was the focus of this case. It was an extremely serious situation, as the United States contemplated entering World War I. With no counterintelligence service, the DON was again unable to identify a perpetrator, leaving officials to wonder which potential adver-

[29] Richard W. Stewart, ed., *American Military History*, vol. 2, *The United States Army in a Global Era, 1917–2008*, 2d ed. (Washington, DC: U.S. Army Center of Military History, 2010), 1–8; "The Lusitania Disaster," Library of Congress, accessed 8 November 2023; and "U.S. Entry into World War I, 1917," Office of the Historian, U.S. Department of State, accessed 8 November 2023.

[30] "John Walker," Federal Bureau of Investigation, accessed 2 September 2023.

[31] James V. Boone, *A Brief History of Cryptography* (Annapolis, MD: Naval Institute Press, 2005), 23, 39, 43, 62, 75, 92; and Capt Linwood S. Howeth, USN (Ret), *History of Communications-Electronics in the United States Navy* (Washington, DC: Bureau of Ships and Office of Naval History, Department of the Navy, 1963), 200.

Figure 6. Herbert A. Jones

Source: *Lucky Bag, 1907* (Annapolis, MD: U.S. Naval Academy, 1907), 68.

USS *Hull* (DD 7)'s commanding officer, Herbert A. Jones, as a midshipman at the U.S. Naval Academy in 1907.

Figure 7. Robert D. Kirkpatrick

Source: *Lucky Bag, 1913* (Annapolis, MD: U.S. Naval Academy, 1913), 116.

USS *Hull* (DD 7)'s executive officer, Robert D. Kirkpatrick, as a midshipman at the U.S. Naval Academy in 1913.

sary would have had a potentially campaign-winning *time and place advantage*. The Navy took no chances, and this case appears to have prompted the creation of the first U.S. naval counterintelligence effort.

1915: USS Hull Codebook

Background

In April 1915, the U.S. Navy discovered that a copy of the *Battle Signal Book* belonging to the destroyer USS *Hull* (DD 7) was missing. This publication was issued to each Navy ship starting in 1913. Marked "Strictly Confidential" and registered with a serial number, the *Battle Signal Book* was issued under a letter of promulgation that stated, "The most important function of this code is that of a secret radio code for

tactical and battle orders." However, the book also contained traditional flag signals to be used during maneuvers.[32]

Investigation and Punishment

As a result of the loss of the publication, the Navy conducted a court martial for *Hulls*'s commanding officer, Lieutenant Herbert A. Jones, and executive officer, Ensign Robert D. Kirkpatrick. In March 1916, both officers were found guilty of "culpable negligence and inefficiency in the performance of duty" for "losing a Battle Signal Book." However, in July 1916, Jones and Kirkpatrick's punishments were reduced from the loss of 100 numbers on the promotion list to the loss of 10 numbers.[33] The DON never recovered the missing book, so the Navy revised and reissued 4,500 copies of the publication later in 1916.[34]

Bureau of Investigation detectives launched an investigation into a Japanese citizen and a Philippines citizen serving as civilians aboard *Hull*. However, the Navy decided not to question them during the court martial.[35] The presiding officer of the court martial noted, "I do not think the Japanese figure in this matter at all."[36] The results of the Bureau of Investigation inquiry are unknown but were likely unproductive.

---

[32] *United States Navy Regulations, 1920* (Washington, DC: Navy Department, 1920), 234; Howeth, *History of Communications-Electronics in the United States Navy*, 200; "Navy Code Book Gone," *Washington Post*, 4 February 1916, 3; and LCdr Harry E. Yarnell, USN, "Notes on Naval Tactics," U.S. Naval Institute *Proceedings* (January 1916). Yarnell describes the *Battle Signal Book* as filled with "descriptions of obsolete and useless maneuvers" that should be revised and declassified.

[33] "26251-11581 Kirkpatrick, Robert D.," RG 125: Records of the Office of the Judge Advocate General (Navy), File Unit: Kirk, Series: Card Index to U.S. Navy General Court Martial Files, NAID: 117397108, NARA, 245–46; and "26251-11580 Jones, Herbert A.," RG 125: Records of the Office of the Judge Advocate General (Navy), File Unit: Jones H, Series: Card Index to U.S. Navy General Court Martial Files, NAID: 117387338, NARA, 83–84.

[34] *Compilation of Court Martial Orders, 1916–1937*, vol. 1, *1916–1927* (Washington, DC: Navy Department, 1940), 11–12; and *Annual Report of the Public Printer for the Fiscal Year Ended June 30, 1917* (Washington, DC: Office of the Public Printer, 1917), 187.

[35] "Code Book Trial Ends," *Washington Post*, 13 February 1916, 4.

[36] "Who Lost Code Book?," *Topeka (KS) State Journal*, 12 February 1916, 5.

Significance

The *Hull* case appears to have had a role in convincing DON leaders to establish an organic counterintelligence entity. Because there was no resolution to the case, the department had no idea what country may have achieved a *time and place advantage* from the compromise or how it would impact the Navy in wartime. Fortunately, the advantage was not unexpected because the perpetrators stole the original code book vice copying it.

Lessons Learned

As with the theft of the *Pennsylvania* blueprints, the Navy's first loss of signaling material was unsolved, and the *Hull* codebook case again forced the Navy to think about creating an organic investigative arm. Without directly referencing the ship plans or battle signal book thefts, in April 1917, as the United States entered World War I and 14 months after the *Hull* court martial concluded, the Secretary of the Navy, Josephus Daniels, tasked ONI to begin counterintelligence investigative duties.[37]

Signals Intelligence and Counterintelligence

The next case brief was not well documented but was nevertheless significant. Mentioned briefly in an overview of U.S. naval intelligence, the corresponding case file remains elusive. While the subject of this case appears to have been an asset of German intelligence, the information he compromised was unknown. The Navy's reaction to the case, reassignment, was typical of the period and did nothing to identify an *unexpected advantage*.

---

[37] Packard, *A Century of U.S. Naval Intelligence*, 248.

1916: The Unidentified Chief Petty Officer

Background

By 1916, World War I had been raging in Europe for two years, and U.S. involvement appeared to be very possible. The DON's new counterintelligence element was already moving far beyond just investigating the Navy, as the new ONI remit included investigating a wide variety of subversive activities in civilian ports across the country. ONI, rapidly expanded with unqualified amateurs, opened a vast number of spurious investigations based primarily on the ethnic heritage of the subjects.[38]

However, prior to the U.S. entry into World War I, one case appears to have had merit. While the historical record is silent on the full identity of the subject of this investigation, a summary suggests that Navy officials suspected him of providing information to German intelligence because of his German ethnic background. The subject, a chief petty officer, was serving aboard a battleship in the U.S. Atlantic Fleet, spoke German fluently, and associated with Germans while on liberty.

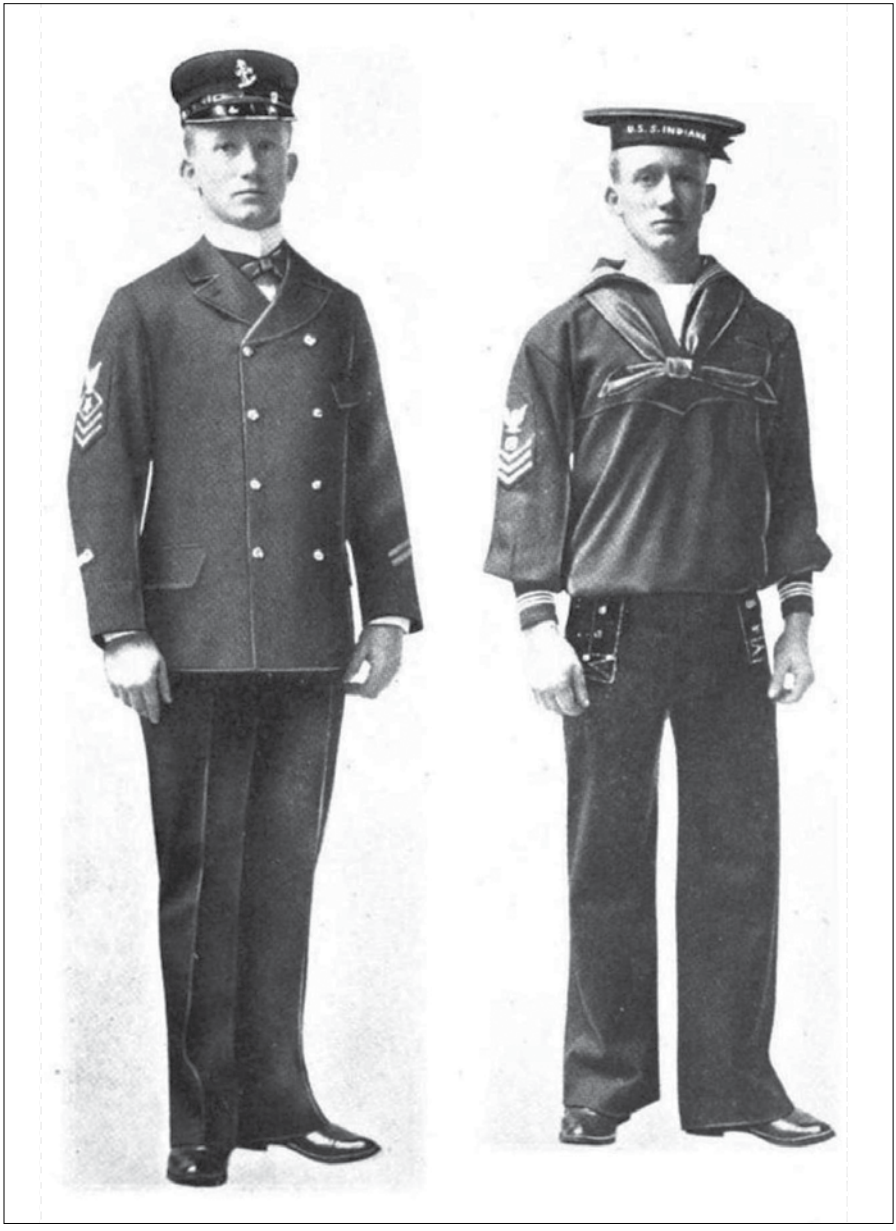
Investigation and Punishment

To investigate its suspicions, ONI assigned an agent as a yeoman aboard the chief's ship. The ONI agent befriended the subject and went on liberty with him. However, despite being convinced that the chief was assisting German intelligence, the ONI agent could not gather enough evidence to warrant an arrest. Instead, ONI arranged the subject's transfer ashore, away from sensitive material.

However, in April 1917, just after the United States entered the war, signals intelligence intercepted a telegram that confirmed the subject

[38] Packard, *A Century of U.S. Naval Intelligence*, 251; Jeffery M. Dorwart, *Conflict of Duty: The U.S. Navy's Intelligence Dilemma, 1919–1945* (Annapolis, MD: Naval Institute Press, 1983), 8–9; and Nathaniel Patch, "The Story of the Female Yeomen during the First World War," *Prologue* 38, no. 3 (Fall 2006).

Figure 8. Unidentified U.S. Navy chief petty officer



Source: Uniform Regulations, United States Navy (Washington, DC: Navy Department, 1917) plate 20.

The unidentified U.S. Navy chief petty officer in 1917 is represented by this uniform illustration. This is a representative image and not the actual espionage suspect.

was an asset of German intelligence. This was the first time that the DON used signals intelligence to identify an espionage suspect. The ultimate disposition of this case is unknown.[39]

Significance

The unidentified chief was a strategically insignificant, militarily ineffective case that demonstrates that the best way to find a spy was for the foreign intelligence service to compromise their own asset through signals intelligence. The DON neutralized the espionage before the war but had no idea what *unexpected advantage* Germany may have gained.

Lessons Learned

Predicated on signals intelligence, ONI had solid evidence of the chief's espionage but, due to the sensitivity of the information, such evidence was nearly impossible to use in court, and the DON had no legal leverage to extract a full confession. That would not change for more than 60 years, until the passage of the Classified Information Procedures Act in 1980 ensured the security of classified evidence presented in court.[40]

ONI's use of an undercover agent was a good investigative step that should have developed additional leads, most importantly information leading to the identity of the chief's German handler or his method of communicating with German intelligence. Apparently, the chief was too cautious to reveal anything to his new liberty partner.

Unlike Jahnke, who may have been a patriotic penetration, the chief was most likely what is referred to as a *recruitment-in-place*. While a patriotic penetration attempts to create access to information by joining an organization, a recruitment-in-place sees foreign intelligence

[39] Packard, *A Century of U.S. Naval Intelligence*, 250.
[40] Classified Information Procedures Act, Pub. L. No. 96-456, 94 Stat. 2025 (1980).

seek out a spy for their existing access to specific information of interest. This asset usually meets the intelligence officer through a legitimate interaction, such as the chief's German liberty associates. Then, once the intelligence officer realizes their placement, access, and, most importantly, motivation, the recruitment process begins. Like a patriotic penetration, recruitments-in-place usually receive specific tasks and provide just that information to the foreign intelligence service.

Counterintelligence Support to Force Protection

Until it was cancelled due to the COVID-19 pandemic in March 2020, exercise Defender-Europe 2020 was intended to test the ability of the U.S. Department of Defense's logistics system to move a division-size Army force from the United States to Europe in an emergency—one division.[41] Between April 1917 and November 1918, a period of 18 months, the United States created and transported 42 Army divisions across the Atlantic to Europe to serve in World War I.[42] While a massive German submarine offensive managed to sink several transports, killing nearly 400 soldiers, approximately 2 million soldiers crossed the "Atlantic Bridge" safely.[43]

Based at the receiving end of the Atlantic Bridge, this next case brief demonstrates how a counterintelligence service can interdict espionage before it results in an *unexpected advantage*. This case brief

[41] "Defender-Europe 20 Exercise," U.S. Embassy and Consulate in Poland, 30 January 2020.
[42] *The U.S. Army in the World War I Era* (Washington, DC: U.S. Army Center of Military History, 2017), 6, 66.
[43] Frank A. Blazich Jr., *United States Navy and World War I: 1914–1922* (Washington, DC: Naval History and Heritage Command, 2020), 139, 170, 205; Samuel J. Cox, "The Contribution of the U.S. Navy during World War I," Naval History and Heritage Command, November 2018; and "Cable Number 577, General John J. Pershing, USA, to General Tasker H. Bliss, U.S. Army Chief of Staff, 6 February 1918," RG 120: Records of the American Expeditionary Forces (World War I), Series: Confidential Cablegrams Sent from General John J. Pershing to the Adjutant General, NAID: 209257222, NARA.

also foreshadows the overseas mission of today's U.S. naval counterintelligence, as ONI agents worked closely—and delicately—with their French allies to uncover German espionage threats to the U.S. Navy and Merchant Marine forces involved in the transportation effort. The combined French and ONI investigations during 1917–18 indicated that despite the Germans' best efforts, their targeting effort did not extend ashore. The German submarines sank ships, but only after they departed France and were mostly empty.[44]

1917: Josephine Alvarez and Victorine Faucher

Background

Unlike today, during World War I, troops traveled overseas by ship, not aircraft. This exposed them to the deadliest German naval weapon of the time—the submarine (U-boat). As in World War II and during the Cold War, the U.S. Navy's primary task in World War I was to safely transport 2 million troops and their supplies and equipment across the Atlantic Ocean and past a hostile submarine fleet.[45]

Despite that threat, ONI agents blanketed ports along the U.S. East Coast looking for German saboteurs, not intelligence collectors who could vector German submarines onto the packed troopships. U.S. troops crossing the Atlantic primarily landed in the United Kingdom and France. One major port of debarkation was Saint-Nazaire in France. German intelligence wanted information from these ports for two reasons: first, to track the arrival of U.S. units; and second, to provide targeting information to German submarines along the French coast. By slowing the arrival of U.S. forces into the theater, the Germans hoped to force a favorable negotiated peace before those rein-

[44] Cox, "The Contribution of the U.S. Navy during World War I."
[45] "Espionnes fusillées [Spies Shot]: Joséphine Alvarez–Victorine Faucher," *Guillotine* (blog), 8 February 2012; and "Lt. C. A. Munn," World War I Investigative Files, Formerly Confidential General Correspondence, 1913–1924, File 25100-603, Box 91, Entries 78 and 78A, RG 38: Records of the Office of the Chief of Naval Operations, NARA.

Figures 9 and 10. Victorine Faucher and Josephine Alvarez

Source: "Espionnes fusillées [Spies Shot]: Joséphine Alvarez–Victorine Faucher," *Guillotine* (blog), 8 February 2012.

Victorine Faucher (left) and Josephine Alvarez, ca 1917.

forcements allowed the Allies (France, the United Kingdom, and the United States) to defeat them.[46]

Initiation and Espionage

ONI was concerned about German agents such as Josephine Alvarez and Victorine Faucher. These two women, variously described as petty thieves, prostitutes, and poets, were fugitives based on a 1916 theft conviction in Paris. They fled across the border into northern Spain and traveled to Barcelona.[47]

There, destitute, they encountered a German who was running an espionage operation into France. Spain was a neutral country during the war, and both sides ran intelligence operations from there. Seizing on the ability of Alvarez and Faucher to speak French and blend into French society, the Germans recruited the two women and paid them the equivalent of nearly $20,000 (USD) today to return to France and report on troop arrivals in Saint-Nazaire. However, a French

[46] "Lt. C.A. Munn"; and *Charles Munn: Blindfolding the Hun*, Office of Naval Investigation Attaché Report, File 10848, Box 704, RG 38: Records of the Office of the Chief of Naval Operations, NARA.

[47] *Charles Munn: Blindfolding the Hun.*

double-agent operation had penetrated the German operation and, due to the Germans' poor compartmentalization and separation of disparate agent operations, the double agent was able to identify Alvarez and Faucher.[48]

Investigation and Punishment

Alvarez and Faucher arrived in Saint-Nazaire in September 1916 and almost immediately ran into trouble with the police. They abandoned their mission and went underground, running through the Germans' money quickly. The pair evaded capture for five months before French authorities located them and placed them under surveillance. Now penniless, they attempted to escape back to Spain, but French authorities arrested them in March 1917, just weeks before the United States entered the war and a few months before the first U.S. transports arrived in Saint-Nazaire. A French military court found Alvarez and Faucher guilty of espionage, and a firing squad executed them in April 1918.[49]

By October 1917, U.S. troopships were pouring into Saint-Nazaire to deliver thousands of soldiers and Marines, and the German submarines found a well-stocked hunting ground. That month, German submarines attacked five empty convoys as they departed Saint-Nazaire en route to the United States for another load of cargo and troops. In the wake of the Alvarez and Faucher case, the Navy asked the French authorities for an investigation of possible German coastwatchers providing targeting information to the submarines.[50]

In response, ONI dispatched what would become the equivalent of a modern-day force protection detachment. Under the direction of U.S.

---

[48] *Charles Munn: Blindfolding the Hun*; and "Letter from the Naval Attaché, American Embassy, Paris, to the Director of Naval Intelligence, 18 April 1918: Espionnage [*sic*] on Western Coast of France," RG 38: Records of the Office of the Chief of Naval Operations, Naval Attache Reports, C-10-g,10203: Espionage on Western Coast of France, NAID: 196036073, NARA.
[49] *Charles Munn. Blindfolding the Hun.*
[50] *Charles Munn: Blindfolding the Hun.*

Figure 11. Charles Munn

Source: *War Records of the Knickerbocker Club, 1914–1918* (New York: Knickerbocker Club, 1922), 242.

U.S. Navy Reserve lieutenant Charles Munn, ca. 1917.

Navy Reserve lieutenant Charles Munn, a wealthy, French-speaking Harvard graduate, ONI agents, cooperating closely with French military counterintelligence, investigated dozens of suspicious incidents but never found another case like that of Alvarez and Faucher.[51]

Munn was typical of ONI agents during the war. Recruited from the upper class of urban America, he was married to an heiress, vacationed in Europe, and was independently wealthy. After the war, he self-published a short book about his wartime experiences and returned to high society in the United States.[52]

Significance

Alvarez and Faucher were strategically insignificant, militarily efficient recruitments-in-place. While they did not penetrate the ranks of the U.S. Navy, they did penetrate wartime France and a vital port of debarkation, but French counterintelligence interdicted them before they could compromise information about U.S. troop arrivals and give the Germans an *unexpected advantage*.

Lessons Learned

While it did not uncover any further German espionage, Munn's force protection mission was a watershed event in the history of naval counterintelligence. Moreover, the French investigation demonstrated that penetrations of adversary intelligence services was a valuable way to identify spies.

[51] *Charles Munn: Blindfolding the Hun*; and *War Records of the Knickerbocker Club, 1914–1918* (New York: Knickerbocker Club, 1922), 242.
[52] *Charles Munn: Blindfolding the Hun*; and Bill Boldenweck, "Charles A. Munn," *San Francisco (CA) Examiner*, 15 March 1981, B7.

Tragedy of Ethnic Profiling

The final case brief from this period takes place in Hawaii just as the United States entered World War I. After the *Lusitania* sinking in 1915 turned public opinion against Germany, official and unofficial discrimination and ethnic profiling targeting German-Americans grew rampant. From renaming sauerkraut "liberty cabbage" and the confiscation of German-language texts to the mob violence that ended with the lynching of German immigrant Robert P. Prager in Collinsville, Illinois, in 1918, World War I was an inflection point for Americans of German heritage. In fact, on 17 April 1917, President Wilson signed a classified Executive Order that authorized the firing of any civil servant based on a confidential record of "sympathies or utterances, or because of other reasons growing out of the war."[53]

Ethnic profiling and discrimination also extended into the DON and into the ONI's counterintelligence investigations. This massive misstep launched thousands of spurious investigations, wasted resources, and scapegoated innocent servicemembers and civilian employees.[54]

In addition, the lack of formal classification markings, a workable espionage law, and vague to nonexistent authorities further hampered ONI's misguided efforts. ONI investigators conducted investigations limited only by their own initiative and force of personality, which

[53] "The Lusitania Disaster"; Frank Trommler, "The *Lusitania* Effect: America's Mobilization against Germany in World War I," *German Studies Review* 32, no. 2 (May 2009): 241–66; Elspeth H. Brown, "Erasing the Hyphen in German American," *Reviews in American History* 33, no. 4 (December 2005): 527–32, https://doi.org/10.1353/rah.2005.0064; "Cabinet Meeting Takes up Collinsville Lynching," *St. Louis (MO) Post-Dispatch*, 5 April 1918, 1; "Bonfire of German Literature in Cleveland Not to Be Held," *St. Louis (MO) Post-Dispatch*, 5 April 1918, 3; "Confidential Executive Order dated April 7, 1917," RG 60: General Records of the Department of Justice, Series: Copies of Executive Orders, File Unit: March 13, 1917–December 26, 1917, NARA, 27–29; and Peter Stehman, "Lynching of Robert Prager (1918)," Madison Historical: The Online Encyclopedia and Digital Archive for Madison, Illinois, accessed 21 August 2021.

[54] Dorwart, *Conflict of Duty*, 8–9.

confused prosecutions. Based on little more than hearsay about alleged German sympathies, the DON largely resorted to dishonorable discharges for active duty servicemembers and dismissals for civilian employees.[55] The situation was so poor that in 1924, the director of ONI publicly admitted, "During the war we necessarily had thousands of agents whose business was to guard against spies and traitors. This was a war condition under which the just suffered with the unjust, for of course many ludicrous mistakes were made by amateur agents."[56]

In the process, the mostly untrained and inexperienced ONI investigators missed important investigative angles and, in the end, prosecuted only one espionage case during World War I. The U.S. Department of Justice (DOJ) prosecuted this case under the March 1911 Defense Secrets Act. Despite glaring problems with this law, the subject pled guilty although he likely could have successfully defended himself.[57]

This case brief demonstrates how a counterintelligence investigation can result in prison time yet still be militarily ineffective because it fails to identify the *unexpected advantage*.

1917: George Roenitz

Background

Like the unidentified chief petty officer, George Roenitz came under suspicion primarily because he was ethnic German. In February 1917, Roenitz was chief clerk of the Pearl Harbor Naval Station in Hawaii.

[55] Wayne Goldstein, "The Office of Naval Intelligence: A Proud Tradition of Service," in *A Counterintelligence Reader*, ed. Frank J. Rafalko (Washington, DC: National Counterintelligence Center, 1998); Eric Setzekorn, "The Office of Naval Intelligence in World War I: Diverse Threats, Divergent Responses," *Studies in Intelligence* 61, no. 2 (June 2017): 43–54; and Patch, "The Story of the Female Yeomen during the First World War."

[56] Capt Luke McNamee, USN, "Naval Intelligence," U.S. Naval Institute *Proceedings* 50, no. 9 (September 1924). This quote is part of a lecture delivered by Capt Luke McNamee, director of naval intelligence, aboard USS *Henderson* (AP 1) at the Washington Navy Yard on 9 March 1923.

[57] Defense Secrets Act of 1911.

Figure 12. George Roenitz

Source: National Archives and Records Administration, College Park, MD.

George Roenitz, 1922.

He was a naturalized U.S. citizen, had lived in Hawaii for decades, and had been working at the naval station for 12 years.[58]

[58] Sandra E. Wagner-Seavey, "The Effect of World War I on the German Community in Hawaii," *Hawaiian Journal of History* 14 (1980): 109–40; and "Memo from the Aid for Information to the Director of the Office of Naval Intelligence, dated July 2, 1918: Subject: George Roenitz," World War I Investigative Files, Formerly Confidential General Correspondence, 1913–1924, File 20940-11, Box 1, Entry 78A, RG 38: Records of the Office of the Chief of Naval Operations, NARA.

A new base commander took over in August 1916 and unsuccessfully attempted to fire Roenitz for undocumented "suspicions." Then, in February 1917, Secretary of the Navy Daniels authorized Roenitz's firing as part of a blanket order to dismiss all German-born employees of the DON. However, a month later the secretary canceled the order because it violated civil service regulations.[59]

Investigation and Punishment

In the meantime, Roenitz found new work as a steward aboard passenger ships and traveled between Manila, Philippines; Hawaii; and San Francisco, California. While Roenitz was at sea, the local ONI agent entered his room in a boarding house and searched his belongings. Among them, he found several Navy related photographs and documents including two "confidential" documents.[60]

ONI interviewed Roenitz in Manila and he admitted to taking the documents, claiming that he had accidentally mixed them up with his personal papers. The DOJ dropped most of the charges against Roenitz because the investigation had not revealed any passage of information to a foreign power. However, Roenitz did plead guilty to violating the 1911 Defense Secrets Act for possessing defense information to which he was not entitled and was sentenced to the maximum penalty of one year.[61]

There was speculation that the entire prosecution was financially motivated. Roenitz was a vice president of a German-owned sugar

[59] "Memo from the Aid for Information to the Director of the Office of Naval Intelligence, dated July 2, 1918: Subject: George Roenitz."
[60] "Former Naval Clerk Held as German Spy," *San Francisco (CA) Examiner*, 23 May 1917, 8; and "Memo from the Aid for Information to the Director of the Office of Naval Intelligence, dated July 2, 1918: Subject: George Roenitz."
[61] Wagner-Seavey, "The Effect of World War I on the German Community in Hawaii"; and "Memo from the Aid for Information to the Director of the Office of Naval Intelligence, dated July 2, 1918: Subject: George Roenitz."

company. After his arrest and the entry of the United States into World War I, the DOJ seized the company and sold it to its competitors.[62]

Significance

Roenitz was a strategically insignificant, militarily ineffective case that was likely not espionage at all.

Lessons Learned

Predicated on the rampant, officially sanctioned ethnic profiling of the period, the case against Roenitz was questionable due to the extralegal search of his residence by ONI, which also failed to coordinate its inquiries with the DOJ. Another problem with the Roenitz case was that the Defense Secrets Act of 1911 required only illegal possession of protected information, not transmission of that information to a foreign power, to secure a conviction. As a result, investigators had little motivation to identify any *unexpected advantage* that Roenitz may have secured for an adversary. This left the DON unable to take any potentially important remedial action.

Development of U.S. Naval Counterintelligence, 1898–1918

Seven significant espionage cases occurred within the DON during the years between the start of the Spanish-American War and the end of World War I. Drawing conclusions from such a small sample is difficult, but some inferences are possible. These cases involved information that spanned all three of the basic elements of naval warfare: shore establishments, weapons, and command and control. Only sensors,

[62] Christopher Capozzla, *Uncle Sam Wants You: World War I and the Making of the Modern American Citizen* (Oxford, UK: Oxford University Press, 2008), 189.

which had remained largely unchanged since the days of sail, were untouched by espionage.

The Downing case was an ineffectual one-off specific to the Spanish-American War but indicative of the predominant form of espionage that the DON would face for the next century: financial volunteers. The Jahnke, Roenitz, and unidentified chief cases, if they were indeed German espionage, all occurred within six years before the U.S. entry into World War I and appeared designed to acquire information from within the DON's shore establishments in both the Atlantic and Pacific to gain *time and place advantages* should the United States and Germany go to war as predicted by both sides. With this information, Imperial German Navy leaders could have been able to better assess the threat posed by the U.S. Navy.

With the Alvarez and Faucher case, German intelligence pointedly aimed at gaining a *time and place advantage* over the introduction of U.S. ground forces into the European conflict. With this information, German military leaders could have been able to fine tune the time and location of their final offensives to crack the stalemate on the western front.

The USS *Pennsylvania* case appeared designed by an unidentified adversary, or even a potential ally, to acquire information about the latest weapons system destined for the U.S. Fleet. Because the external investigators never solved the case, the DON was not able to determine if an adversary had gained a *manner advantage* from the espionage. While not tested in combat during World War I, this espionage could have allowed an adversary, probably Germany, or an ally, such as the United Kingdom, to assess the U.S. Navy's preparedness to fight a traditional naval force-on-force surface battle if the United States became involved in the war.

Finally, the USS *Hull* codebook case may have compromised elements of the U.S. Navy's command and control for nearly two years between 1915 and 1917, potentially giving an unidentified adversary

a tremendous *time and place advantage*. Because the external investigators never solved the case, the Navy leadership did not have a full understanding of which potential adversary had gained this critical advantage, and they were not able to fully grasp the damage done to the Navy's communications security efforts because the adversary codebreakers could dissect the techniques used to construct the code. Moreover, if the replacement encipherment system was based on those same techniques, then the unidentified adversary would have had an advantage breaking the new code. Fortunately for the Navy, the perpetrators bungled the espionage. Rather than steal the book outright, they should have copied it so the DON would not discover the compromise and change the code.

By 1917, as the United States crept toward entry into World War I, DON leaders faced the prospect that the Imperial German Navy may have had tremendous *time, place, and manner advantages* over the U.S. Navy. Worst case, the Germans could have been reading U.S. Navy communications for nearly two years, possessed the designs of the latest U.S. warships, and had insiders watching the U.S. Fleet's every move from critical shore establishments in both the Atlantic and Pacific. To make matters worse, the DON had no organic capability to resolve any of these issues and pled for assistance from the DOJ or hired private detectives. Faced with this array of espionage that could result in both strategic and tactical defeats, looming combat with the Imperial German Navy, and a general change in U.S. attitudes toward espionage, the DON cobbled together a counterintelligence capability, and by the end of World War I in 1918 the department had forged a nascent counterintelligence organization. Too little, too late—raw and often misguided, this early attempt at naval counterintelligence set the stage for the 1920s and 1930s as the world marched steadily toward another world war.

Lessons Learned

The World War I period generated several lessons learned that the DON largely failed to apply until after the end of World War II: first, that an organic investigative capability was necessary at all; second, that signals intelligence was a useful counterintelligence tool that generated leads for further investigation; third, that ethnic profiling was ineffective; fourth, that penetrations of an adversary intelligence service produced solid espionage leads; and fifth, that counterintelligence investigations required trained and experienced personnel.

Chapter 2
World War II Case Briefs, 1919–1945

Despite the best efforts of some politicians and diplomats, the 20 years following the end of World War I were simply a leadup to World War II. For the U.S. Navy, the period between the two wars was one of great change prompted mainly by the development of the airplane and, more specifically, the aircraft carrier. During those two decades, the U.S., British, and Japanese navies all worked diligently to build the capability to launch and recover warplanes at sea. Even more importantly, they determined how to accurately drop bombs from an aircraft and hit a moving ship. The navies of the world eventually settled on two ideas: the dive bomber, which dove nearly straight down at the ship to ensure that the bomb was heading in the right direction; and the torpedo bomber, which dropped a torpedo into the water aimed at the ship. Both required skilled pilots willing to brave antiaircraft fire.[1]

Together, groups of warships centered around the aircraft carriers that carried torpedo and dive bombers aboard were major innovations that reshaped naval warfare in the years leading up to World War II. Responsible for the destruction of four Japanese aircraft carriers at the Battle of Midway in June 1942, the U.S. Navy's Douglas SBD Dauntless dive bomber was a critical weapons system that turned the tide of the

[1] Cdr Jan M. van Tol, USN, "Military Innovation and Carrier Aviation: The Relevant History," *Joint Forces Quarterly* (Summer 1997): 77.

Pacific War in its first year.[2] Using the principle of surprise, aircraft carrier task forces and dive bombers were the *manner advantage* of the 1930s. Because they were the great naval warfare innovation of the time and presented a huge *manner advantage*, they became a significant espionage target as Japan, the United Kingdom, and the United States all sought to avoid being the victim of an *unexpected manner advantage*.

For the U.S. Navy, the theft of the USS *Pennsylvania* (BB 38) plans established this pattern of espionage in 1913. Naval leaders on all sides incorrectly believed that battleships were to be the great naval warfare innovation of World War I. Instead, it was the submarine, which remained a major espionage target throughout the Cold War and into the present.

The question for naval counterintelligence at this time should have been: What great naval warfare innovation provides the United States with a *manner advantage* that an adversary will seek to ensure is *not unexpected*? As the next series of case briefs demonstrates, naval warfare innovations were often an espionage target.

The first World War II period case brief starts with Japan seeking an aircraft carrier *manner advantage*. Later, using the same asset, the Imperial Japanese Navy (IJN) sought much more basic information about the locations and movements of the U.S. Pacific Fleet, a *time and place advantage*. The case began in 1923, 18 years before the Japanese attack on Pearl Harbor, Hawaii, and the U.S. entry into World War II.

1923: Frederick J. Rutland

Background

In 1923, Frederick J. Rutland was a married 37-year-old former British Royal Air Force (RAF) officer, a decorated World War I war hero, and

[2] Peter Smith, "Did the Dauntless Dive-Bomber Decide the Battle of Midway?," *History Hit*, 20 November 2019.

Figure 13. Frederick J. Rutland

Source: [British] National Archives, Japanese Intelligence Agents or Suspected Agents (KV2/337), Kew, Richmond, UK.

Former Royal Air Force squadron leader Frederick J. Rutland, 1933.

an expert in carrier aviation. After resigning his commission in 1923 and leaving the RAF, he ostensibly worked for the Japanese Mitsubishi Shipbuilding Company but was divulging sensitive information to assist with the development of Japanese carrier aviation. British intelligence was aware of his activities but legally powerless to stop him. In

Figure 14. Arata Oka

Source: [British] National Archives, Rutland, Frederick Joseph, Case PF 37996 Volume 6, (KV2/332), Kew, Richmond, UK.

Imperial Japanese Navy commander Arata Oka, ca. 1934.

1927, with his technical knowledge exhausted, Rutland returned to the United Kingdom and found work with an engineering firm in London.[3]

Initiation and Espionage

In 1932, with Japan's aircraft carrier program well underway, Japanese naval intelligence recruited Rutland to create an espionage network inside the United States. IJN commander Arata Oka, the Japanese naval attaché in London, served as Rutland's case officer.[4] Rutland made his first trip to the United States in 1933 and moved to Los Angeles, California, the following year. Living in Beverly Hills, Rutland spent vast sums of money to maintain his cover as a business executive while producing little information of value for the Japanese. Beginning in 1935, the Japanese repeatedly urged him to focus on Pearl Harbor, but he made only a few trips to Hawaii under the guise of seeking to establish a whiskey import business. British intelligence continued to track Rutland through intercepted Japanese diplomatic messages and via its own agents but only officially informed the U.S. Federal Bureau of Investigation (FBI) of the case in 1939.

In September 1939, an unidentified source, probably a British liaison officer, advised the FBI that Rutland was a Japanese intelligence asset and had been under investigation by the British for some time. A subsequent FBI investigation failed to develop any evidence of espionage. In July 1940, the United Kingdom's Security Service (MI5) fully informed the FBI of its extensive investigation of Rutland. Finally, in June 1941, resulting from the arrest in Los Angeles of IJN commander

[3] "Frederick Joseph Rutland, Spare Copy as Sent to SIS, undated," Records of the [British] Security Service Rutland, Frederick Joseph, Case PF 37996 Volume 11, British National Archives, Kew, Richmond, UK, KV-2-333.
[4] "Notes Comparing MI5 Information to Rutland Confession, undated," Records of the [British] Security Service, Rutland, Frederick Joseph, Case PF 37996 Volume 5, British National Archives, KV-2-331.

Itaru Tachibana for espionage, the FBI obtained evidence that Rutland was conducting espionage in the United States.[5]

Investigation and Punishment

In 1940, Rutland partially confessed to Office of Naval Intelligence (ONI) agents from the 11th Naval District about his relationship with the IJN and volunteered to report on Japanese activities. He strung ONI along for more than a year but provided no information of value.[6] However, the FBI's surveillance of Rutland led them to his contact, a Japanese naval officer also living in Los Angeles, whom the FBI arrested. In a panic, Rutland volunteered to serve the FBI, ONI, and British intelligence as a double agent. Fearing a diplomatic flap, the British quickly repatriated Rutland.[7] After the Japanese attack on Pearl Harbor in December 1941, British authorities interned him as an enemy collaborator until December 1943. Rutland committed suicide in 1947.[8]

Significance

Like Jahnke in 1909 and the unidentified chief in 1916, Rutland was a recruitment-in-place because, as a non-Asian and citizen of an Allied country, he easily moved through American society. While U.S. and British counterintelligence eventually neutralized Rutland, this case was not militarily effective because U.S. authorities were not able to

[5] "Letter from American Embassy (Thurston) to British Security Service (Gibbs), dated 10 July 1943," Records of the [British] Security Service, Rutland, Frederick Joseph, Case PF 37996 Volume 10, British National Archives, KV-2-336; and "Memo Re: Frederick J. Rutland, dated 18 April 1942," Records of the [British] Security Service, Rutland, Frederick Joseph, Case PF 37996 Volume 8, British National Archives, KV-2-334.

[6] "Home Office Internment Appeal Meeting Transcript, dated 15 January 1942, 21–24," Records of the [British] Security Service, Rutland, Frederick Joseph, Case PF 37996 Volume 7, British National Archives, KV-2-333; and "Security Coordination Washington letter, dated 30 October 1941," Records of the [British] Security Service (Rutland, Frederick Joseph, Case PF 37996 Volume 8, British National Archives, KV-2-334.

[7] Records of the [British] Security Service (Rutland, Frederick Joseph, Case PF 37,996 Volume 5, British National Archives, KV-2-331-092.

[8] "Frederick Joseph Rutland, Spare Copy as Sent to SIS."

determine the full extent of any compromise, and consequently any *advantage* gained by the Japanese remained *unexpected*.

Lessons Learned

While British counterintelligence demonstrated excellent liaison, coordination between ONI and the FBI was poor, leaving the Department of the Navy (DON) leadership blind to this facet of Japanese naval intelligence collection. Seventeen years after the unidentified chief case, British signals intelligence again demonstrated the utility of leads generated through monitoring the communications of an adversary intelligence service. In addition, as with the Secret Service surveillance of Downing 40 years earlier, the FBI's ability to surveil Rutland was critical to linking him to his Japanese case officer, which would have helped build a legal case against him. Those two capabilities—signals intelligence and surveillance—continued to be key elements of successful counterintelligence investigations throughout the span of this study.

First U.S. Navy Espionage Prosecution

As historian Ken Kotani wrote in his 2009 book *Japanese Intelligence in World War II*, "From 1909, the Imperial Japanese Navy (IJN) intelligence apparatus targeted its information gathering efforts on the United States. Yet the Intelligence Department remained in peacetime mode until the outbreak of the Pacific War, and [the section] that specialized in intelligence about the United States, consisted of fewer than ten staff until the attack on Pearl Harbor."[9] He added, "Yet, the IJN also dispatched 18 officers to the United States, and the military attachés

[9] Ken Kotani, *Japanese Intelligence in World War II* (New York: Osprey, 2009), 69.

office in America was quite a large establishment comprising 30 staff including assistants for the officers."[10]

According to British Security Service records, the IJN in the 1920s wanted information on the latest naval technologies to contribute to Japanese construction of aircraft carriers and submarines. However, by 1935, IJN intelligence wanted an agent to "engage in collecting information in Hawaii not only as a sleeper [in case of war], but as an active agent."[11]

Kotani and the British Security Service brought out two important points about the Japanese that have application today. First, the IJN was blundering into a war with the United States with minimal intelligence. Second, as Japan and the United States inched toward war, naval human intelligence shifted from collecting about technology to collecting strategic and then tactical intelligence in preparation for combat. These points are based largely on the Rutland case, but subsequent Japanese espionage operations targeting the U.S. Navy, which Kotani and the British Security Service did not consider, support their conclusions.

These World War II insights are particularly important for today's DON leaders who seek to use fleet assets as a deterrent. A clear-eyed understanding of a potential adversary's naval intelligence capabilities was needed to ensure that the adversary the DON sought to deter was not dysfunctional, as Japanese naval intelligence proved to be in the 1930s. An adversary with a dysfunctional intelligence system may underestimate U.S. naval capabilities and fail to grasp the intended deterrent effect.

Kotani's work also highlights what may now be a repeating pattern: long periods of technology collection followed by a shorter period of operational intelligence collection. That pattern was first set by the U.S.

[10] Kotani, *Japanese Intelligence in World War II,* 69.
[11] Kotani, *Japanese Intelligence in World War II,* 79, 83.

Navy in the late nineteenth century preceding the Spanish-American War. Japan followed the same pattern in the early twentieth century prior to World War II, and the People's Republic of China (PRC) may be following the same pattern today. The culmination of this pattern in each of these cases was naval conflict.

The Rutland case highlights another parallel between Japan's naval modernization before World War II and the PRC's military modernization today. As previously discussed, like Japan in the early 1900s, the PRC in the early 2000s relied on technology theft to modernize its naval forces. Rutland was employed to help the IJN learn how to use the weapons they built, specifically carrier-based aviation. Today, the PRC is doing much the same. As a U.S. Air Force press release in February 2024 noted, "Current and former U.S. and NATO members with air operations experience are in demand by the PLA and have been the targets of both overt and covert recruitment . . . targeted experience includes that of pilots, maintainers, air operations center personnel, and a variety of other technical experts from across multiple occupations that could provide insight into U.S. and NATO air tactics, techniques, and procedures."[12] A century apart, Japan and the PRC appear to have used identical techniques to prepare for a possible war.

With this in mind, the second World War II period case brief saw the IJN attempt to ensure that the United States did not have an *unexpected manner advantage* by gathering information about U.S. advancements in aircraft carrier design and dive bombing in the mid-1930s.

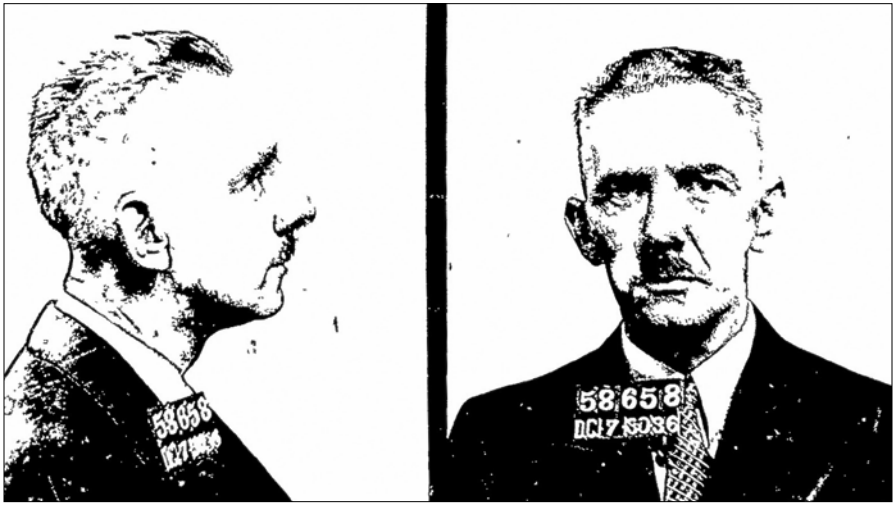
1933: John S. Farnsworth

Background

In 1933, John S. Farnsworth was a married 40-year-old defense contractor working for the Bosch-American Company selling aviation

[12] 1stLt Cameron Silver, USAF, "Chinese Attempts to Recruit U.S., NATO Service Members as Advisors Prompts Ramstein Conference," U.S. Air Forces in Europe and Africa, 8 February 2024.

Figure 15. John S. Farnsworth



Source: "John Semar Farnsworth" (Washington, DC: Federal Bureau of Investigation, File #65-632).

Former U.S. Navy lieutenant commander John S. Farnsworth, 1936.

parts to the U.S. Navy. He had been a lieutenant commander, a naval aviator, and a pioneer of U.S. Navy carrier aviation. However, a variety of personal problems to include relationships and alcohol had left him destitute. In 1927, Farnsworth was court-martialed at the Philadelphia Navy Yard for "violation of a lawful regulation" and "scandalous conduct" stemming from three specifications of financial dealings with an enlisted man. He pled not guilty and claimed that he was being blackmailed. The court-martial found Farnsworth guilty and sentenced him to dismissal from the U.S. Navy.[13]

[13] "John Semar Farnsworth," Federal Bureau of Investigation, File #65-632, hereafter Farnsworth FBI file. Author's records received per FBI Freedom of Information Act no. 1158286. See also William Mangil, "Snaring Farnsworth: Betrayer of the Navy," *True Detective* 28, no. 5 (August 1937): 4–9, 80–86; John Alexander, "Spy," *Front Page Detective* (September 1937): 54–59, 106; James Booth, "Smashing the Japanese Spy Menace," *Real Detective* 40, no. 4 (June 1937): 28; and "Farnsworth, John S., Case No. 67865," RG 125: Records of the Office of the Judge Advocate General (Navy) Series, Card Index to U.S. Navy General Court Martial Files, File Unit Farm 135–36, NAID: 117324283, NARA.

Initiation and Espionage

Six years after his dismissal, newly married to a Washington, DC, socialite but living with his parents, Farnsworth was desperate for money. He attempted to sell his knowledge of carrier aviation to the Japanese, since he understood that they were trying to build their own carrier air arm. In 1933, he offered his services by mail to the Japanese embassy, and the Japanese naval attaché sent him $100 ($1,700 USD today) to make the trip from Cincinnati, Ohio, to Washington.[14]

The Japanese naval attaché was not a professional intelligence officer because the IJN had no intelligence specialty or training school. Intelligence was either an out-of-specialty tour or a collateral duty.[15] As a result, the naval attaché, who was under pressure to obtain information about the U.S. Navy, learned espionage tradecraft on the job. He pitched Farnsworth, who readily accepted.[16]

Despite having no access to classified material, Farnsworth's status as a defense contractor gave him access to the Navy Building in Washington. There, much the same as Downing 35 years prior, Farnsworth lingered, picking up gossip and unattended documents wherever he went. He took the documents directly to the Japanese naval attaché's office residence in the Alban Towers Apartments in Northwest Washington or to various personal meetings and at least one brush pass between vehicles in Chevy Chase Circle.[17]

[14] Farnsworth FBI file.
[15] Pedro A. Loureiro, "Japanese Espionage and American Countermeasures in Pre-Pearl Harbor California," *Journal of American-East Asian Relations* 3, no. 3, Special Issue, "December 7, 1941: The Pearl Harbor Attack" (Fall 1994): 207; and "Interrogation No. 309 (Japanese Intelligence No. 15): Fleet Intelligence Organization and Procedure," in *United States Strategic Bombing Survey*, vol. 1, *Interrogations of Japanese Officials* (Washington, DC: Government Printing Office, 1946).
[16] Farnsworth FBI file.
[17] Farnsworth FBI file.

Investigation and Punishment

Like the Rutland case, decoded Japanese diplomatic messages eventually provided clues to Japanese espionage in Washington, and subsequent surveillance of the Japanese naval attaché led to an identification of Farnsworth. Likely attempting to identify the full Japanese espionage network, the FBI delayed attempting to prosecute Farnsworth, but it did not inform ONI of their investigation.[18]

This continued until April 1935, when Farnsworth stole a classified publication from the desk of a Navy officer. The officer reported Farnsworth to ONI, and ONI's investigative response was to publish a Navy-wide bulletin to report any approaches by Farnsworth, initiate a mail cover, and to ask the Metropolitan Police Department of the District of Columbia to surveil him. ONI did not appear to coordinate any of these actions with the FBI.[19]

The ONI investigation revealed that Farnsworth was visiting the Japanese naval attaché, that he was in mail contact with the Japanese naval attaché, and that he had attempted to elicit information from Navy officers in Norfolk, Virginia, and Annapolis, Maryland. However, the Navy-wide bulletin also exposed the case when an officer told Farnsworth about it. Farnsworth approached ONI and denied espionage but admitted offering consulting services to the Japanese.[20]

At this point, ONI informed the FBI. The FBI documented the allegation of the stolen classified document along with numerous additional allegations that Farnsworth had attempted to elicit information from Navy officers. They also worked with ONI to surveil Farnsworth, but he never met with the Japanese naval attaché again.[21]

Instead, Farnsworth began drinking heavily and went to the press. He tried to sell a story that he was conducting a personal double agent

[18] Farnsworth FBI file.
[19] Farnsworth FBI file.
[20] Farnsworth FBI file.
[21] Farnsworth FBI file.

operation to expose security flaws in the United States. The journalist reported the approach to ONI.[22]

With the story about to go public, the FBI arrested Farnsworth in July 1936. He confessed to having provided the classified publication to the Japanese in May 1935 and receiving funds worth $300,000 in today's money. He also confessed to providing engineering data for the first purpose-built U.S. aircraft carrier, USS *Ranger* (CV 4), and the U.S. Navy bombsight in use at the time, the D-4.[23]

Farnsworth pled guilty to violating the espionage statute solely for the one classified document he stole and sold. The court sentenced him to 4–12 years in prison, and he served 8 before being granted probation in 1945. He worked briefly for the Douglas Aircraft Company after the war but continued his heavy drinking and died in New York City in 1952 at the age of 59.[24]

Significance

Farnsworth was the first DON-related espionage conviction, and like Downing, he was a financial volunteer, the second of many for the department. Thirty-two of 58 subjects identified in this study as bonafide espionage subjects were financial volunteers, comprising approximately 55 percent of the total number of espionage cases considered. While the Department of Justice (DOJ) secured a conviction, militarily the case was a partial failure. The FBI and ONI neutralized Farnsworth and he confessed, but the DON never got a complete understanding of what, if any, *manner advantages* the Japanese may have acquired through his espionage.

[22] Farnsworth FBI file.
[23] Farnsworth FBI file.
[24] Farnsworth FBI file.

Lessons Learned

Like Downing, Farnsworth attempted to use his former affiliation with the DON to make money from its most obvious adversary. More importantly though, Farnsworth's case exposed both the abysmal interagency coordination between ONI and the FBI and ONI's resource-starved investigative capacity, particularly in surveillance assets. Moreover, it exposed ONI's amateurish investigative skills.

The Germans Make Their Appearance

The third and fourth World War II case briefs shift from the Pacific and Japan to the Atlantic and Germany. As in World War I, a major mission for the U.S. Navy was to recreate the "Atlantic Bridge" to move personnel and material overseas to liberate continental Europe.

Long before the average American was aware that the United States would be fighting in World War II, the U.S. military was preparing for war. As mentioned earlier, the Navy was creating and perfecting carrier aviation and the carrier task force. While that organization is taken for granted today, in the 1930s it was a novel concept, and implementing it required massive changes in systems and training. The destroyer's new mission developed at the same time. In addition to screening surface forces and hunting submarines, destroyers now also needed to provide an antiaircraft screen for aircraft carriers so that the carriers did not have to fire their own guns in self-defense and inhibit flight operations.[25] The speed of World War I-era destroyers was sufficient to screen slow-moving merchant ship convoys against submarines. However, aircraft carriers operated at much higher speeds to maximize airspeed over the flight deck. The new generation of destroyers

[25] LCdr Jason H. Davis, USN, "The Influence of the General Board of the Navy on Interwar Destroyer Design" (master's thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 1994), 87.

had to have the speed to keep up with aircraft carriers as well as the armament to fight both enemy aircraft and submarines.[26]

As a result of these new requirements, the entire U.S. Navy destroyer fleet became obsolete within a few years. So, despite the Great Depression, the Navy found the funds to begin construction of several new classes of destroyers, improved to keep up with and protect aircraft carriers.[27]

This was the situation in the United States when the next two cases began to unfold in 1934. Unlike 1913, when the *Pennsylvania* blueprints were stolen, the U.S. Navy was now employing contractors to design warships. However, 20 years later, the Navy had not learned its lesson, as the blueprints for the next generations of destroyers were circulating at Navy contractors' shipyards with haphazard internal security. The result was that years before World War II began, German espionage agents allegedly stole the designs for two different classes of destroyers before the ships entered service, a circumstance that violated part of the eighth principle of war: *Surprise. Strike the enemy . . . in a manner for which he is unprepared.* In theory, with these designs, the Germans would be prepared. And because the DON and FBI allegedly never solved these cases, they may also violate the ninth principle of war: *Security. Never permit the enemy to acquire unexpected advantage.* The U.S. Navy was unaware that Germany had the designs.

Yet, despite the incredible scope of these compromises, the loss of this naval technology information appears to have had no strategic effect on the outcome of the naval campaigns of World War II because the Germans were never in a position to capitalize on the advantage they allegedly gained.

The *Pennsylvania* case, Farnsworth's compromise of *Ranger*, and the next two case briefs have modern equivalents. Sometime prior to

[26] Davis, "The Influence of the General Board of the Navy on Interwar Destroyer Design," 108.
[27] Davis, "The Influence of the General Board of the Navy on Interwar Destroyer Design," 105–9.

2013, PRC hackers breached the cyber security of a defense contractor and stole the blueprints for a new U.S. Navy combatant, the littoral combat ship, costing the United States some element of a *manner advantage*. Thankfully, due to a comprehensive counterintelligence investigation, that advantage was *not unexpected*.[28]

Most naval intelligence collection by Germany's military intelligence service, the *Abwehr*, centered on its office in the city of Bremen, called Nebenstelle (Nest) Bremen, primarily because it nurtured sources among the crews of passenger liners that plied the New York-Hamburg route. As with the Japanese in the 1920s, the Germans at this time were not interested in the U.S. Navy because they foresaw little potential for an immediate war with the United States. Instead, they focused on technical information to help Germany with its naval and air force development. Abwehr headquarters in Belin noted in mid-1934, "The only subject of immediate interest, so far as American sources were concerned, were technical matters connected with the Navy and Air Force."[29]

Led by German *Kriegsmarine* (Nazi Germany's Navy) commander Erich Pheiffer, Nest Bremen set up its office in 1935 within the "Kriegsmarine Dienststelle," the naval coordinator of merchant shipping, which gave them easy access to files on merchant vessels. Beginning in 1936, Pheiffer and his assistant, Lieutenant Hans Bendixen, began recruiting sources and collecting information about U.S. naval and air technology. Through one of their Bremen-based passenger liner crew sources, Nest Bremen recruited a U.S. Army Reserve physician in New York named Ignatz Griebl who agreed to organize an agent network in

[28] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, 27 May 2013.
[29] "Interim Report in the Case of Erich Pheiffer," Records of the [British] Security Service, Pheiffer, Erich, Case PF 46969 Volume 1, British National Archives, KV-2-267_1, 7, 55 electronic file.

Figure 16. Erich Pheiffer

Source: [British] National Archives,
German Intelligence Officers (KV2/267), Kew, Richmond, UK.

German *Kreigsmarine* commander Erich Pheiffer, 1945.

the United States.[30] One of Griebl's first recruitment attempts appears to have been a naval architect employed by Bath Iron Works.

1934: Christian F. Danielsen

Background

In 1934, Christian F. Danielsen was a married 57-year-old draughtsman at Bath Iron Works in Maine. A German immigrant, he had worked for decades as a marine draughtsman in New York but moved to Bath late in his career. Bath Iron Works had previously built luxury yachts for the wealthy but was now retooling after the company won a substantial contract with the U.S. Navy to build the new *Farragut*-class destroyers. Despite the new contracts, Bath Iron Works allowed Danielsen, an outspoken supporter of Nazi German dictator Adolf Hitler and member of the pro-Nazi German American Bund, to remain at work.[31]

Allegations of Espionage

In 1938, Danielsen testified that in December 1936, Griebl, a fellow Bund member in Bangor, Maine, who had moved to New York, contacted Danielsen and offered him a job as head of a German shipyard. Danielsen admitted to travelling to New York twice to meet with Griebl and discuss the job offer, which never came to fruition. In 1939, Danielsen relayed a slightly different version of events, claiming that he only met Griebl by coincidence once at a convention and the job offer was completely theoretical. According to Danielsen's 1938 tes-

[30] "Interim Report in the Case of Erich Pheiffer," 7–11, 55–58 electronic file; and "Interim Report in the Case of Erich Pheiffer," appendix 21: "Some General Contacts of Korv. Kpt. Dr. Erich Pheiffer–Abwehr Officers: Agents: Other Contacts," Pheiffer, Erich, Case PF 46969 Volume 1, British National Archives, KV-2-267_4, 57, 3 electronic file.

[31] "The City Record: Officials and Employees of the Departments, Bureaus and Offices of the City of New York and of the Counties Contained Therein," 10, no 11927, City of New York, 31 July 1912, 66; and Ralph L. Snow, *Bath Iron Works: The First Hundred Years* (Portland, ME: Anthoensen Press, 1987), 295–96.

Figure 17. Bath Iron Works

Source: "USS *Dewey* (DD-349)," NavSource Naval History Destroyer Photo Archive, n.d.
Launch of the *Farragut*-class destroyer USS *Dewey* (DD 349) at Bath Iron Works, ME, the workplace of Christian F. Danielsen, in 1934.

timony, his 1939 interview, and a 1946 British debrief of Pheiffer, the job offer was made at Griebl's request. Pheiffer had arranged passage for Danielsen to visit Germany, but Danielsen never made the trip.[32]

However, in his 1971 book *The Game of Foxes*, Ladislas Farago claimed that after a meeting in New York, Griebl had accompanied Danielsen back to Maine and waited while Danielsen went to the shipyard and copied a set of the *Farragut*-class destroyer blueprints. Farago further alleged that Griebl passed these blueprints to his handler via couriers who were crew members on German transatlantic passenger ships.[33] A 1972 book review by a Central Intelligence Agency (CIA)

[32] "Bath Draftsman in Nazi Spy Case Testifies He Was Asked to Leave U.S.," *Portland (ME) Press Herald*, 5 November 1938, 1; "Bath Iron Works Notes and Gossip," *Bath* (*ME*) *Daily Times*, 11 April 1939, 4; and "Interim Report in the Case of Erich Pheiffer," appendix 21, no. 63, 9 electronic file.

[33] Ladislas Farago, *The Game of Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II* (New York: David McKay, 1971), 23–42.

Figure 18. Ignatz Griebl and accomplices

Source: "A Byte out of History: Spies Caught, Spies Lost, Lessons Learned," Federal Bureau of Investigation, 2007.

Dr. Ignatz Griebl (far left), who fled the United States, and his accomplices (left to right): Otto Hermann Voss (sentenced to six years), Johanna Hoffman (four years), and Erich Glaser (two years).

employee cast doubt on Farago's description of events, claiming that he had fabricated and embellished many of the details and that the source records that Farago reportedly used did not support the allegations made in his book.[34]

Investigation

In 1938, the FBI arrested one of Griebl's other contacts and soon detained Griebl as well. Released on bail, Griebl immediately fled the country. The FBI eventually learned of Griebl's connection to Danielsen and detained the latter as a material witness. In June 1938, Danielsen testified six times before a grand jury considering the case. As described above, he testified that Griebl had offered him a job in Germany. At the end of the trial, the court released Danielsen.[35]

[34] "Recent Books: The Game of the Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II, by Ladislas Farago," *Studies in Intelligence*, RG 263, Records of the Central Intelligence Agency, 1894–2002, Articles from "Studies in Intelligence," Fall 1972, 1955–1992, NAID: 7282944, NARA.

[35] "Danielson Cleared of All Suspicion," *Bath* (*ME*) *Daily Times*, 8 November 1938, 8.

In 1945, as World War II ended in Europe, the U.S. Navy took control of the German ports of Bremen and Bremerhaven and located the complete records of Nest Bremen in a salt mine near Verden, approximately 40 kilometers southeast of Bremen.[36] The records were recovered by British forces and loaned to ONI Bremen for microfilming and review.[37] An FBI agent in Bremen also reviewed the records and made copies of those that applied to the United States.[38] During his postwar debrief, Pheiffer admitted that Griebl "had obtained much information on American technical developments in naval and air construction, supplemented occasionally with blueprints; among these reports were several on constructional details of Seversky planes and a few on American destroyers."[39] While Danielsen worked at Bath Iron Works, his access to the *Farragut*-class destroyer plans is unknown and in 1938 company officials claimed that his work was not related to the DON.[40] There is no direct evidence linking him to the theft.

Significance

Like Farnsworth, Danielsen may have been a recruitment-in-place, but the FBI contained the damage to the DON through its arrest of Griebl. The result was a potential German *manner advantage* as the United States entered World War II. However, all eight *Farragut*-class destroyers built from the blueprints that Farago alleged Danielsen stole fought in the Pacific against the Japanese, rendering the thefts strategically insignificant.[41]

---

[36] "U.S. Navy in Europe," Naval History and Heritage Command, accessed 10 November 2023.
[37] "Office of Strategic Services Semi-Monthly Operations Report for 15–30 September 1945, dated 1 October 1945," Central Intelligence Agency, Langley, VA.
[38] *History of the SIS Division* (Washington, DC: Federal Bureau of Investigation, 1947), 437.
[39] "Interim Report in the Case of Erich Pheiffer," 20, 68 electronic file.
[40] "Danielson Employed 18 Months at Bath," *Lewiston* (*ME*) *Daily Sun*, 4 June 1938, 4.
[41] "Farragut Class," Destroyer History Foundation, accessed April 2021.

Lessons Learned

This case was significant because it highlights one of the reasons that the DON created a counterintelligence capability within ONI in 1917: the department could not unconditionally rely on the FBI to be empathetic to the military objective of counterintelligence. Worse, the FBI bungled the investigation and may have been unable to resolve Danielsen's role in Griebl's espionage network.

1934: Gustav E. Guellich

Background

In 1934, Gustav E. Guellich was an experienced 28-year-old metallurgist working in the research laboratory at the Kearny Point, New Jersey, shipyard for the Federal Shipbuilding and Drydock Company, a subsidiary of United States Steel.[42] Originally from Bayreuth in Bavaria, Germany, he had been a Nazi Party member since 1930 and moved to New Jersey in 1932.[43]

Espionage Allegation

In 1934, Guellich voluntarily began to send information about the United States to the Nazi Party's press office in Berlin. He provided them press clippings and a report on American attitudes toward Germany and the American Jewish population.[44] As with Danielsen, in his 1971 book *The Game of Foxes*, Farago claimed that in 1934–38 Guellich compromised a wide variety of technical information that passed through the U.S. Steel research laboratory. The Navy information in-

[42] "Federal Shipbuilding and Drydock Company," Destroyer History Foundation, accessed April 2021; and *Transactions of the American Institute of Mining and Metallurgical Engineers, Iron and Steel Division*, vol. 100 (New York: American Institute of Mining and Metallurgical Engineers, 1932), 46.

[43] *Chemisches Zentralblatt* [Chemical Central Journal] 2, no. 24 (Berlin: Deutsche Chemische Gesellschaft, 1932), 3620; and *Nazi Party Membership Records, Submitted by the War Department to the Subcommittee on War Mobilization of the Committee on Military Affairs, United States Senate*, pt. 1 (Washington, DC: Government Printing Office, 1946), 5.

[44] "NSDAP," European Holocaust Research Infrastructure Portal, accessed 10 November 2023.

Figure 19. Federal Shipbuilding and Drydock Company

Source: "USS *Benham* (DD-397)" NavSource Naval History Destroyer Photo Archive, n.d.

Launch of USS *Benham* (DD 397) at the Federal Shipbuilding and Drydock Company, NJ, the workplace of Gustav E. Guellich, in 1938.

cluded a classified manual on metal testing for warships, specifications for a passive sonar system, deck guns, and ammunition, and the blueprints for the new *Benham*-class destroyers Federal Shipbuilding was then building. Farago claimed that Guellich and Griebl met openly at restaurants where classified documents and cash changed hands.[45] While Guellich theoretically had access to the destroyer blueprints that Pheiffer admitted to receiving, there is no evidence that Guellich knew Griebl. Farago may have assumed that Guellich committed espionage based on his access to information at the Federal Shipbuilding and Drydock Company and the fact that he had been exposed as a previous Nazi Party member. It is quite possible that Farago falsified the entire case. The 1972 CIA review of Farago's book calls it "unremittingly sensationalized" and says the it "can neither be trusted nor ignored." This is why, despite the likely inaccurate allegations, both the Danielsen and Guellich cases remain in this study—because the inaccuracies, even after 90 years, should not be ignored.[46]

Facts

After the FBI arrested Griebl and he subsequently fled to Germany, Guellich's name was not among those detained. Guellich later moved to Buffalo, New York, and began working as a researcher for the American Optical Company.[47] In 1945, he joined the Allied Combined Intelligence Objectives Subcommittee (CIOS), the Allied effort to exploit captured German technology.[48] CIOS tasked Guellich with exploiting two German optics companies, Zeiss and Leitz.[49] The United States

[45] Farago, *Game of Foxes,* 29, 33, 39–41.
[46] "Recent Books: The Game of the Foxes."
[47] Gustav Guellich and David Lowber, "Pantographic Sighting Apparatus for Forming Machines," Patent 2,553,099, 15 May 1951; and Gustav Guellich, "Process of Making Optical Devices," Patent 2,399,799, 7 May 1946.
[48] John Gimbel, "U.S. Policy and German Scientists: The Early Cold War," *Political Science Quarterly* 101, no. 3 (1986): 445, https://doi.org/10.2307/2151624.
[49] John Gimbel, *Science, Technology, and Reparations: Exploitation and Plunder in Postwar Germany* (Stanford, CA: Stanford University Press, 1990), 91.

occupied the Zeiss Works from April to June 1945, requisitioning patents, design documents, and special production equipment.[50]

In 1946, captured records exposed Guellich's previous Nazi sympathies, and the FBI briefly investigated him.[51] Guellich died in 1953, 18 years before Farago alleged that he committed espionage.[52]

Significance

If ever proven guilty, Guellich would have been a strategically insignificant, militarily ineffective recruitment-in-place. Militarily, this case was a counterintelligence failure because the Germans may have been able to acquire a theoretical *manner advantage*. Fortunately, all the *Benham*-class destroyers that fought against the Germans survived the war, suggesting that Guellich's espionage had no strategic or operational impact.[53]

Lessons Learned

Again, the FBI bungled its pursuit of Griebl, and if Farago's claims are to be believed, it potentially failed to detect all of his contacts, allowing Guellich to slip through the net. Again, the DON failed in its oversight of contractor security.

Japanese Espionage on the West Coast

The fifth World War II espionage case brief also takes place in 1934 but on the West Coast, in California. Until 1940, the U.S. Pacific Fleet was

---

[50] Wolfgang Mühlfriedel and Edith Hellmuth, "The Company's History of ZEISS—At a Glance," Zeiss International, 1996.
[51] "Four from Paterson Area Named as Nazis in Captured Records," *Paterson* (*NJ*) *Evening News*, 12 March 1946; and National Archives and Records Administration, email to Stephen C. Ruder, "RD 78050 Initial Response," 20 November 2023.
[52] "Gustave E. Guellich, 47; Physicist and Engineer," *Buffalo* (*NY*) *Evening News*, 18 July 1953.
[53] "Benham Class," Destroyer History Foundation, accessed April 2021.

Figure 20. Joseph J. Rochefort

Source: Naval History and Heritage Command, Washington, DC.

U.S. Navy lieutenant Joseph J. Rochefort, 1934.

stationed in Long Beach and San Diego, California, not Hawaii as it is now.[54] That made southern California a prime target for Japanese naval intelligence, and Japan placed several naval officers in the state under the guise of students studying English. However, the racism prevalent in the United States at the time restricted their ability to operate. So, the Japanese looked for assets, such as Frederick Rutland, who could move more easily through American society.[55] That is where the next case began.

The FBI was able to neatly investigate and secure a conviction in this case, but what use was that conviction to the Navy? In the Farnsworth case, the Navy learned some of what the subject compromised, giving them time to adjust if necessary. In the next case, the inadequate ONI response and the FBI's rush to secure a conviction did not result in a full understanding of what information was stolen and sold to Japan. ONI and the FBI failed to fully ensure that the advantage gained by the IJN was *not unexpected*. Therefore, despite a conviction, militarily the investigation was a partial failure because it violated the ninth principle of war: *Security. Never permit the enemy to acquire unexpected advantage.*

This case set a precedent that would continue for another 30 years until the Naval Investigative Service devised a legal means to extract complete confessions from spies.

In an interesting historical twist, U.S. Navy lieutenant Joseph J. Rochefort, then serving as a staff officer with the U.S. Fleet aboard the flagship *Pennsylvania*, received the initial report about the sub-

[54] Wendy Arevalo, "The Navy at San Pedro: Terminal Island, California," Naval History and Heritage Command, 21 January 2022; and Harvey M. Beigel, "The Battle Fleet's Home Port: 1919–1940," U.S. Naval Institute *Proceedings* 111, no. 3 (March 1985).
[55] Loureiro, "Japanese Espionage and American Countermeasures in Pre-Pearl Harbor California."

ject of the next case brief.[56] Rochefort had served multiple intelligence tours and spoke Japanese, so a civilian that came to the ship to report a case of Japanese espionage was shuttled to him. Six years later, then-Commander Rochefort was assigned as officer in charge, Combat Intelligence Unit, Pearl Harbor, Hawaii—better known as Station HYPO. The work of Rochefort's team at Station HYPO in early 1942 would be the single most important intelligence breakthrough of the Pacific War, leading to the U.S. victory at the Battle of Midway.[57]

In another piece of Navy counterintelligence trivia, some of the ONI investigators who worked on this case at the time were under shallow cover in San Pedro, California, in an office with the euphemistic title of "Branch Hydrographic Office."[58]

1934: Harry T. Thompson

Background

In June 1934, Harry T. Thompson was 34 years old, unemployed, and destitute, living in Los Angeles.[59] He was a former Navy and Coast Guard yeoman who had been discharged in 1931 and was unable to find work. So, Thompson walked into the Japanese consulate to attempt to sell his knowledge of the U.S. Navy. The consulate told him to contact the Japanese naval attaché in Washington, so he wrote to the Japanese embassy. Recontacted, the Japanese told Thompson that their agent would contact him in Los Angeles.[60]

---

[56] "NH 67583: USS *Pennsylvania* (BB 38)," Naval History and Heritage Command, accessed 28 September 2021; and "NH 64844: Lieutenant Joseph J. Rochefort," Naval History and Heritage Command, accessed 28 September 2021.
[57] Elliot Carlson, *Joe Rochefort's War: The Odyssey of the Codebreaker Who Outwitted Yamamoto at Midway* (Annapolis, MD: Naval Institute Press, 2011), 71.
[58] "Re: Harry Thomas Thompson. Espionage. L.A. File 65-7, dated 14 December 1935," Federal Bureau of Investigation, File # 65-615, author's records, hereafter Thompson FBI file; and Carlson, *Joe Rochefort's War*, 71.
[59] "Spy Convicted in California," *Chattanooga* (*TN*) *Daily Times*, 4 July 1936. 1.
[60] Thompson FBI file.

Figure 21. Harry T. Thompson

Source: "Harry Thomas Thompson" (Washington, DC: Federal Bureau of Investigation, File # 65-615).

Former U.S. Navy yeoman Harry T. Thompson, 1935.

Initiation and Espionage

Thompson's contact was Toshio Miyazaki, a Japanese naval officer living in San Francisco.[61] His colleague, Lieutenant Commander Torii, who would have covered Los Angeles, was killed in a car accident in Gardena, California, in October 1933. Based on the documents discovered in Torii's briefcase, the FBI and ONI knew that he was gathering intelligence, and they began to investigate his contacts in Los Angeles. Meanwhile, Miyazaki was auditing classes at Stanford University as an English language student, so he did not have diplomatic immunity.[62]

As a former sailor, Thompson did not have access to classified information, but while wearing the uniform of a chief yeoman, he was

[61] "Sought: In Spy Plot," *Honolulu* (*HI*) *Advertiser*, 19 July 1936. *7.*
[62] Thompson FBI file.

Figure 22. Toshio Miyazaki

Source: Wikimedia Commons.

Imperial Japanese Navy captain Toshio Miyazaki, ca. 1941.

able to bluff his way aboard at least a dozen U.S. Navy ships in both San Diego and Long Beach, including the fleet flagship *Pennsylvania*. During the course of eight months, Thompson stole a variety of official documents and publications from those ships and sold them to Miyazaki.[63]

Thompson usually mailed the information he gathered to Miyazaki at his hotel in San Francisco, but sometimes they met at Thompson's apartment in Long Beach to exchange documents and money. The Japanese paid Thompson today's equivalent of $8,000 a month. Amazingly, during those eight months, Thompson confided in no less than three friends and his sister that he was committing espionage for the

[63] Thompson FBI file.

Japanese, and three of the four attempted to report him. The first tried to report him to ONI and the other two to the FBI.[64]

Investigation and Punishment

In February 1935, after a falling out, Thompson's roommate reported him to ONI. ONI was so short-handed that they asked a Navy physician who was an amateur detective to follow up with the case. ONI did not inform the FBI, but the physician and an ONI reservist recruited the roommate as an informant and initiated surveillance on Thompson.[65]

After confirming the allegations, ONI still did not notify the FBI. Instead, ONI attempted to recruit Thompson as a double agent by threatening him with espionage charges if he did not consent. Thompson agreed and passed disinformation produced by ONI to Miyazaki. However, Thompson soon fell out with his ONI handlers and warned Miyazaki, who fled the country. Thompson's roommate also fled to Texas, where police soon arrested him for check fraud.[66]

By the end of June, Thompson was destitute again. The ONI agents rejected his pleas for more money. He then turned back to the Japanese consulate, who gave him airfare to Washington to meet with the Japanese naval attaché. Realizing the danger Thompson was in, they paid him several thousand dollars and advised him to flee the country. Instead, he loitered at his sister's house in Baltimore, Maryland, that summer and then began a long, slow car trip back to Long Beach.[67]

After he left Baltimore in September 1935, Thompson's sister reported him to the city police for stealing her radio. When they showed little interest in the theft, she revealed his espionage. The police forwarded the report to the FBI. The same month, a former Coast Guard

[64] Thompson FBI file.
[65] Thompson FBI file.
[66] Thompson FBI file.
[67] Thompson FBI file.

shipmate reported Thompson's drunken confession, made months earlier, to the FBI. At this point, the FBI began to investigate the entire affair, interviewing numerous witnesses and ONI officials alike to build an espionage case.[68]

By December 1935, Thompson had arrived back in Long Beach and recontacted ONI. Instead of restarting the operation, ONI had him jailed in Long Beach on the theft charge to buy time to build the espionage case. The FBI then had him charged with wearing a uniform without authorization to stall for another 60 days.[69]

Thompson was convicted of violating the espionage statute and sentenced to 15 years in prison. He served 10 years and was released in 1946. Critically, the FBI was never able to get a full accounting of the documents that Thompson stole and compromised.[70]

Significance

Like Downing and Farnsworth, Thompson was a potentially strategically significant, militarily ineffective financial volunteer. This case was militarily ineffective because the DON was unable to get a full accounting of the compromise and therefore could not ascertain what *manner advantage* the Japanese may have gained.

Lessons Learned

ONI's attempt to turn this case into a double agent operation by threatening and intimidating Thompson predictably failed and only served to warn his Japanese case officer. ONI's failure to coordinate their investigation unnecessarily complicated the situation. Despite multiple tips from friends and family, the FBI was slow to start but eventually conducted a thorough investigation.

---

[68] Thompson FBI file.
[69] Thompson FBI file.
[70] Thompson FBI file.

Japanese Intelligence Collection Shifts toward War

The sixth World War II case brief marks the beginning of a shift in prewar espionage from seeking *manner advantages* to seeking *time and place advantages*. War was coming, and all sides knew that it would start with the fleet and weapons they had then, not those in development. This subtle shift in the patterns of espionage, had U.S. naval and military counterintelligence detected it, would have been a vital clue about the impending surprise attack on Pearl Harbor in December 1941.

By the mid-1930s, Japanese naval intelligence was collecting naval technical information from assets such as Farnsworth and Thompson, but they also pushed Rutland to begin collecting information about the U.S. military operational posture in California and Hawaii. The IJN had long viewed the U.S. Navy as its principal adversary and had been practicing tabletop attacks on Pearl Harbor since 1927. In 1936, the Japanese naval staff college recommended a surprise attack on Pearl Harbor if U.S. aircraft carriers were anchored there.[71] So, as the IJN achieved parity with the U.S. Navy in the mid-1930s, their intelligence operations shifted from collecting technical information to collecting information about the movements and operations of the U.S. Pacif-

[71] Note: in 1991, Yoichi Hirama, a retired Japanese Maritime Self-Defense Force admiral and a former professor of military history at the Japanese National Defense Academy, sourced this unique insight into the IJN's early preparation for a Pearl Harbor raid to two books. One, *A Private View of the Pacific War*, was published in Japanese in 1969 by Takagi Sokichi, an IJN rear admiral during World War II, and the other, *Japanese Naval Vessels*, was published in Japanese in 1956 by Fukui Shizuo, an IJN officer and naval constructor during the war who also participated in an IJN historical project after the war. Neither of these rare and untranslated books were available to the author, and the original records were almost certainly destroyed when the IJN archives were destroyed by a fire resulting from a U.S. firebombing attack on central Tokyo on 25 May 1945, as described in *U.S. Strategic Bombing Survey*, "Interrogation no. 487." See also "Interrogation No. 487," 23 November 1945, in *U.S. Strategic Bombing Survey*, 12; and Yoichi Hirama, JMSDF (Ret), "Japanese Naval Preparations for World War II," *Naval War College Review* 44, no. 2 (Spring 1991): 71.

ic Fleet in California and Hawaii. This marked the shift from seeking *manner advantages* to seeking *time and place advantages* described by Ken Kotani. With Rutland's failure to establish himself in Hawaii, Japanese naval intelligence needed eyes on Pearl Harbor. That was where the next case brief began.

1935: Bernard J. O. Kuehn

Background

In 1935, Japanese naval intelligence was not satisfied with their coverage of Pearl Harbor. Rutland was occupied on the West Coast and neither Farnsworth nor Thompson had any access. The Japanese wanted a non-Asian operative there who could operate in Hawaii without attracting attention.[72]

For reasons lost to history, they chose 40-year-old Bernard J. O. Kuehn. Kuehn was a married former German Navy sailor who had served in World War I and who had more recently served as a naval counterintelligence investigator before he was fired. Kuehn joined the Nazi Party in 1928 and claimed that he narrowly missed being named head of the Gestapo in 1932. The Nazi Party expelled him 1933 for having a Jewish friend.[73]

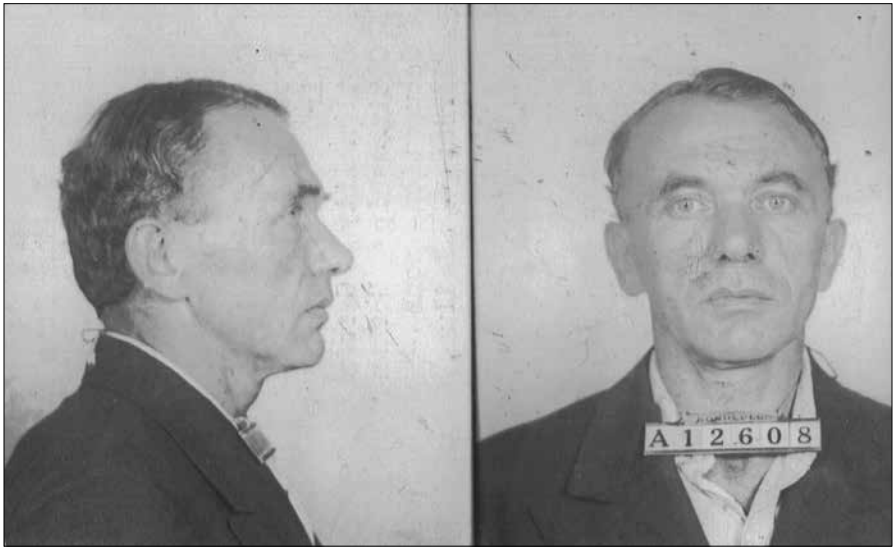
Initiation and Espionage

In 1935, the Japanese naval attaché in Berlin approached Kuehn with an offer to settle in Hawaii and establish an intelligence network there. Kuehn accepted, and he and his family moved to Oahu later that year.[74]

Contrary to the Japanese hopes, within a year Kuehn was widely known in Hawaii as a pro-Nazi German and was already the subject of an ONI investigation. As they did with Thompson in Long Beach,

[72] "Bernard Julius Otto Kuehn," Federal Bureau of Investigation, File # 65-1574, author's records, hereafter Kuehn FBI file; and Kotani, *Japanese Intelligence in World War II*, 82.
[73] Kuehn FBI file.
[74] Kotani, *Japanese Intelligence in World War II*, 82.

Figure 23. Bernard J. O. Kuehn



Source: "Bernard Julius Otto Kuehn" (Washington, DC: Federal Bureau of Investigation, File # 65-1574).

Bernard J. O. Kuehn after being detained by the FBI in Hawaii, 1941.

ONI attempted to recruit Kuehn as a double agent, but he turned them down.[75]

For the next three years, with ONI attempting to watch, Kuehn and his wife entertained U.S. military personnel at their house and reported the gossip, their own observations, and fabricated order of battle information to the Japanese. The Japanese paid Kuehn at least $14,000 (more than $200,000 today) and he made his deliveries at personal meets in remote rural areas of Oahu, but the ONI investigators lacked the resources to maintain the necessary surveillance to catch him.[76]

In 1939, a reserve ONI agent who was also a Honolulu police captain told the FBI about the ONI investigation. The FBI, with its nearest office in San Francisco, was about to reopen its Honolulu of-

[75] Kuehn FBI file.
[76] Kuehn FBI file.

fice. The FBI launched its own investigation and recruited several of Kuehn's neighbors and business contacts to no avail. However, one of his neighbors reported that in the fall of 1940 Kuehn had installed a new dormer window in the roof of his house. The FBI did not know what to make of the report.[77]

In 1941, as war with Japan appeared inevitable, Kuehn attempted to craft a plan that would allow him to remain in contact with Japanese naval intelligence. The plan involved a series of signal lights that he would shine from the newly installed dormer window in his house in Kailua to a submarine offshore. The house was 500 meters from Kailua Bay, and at the time only one house lay between it and the beach. The lights would have been visible from offshore.[78]

By now, Kuehn was meeting with a Japanese naval intelligence officer assigned under diplomatic cover at the Honolulu consulate. Kuehn pitched the dormer window idea to him, and he agreed to take it up with Tokyo.[79]

Investigation and Punishment

On 7 December 1941, Kuehn was just as surprised as everyone else on Oahu when the Japanese attacked Pearl Harbor. Within a few hours of the attack, the FBI and Honolulu police occupied the Japanese consulate and interrupted the diplomats' emergency destruction. One of the reports that the consulate failed to destroy contained the details of a plan involving lights and a dormer window. The investigators quickly connected Kuehn to the plan.[80]

The FBI arrested Kuehn the next day, and in February 1942 a military commission found him guilty of violating the espionage statute

[77] Kuehn FBI file.
[78] Kuehn FBI file; "Geologic Map and Guide of Oahu Hawaii," Hawaii Commission on Water Resource Management, 1939; and author's observations of the former Kuehn house, March 2016.
[79] Kuehn FBI file.
[80] Kuehn FBI file.

and sentenced to him to death "by musketry" under the "in time of war" provision of the Espionage Act of 1917.[81] Just six months later, in August 1942, six German sabotage agents captured on the East Coast were executed.[82] However, in October 1942, the United States commuted Kuehn's death sentence because all of his espionage acts occurred before the nation was at war with Japan, so he was instead sentenced to 50 years.[83]

Kuehn served only four years before the United States again commuted his sentence and ordered him deported. He waited two more years at Ellis Island in New York harbor until 1948, when he was simply paroled. He decided to go to Argentina to join the colony of escaped Nazis there. In 1955, Kuehn finally returned to Germany, where he died of cancer a year later at the age of 61.[84]

Significance

Kuehn was a recruitment-in-place, largely due to his race and his ability to move more easily within American society. The most significant aspect of the Kuehn case was the notable shift toward targeting fleet movements vice naval technology; from *manner advantages* to *time and place advantages*. Militarily this case was a failure because the FBI and ONI only neutralized Kuehn after the surprise attack on Pearl Harbor. The DON and the Pacific Fleet never knew what *time*

[81] Ryan Norwood, "None Dare Call It Treason: The Constitutionality of the Death Penalty for Peacetime Espionage," *Cornell Law Review* 87, no. 3 (March 2002): 826; and Espionage Act of 1917, Pub. L. No. 65–24, 40 Stat. 217 (1917).

[82] Michael Dobbs, *Saboteurs: The Nazi Raid on America* (New York: Alfred A. Knopf, 2004), 260–63; and "Nazi Saboteurs and George Dasch," Federal Bureau of Investigation, accessed 19 January 2024.

[83] Kuehn FBI file; and Letter from MajGen James A. Ulio, Adjutant General, to Mr. Walter Hunter, Warden, U.S. Penitentiary, Leavenworth, KS, dated 20 December 1942, RG 129: Records of the Bureau of Prisons, Series: Inmate Case Files, File Unit: Inmate File of Bernard Julius Otto Kuehn, NAID: 55286191, NARA, 64108.

[84] John Fiehn, "Widow of Man Convicted as P.H. Spy Sues U.S.," *Honolulu* (*HI*) *Star Bulletin*, 24 July 1962, 1.

and place advantage Kuehn's espionage might have afforded the Japanese until it was too late.

Lessons Learned

The DON was ill-served by ONI, which bungled the investigation by attempting to turn Kuehn into a double agent and by its lack of surveillance capability on Oahu. The department was also ill-served by the FBI, which was slow to establish a permanent presence in Hawaii despite the massive U.S. military buildup there, which resulted in the FBI lacking the surveillance resources to properly investigate Kuehn.

Espionage and the Battle of the Atlantic

The seventh World War II case occurs on the East Coast of the United States and involves Germany. By the late 1930s, the United States was already becoming the "arsenal of democracy" as it shipped huge amounts of military supplies to the United Kingdom.[85] As during World War I, those supplies and eventually U.S. troops would make the difference between defeat and victory for the Allies. However, again, the ships carrying the troops and supplies had to run the gauntlet of German submarines patrolling the Atlantic. According to eminent

[85] "Franklin Delano Roosevelt: The Great Arsenal of Democracy, Radio Broadcast on 29 December 1940," American Rhetoric, accessed 10 November 2023; "Biography of Jean Monnet," Institute Jean Monnet, accessed 10 November 2023; and "Lend-Lease Act (1941)," National Archives, accessed 10 November 2023. Note: during a "fireside chat" radio broadcast on 29 December 1940, President Franklin D. Roosevelt described to the citizens of the United States the increasing effort that the country was making to supply lethal aid to the United Kingdom and other allies in their fight against Germany. In minute 33 of a 36-minute speech, Roosevelt made the point that the United States "must be the great arsenal of democracy." The speech helped lay the foundation for the passage of the Lend-Lease Act of 1941, which authorized lethal aid for the United Kingdom. Jean Monnet, a French national and British emissary to the United States, originally coined the phrase that Roosevelt used in the speech. After the fall of France in 1940, Monnet, a French diplomat, businessman, bureaucrat, and anglophile, lobbied the Roosevelt administration to supply lethal aid to the United Kingdom. Monnet was later credited with laying the foundations for today's European Union.

U.S. naval historian Samuel Eliot Morison, "the Battle of the Atlantic was second to none in its influence on the outcome of the war."[86]

This time, the Germans were much more deadly. Between 1939 and 1945, during the Battle of the Atlantic, German submarines sank approximately 3,500 Allied merchant ships and 175 Allied warships, killing approximately 72,200 Allied naval and merchant sailors.[87] Three troop transports were among the victims, resulting in the deaths of more than 1,500 embarked troops. USAT *Dorchester* (1926), sunk on 3 February 1943, was transporting U.S. Army Air Forces personnel to Greenland; 558 died.[88] USS *Henry R. Mallory* (ID 1280), sunk on 7 February 1943, was transporting U.S. Marine and Navy personnel to Iceland; 208 died.[89] SS *Léopoldville* (1929), sunk on 24 December 1944, was transporting personnel assigned to the U.S. Army's 66th Infantry Division from England to France; 763 died.[90] As these examples show, the threat of spies assisting German submarine attacks was deadly serious.

To gain an *unexpected advantage* by gathering intelligence about the United States, German military intelligence, the Abwehr, had organized a large network of assets along the U.S. East Coast, primarily operating in the New York City area. A walk-in source who claimed that the Germans had pressured him to act as the network's radio operator betrayed nearly all of them. He worked with the FBI as a double agent, eventually identifying nearly every German asset in the United States, a case now known as the Duquesne Spy Ring. Fifty years later,

[86] Samuel Eliot Morison, *History of United States Naval Operations in World War II*, vol. 1, *The Battle of the Atlantic, September 1939–May 1943* (Boston, MA: Little, Brown, 1947), xii–xiii.
[87] "Battle of the Atlantic: Countering the U-Boat Threat and Supplying the Allies," Naval History and Heritage Command, 10 May 2019.
[88] Gudmundur Helgason, "Dorchester," UBoat.net, accessed 15 March 2021.
[89] Gudmundur Helgason, "Henry R. Mallory," UBoat.net, accessed 15 March 2021.
[90] Gudmundur Helgason, "Leopoldville," UBoat.net, accessed 15 March 2021.

a similar scenario would play out with a Cuban intelligence network that targeted the U.S. military in southern Florida.[91]

This next case identifies the dangers of a lack of cooperation between the FBI and naval counterintelligence. The subject, suspected of being a German espionage asset, moved from New Jersey to Norfolk, Virginia, just as the Lend-Lease Act introduced unprecedented cooperation between the U.S. and British Royal Navies, though naval counterintelligence was never involved. That was how the next case brief unfolded: while the Battle of the Atlantic loomed, nearly 40 German military intelligence assets operated on the U.S. East Coast, and the FBI and naval counterintelligence competed instead of cooperating.

Another more esoteric aspect of this case was a wartime practice known as "exclusion." On 19 February 1942, President Franklin D. Roosevelt signed Executive Order 9066, which authorized the U.S. War Department to create areas from which "any or all people" could be excluded to prevent espionage and sabotage.[92]

Based on this executive order, in May 1942, the commanding general of the Eastern Defense Command, U.S. Army lieutenant general Hugh A. Drum, declared the entire eastern seaboard of the United States the Eastern Military Area, noting that the area was subject to espionage and sabotage.[93] While originally conceived to enforce blackout rules, a follow-on order in September 1942 designated nearly 1,000 locations as prohibited or restricted zones and under the control of the Eastern Defense Command. The order declared, "Any person whose presence in the Eastern Military Area, or any part or Zone thereof, is deemed dangerous to the National Defense by the Commanding

[91] "Subject: Frederick Duquesne, Interesting Case Write-Up," Federal Bureau of Investigation, 12 March 1985; and Elias Groll, "Agent at Center of Spy Swap Was Cuban Crypto Expert," *Foreign Policy*, 19 December 2014.
[92] "Executive Order 9066," RG 11: General Records of the United States Government, Series: Executive Orders, File Unit: Executive Orders 9041–9070, Item Executive Order 9066: Authorizing the Secretary of War to Prescribe Military Areas, NAID: 124450932, NARA.
[93] "Public Proclamation No. 1," *Holyoke* (*MA*) *Daily Transcript-Telegram*, 16 May 1942. 1.

General, Eastern Defense Command and First Army, will be ordered excluded from the Military Area, or such part or Zone thereof, by the Commanding General, Eastern Defense Command and First Army." The subject of the next case was employed in Zone A-179, otherwise known as Camp Pendleton, Virginia, which is today called the State Military Reservation.[94] In 1943, the restricted zone was reduced to narrow coastal strips, but the overall Eastern Military Area boundaries remained the same.[95]

In July 1943, General Drum, speaking at an FBI National Police Academy graduation, credited the lack of enemy espionage and sabotage in the United States to three factors: the skill of the FBI; close cooperation between the FBI and the Army; and the power of exclusion give to him by the president.[96] However, this review of DON espionage cases in the period before World War II suggests that contrary to Drum's claim, exclusions appear to have had very little influence on espionage. Good FBI investigations alone were the key to success.

1936: Maximilian G. Waldemar Othmer

Background

In 1936, Maximillian G. Waldemar "Walter" Othmer was a 28-year-old naturalized German-American electrician who had emigrated to the United States and lived in New Jersey for the past seven years.[97] He had become radicalized and joined a pro-Nazi organization, the German American Bund, in 1935, rising to secretary and treasurer of the Tren-

[94] *Public Proclamation No. 2* (Governors Island, NY: Headquarters, Eastern Defense Command and First Army, 7 September 1942).
[95] *Public Proclamation No. 5* (Governors Island, NY: Headquarters, Eastern Defense Command and First Army, 9 August 1943).
[96] "Say We're Wining War on Sabotage; Hoover and General Drum Tell FBI Academy Graduates of Success against Spy Rings," *New York Times*, 18 July 1943, 22.
[97] "Waldemar Othmer," Federal Bureau of Investigation, File #100-30234, author's records received per National Archives and Records Administration Freedom of Information Act no. RD 781276, hereafter Othmer FBI file; and "Former Bund Leader Is Arrested Here by FBI as Suspected Spy," *Knoxville* (*TN*) *News-Sentinel*, 20 July 1944, 1.

Figure 24. Maximillian G. Waldemar Othmer

Source: "FBI Knoxville History," Federal Bureau of Investigation, n.d.
Maximillian G. Waldemar Othmer, ca. 1938.

ton, New Jersey, chapter.[98] Unable to find work in the United States, he traveled to Germany in December 1936 to see if he could find work there.[99]

Initiation and Espionage

In Germany, Othmer was treated with suspicion and again struggled to find work. When an Abwehr naval intelligence officer offered him paid work as an intelligence asset in the United States, he accepted. He returned to New Jersey a month later in January 1937 and found work as the director of a Trenton YMCA.[100] Considering his potential role as a German intelligence operative, Othmer was astonishingly outspoken about his support for the Nazi cause. He was notorious enough that

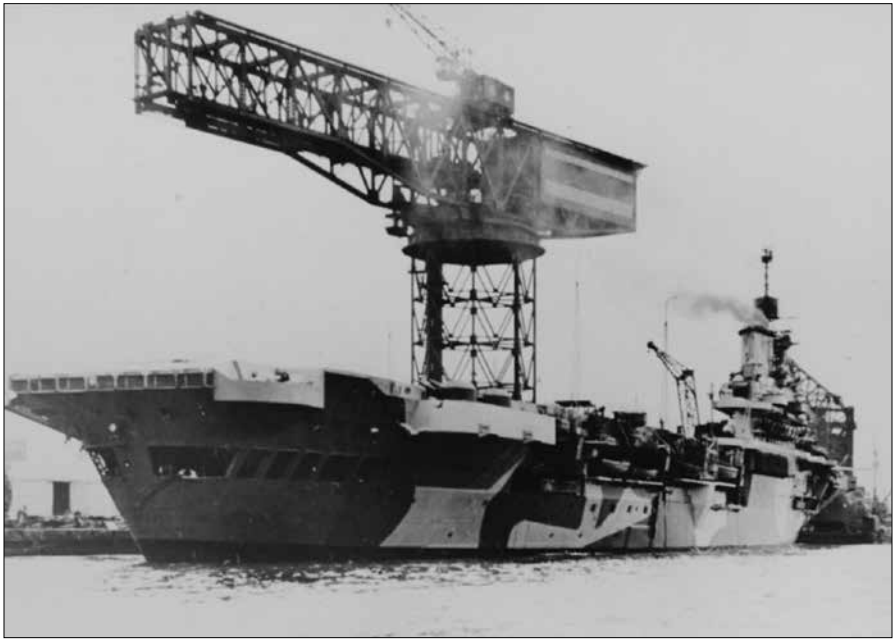
[98] "Congressman Samuel Dickstein (D-NY) Speaking about Un-American Activities," 75th Cong., 1st Sess., *Congressional Record* (1937): 8150.
[99] "German-born U.S. Citizen, Spy against Britain Here, Othmer Sentenced to 20 Years in Prison," *Norfolk Virginian-Pilot*, 1 August 1944.
[100] "German-born U.S. Citizen, Spy against Britain Here, Othmer Sentenced to 20 Years in Prison"; and "Congressman Samuel Dickstein (D-NY) speaking about Un-American Activities."

by August 1937, U.S. congressional representative Samuel Dickstein (D-NY) had publicly declared Othmer a Nazi and a "prominent member of the bund in New Jersey."[101] By March 1938, Othmer was the leader of the Trenton chapter.[102]

From November 1938 to March 1940, Othmer again traveled to Germany, during which he married and started a family. He also continued training with the Abwehr in offices on the fifth floor of 27/29 Wachtstrasse in Bremen (now a hotel) to use invisible or disappearing ink—also called "secret writing"—as well as radio communications.[103] He returned to the United States with funds to buy a radio but left his wife and infant behind in Germany. Othmer moved to Norfolk because it was a major East Coast port and, he reasoned, "activities there would be of particular interest to the Germans."[104] His primary collection requirement was the lethal aid that the United States was providing to the United Kingdom, which he gathered by working as a tradesman aboard military installations in the Norfolk area.[105] His communications plan required him to send the information by mail, using the invisible ink method he was taught in Bremen, to accom-

[101] "Dickstein Names Nazi 'Agitators,'" *Asbury Park* (*NJ*) *Press*, 4 August 1937. Note: according to former KGB files cited in Allen Weinstein and Alexander Vassiliev, *The Haunted Wood: Soviet Espionage in America—The Stalin Era* (New York: Random House, 1999), within four months of denouncing Othmer, Dickstein volunteered to Soviet intelligence and provided information about American fascists in return for money.
[102] "Bund Meeting Given Approval at Trenton," *Morning Post* (Camden, NJ), 25 March 1938.
[103] "Former Bund Leader Is Arrested Here by FBI as Suspected Spy"; "Interim Report in the Case of Erich Pheiffer," appendix 21, no. 85, 31 electronic file; and "Chronological Survey, Derived from War Room Sources, on Johannes Bischoff," Records of the [British] Security Service, Bischoff, Johannes W., Case PF 601785 Volume 1, British National Archives, KV-2-2749, 31–32 electronic file.
[104] "Former Bund Leader Is Arrested Here by FBI as Suspected Spy."
[105] "German-born U.S. Citizen, Spy against Britain Here, Othmer Sentenced to 20 Years in Prison."

Figure 25. Norfolk Navy Yard



Source: Naval History and Heritage Command, Washington, DC.

HMS *Illustrious* (87) undergoing battle damage repairs at Norfolk Navy Yard, VA, in November 1941, one month before the United States entered World War II.

modation addresses in Bremen and Milan, Italy.[106] This was the same technique taught to Downing by Spanish naval intelligence in 1898, 42 years before.

Here, the Abwehr made a critical mistake. Othmer's handlers instructed him to use an invisible ink made from Pyramidon, a widely available over-the-counter painkiller sold only in Europe at the time. Desperate to find Pyramidon, Othmer at one point even wrote to his

[106] "Summary of Information Obtained from Bischoff," Records of the [British] Security Service, Bischoff, Johannes W., Case PF 601785, Volume 1, British National Archives, KV-2-2749, 7, 17 electronic file; and "Re: Dr. Carl Hermann Nicolaus Bensmann; May 4, 1945," Records of the British Security Service, Bischoff, Johannes W., Case PF 601785, Volume 1, British National Archives, KV-2-2749, 36–37 electronic file.

former doctor in Trenton, lying about a back injury and asking specifically for that medication. Like Kuehn's dormer window report, an FBI agent entered that seemingly unimportant piece of trivia into Othmer's file.[107]

Once in Norfolk, Othmer sold vacuum cleaners, worked as a plumber's helper aboard the Naval Operating Base (modern-day Naval Station Norfolk), and later worked as an electrician for a local building contractor aboard Camp Pendleton in Virginia Beach.[108]

In June 1940, just three months after Othmer returned to the United States as a trained espionage agent, the Germans captured Paris, and Congress began passing a series of measures to dramatically expand the U.S. military to prepare for war. Othmer's hunch about the Norfolk area was accurate. Long a military area, the influx of funding in 1940 resulted in significant expansions of Hampton Roads bases, including the Naval Operating Base, the Naval Air Station, and Army facilities such as Camp Pendleton in Virginia Beach. The naval presence in the region expanded further in March 1941 after Congress passed the Lend-Lease Act, which included a measure to allow the United States to repair British Royal Navy ships in U.S. shipyards. Within weeks, Royal Navy ships began entering U.S. shipyards, including both the Norfolk Naval Shipyard and Newport News Shipbuilding and Drydock. Othmer would have had the opportunity to both observe and report about Royal Navy battle damage, ship modifications, and basic

[107] Bob Woodward, *The Secret Man: The Story of Watergate's Deep Throat* (New York: Simon & Schuster, 2005), 61–62.
[108] "German-born U.S. Citizen, Spy against Britain Here, Othmer Sentenced to 20 Years in Prison."

order of battle for the ongoing Battle of the Atlantic, as well as U.S. war preparations within Hampton Roads.[109]

Investigation and Punishment

In June 1941, the FBI arrested the Duquesne Spy Ring, neutralizing 33 Abwehr intelligence assets in the United States, all thanks to the double agent radio operator and a tremendous operations security failure by the Germans. This one double agent served as the clandestine radio operator for almost all the Abwehr agents in the United States. By serving as a front for a radio station operated by FBI agents on Long Island, the double agent became the main channel of communication between German espionage assets in New York and their Abwehr handlers in Germany.[110] Only Abwehr assets using mail to report, such as Othmer, escaped the FBI dragnet.

When Othmer returned from Germany and moved to Norfolk in the spring of 1940, the FBI was unaware. A year later, Othmer's landlady reported his pro-Nazi remonstrations to the Fifth Naval District ONI office, but with no known Navy link at the time, ONI forwarded

[109] "Record of the Committee on Naval Affairs, 76th Congress, Third Session, 1940," 76th Cong., 3d Sess., *Congressional Record* (1940): 13351; "Virginia SP Camp Pendleton—State Military Reservation Historic District," RG 79: Records of the National Park Service, Series: National Register of Historic Places and National Historic Landmarks Program Records, File Unit: National Register of Historic Places and National Historic Landmarks Program Records: Virginia, Virginia SP Camp Pendleton—State Military Reservation Historic District, NAID: 41684005, 18 August 2005, NARA, 43; "RMS Aurania III (1924–61)," HSM Ausonia, accessed 11 November 2023; Gudmundur Helgason, "HMS Queen of Bermuda (F 73)," UBoat.net, accessed 15 March 2021; "Before Pearl Harbor Fifth Naval District," RG 38: Records of the Office of the Chief of Naval Operations, Series: World War II War Diaries, Other Operational Records and Histories, File Unit, COM 5–War Record of 5th N.D., 1942, NAID: 134295283, NARA, 9; "History of NAS Norfolk, Virginia, 1917–1944," RG 38: Records of the Office of the Chief of Naval Operations, Series: World War II War Diaries, Other Operational Records and Histories, File Unit: NAS, NORFOLK–War History, NAID: 77706455, NARA, 5, 35–37; Corbin Williamson, "Industrial-Grade Generosity: British Warship Repair and Lend-Lease in 1941," *Diplomatic History* 39, no. 4 (2015): 745–72, https://doi.org/10.1093/dh/dhu040; "HMS Illustrious-May 1941," Defense Visual Information Distribution Service, 1 June 2018; and "HMS Royal Sovereign in Norfolk Naval Shipyard," NavSource Online: Battleship Photo Archive, August 1941.

[110] "Subject: Frederick Duquesne, Interesting Case Write-Up."

the report to the FBI. The FBI continued to investigate Othmer, and in May 1943, due to his well-known Bund membership, the Army, with ONI participation, excluded Othmer from the Eastern Military Area. Othmer then moved inland to Knoxville, Tennessee.[111]

By 1944, Othmer's FBI file had grown to four volumes, but the FBI did not suspect him of being a German intelligence asset. However, with the war nearing its end and few German or Japanese agents left to find, the FBI was reviewing its old files, including that of Othmer. It was during this review that an agent noticed the reference to Pyramidon. After the 1941 arrests, the agent heard about the invisible ink recipe and became convinced that Othmer too was a German agent.[112] That same year, Othmer was further implicated by a fellow Bremen espionage trainee who was detained in Colombia, extradited to the United States, and interrogated by the FBI.[113]

When they finally confronted Othmer in Knoxville in July 1944, the FBI interviewers took time to build rapport with him. As a result, Othmer confessed and provided information about the code and accommodation addresses he had used.[114] He claimed that he had never betrayed the United States and that his only target was U.S. lethal aid being provided to the United Kingdom under the Lend-Lease Act; after the United States entered World War II, he had ceased contact with the Abwehr. Othmer pled guilty to violations of the espionage

[111] "One-Time Nazi Bund Leader, Former Richmonder, Arrested," *Richmond* (*VA*) *Times Dispatch*, 21 July 1944, 11.
[112] Woodward, *The Secret Man*, 61–62. Note: the timing in this account is somewhat suspect as the FBI case file suggests the Pyramidon connection to espionage was already known at FBI headquarters in late 1942.
[113] *History of the SIS Division*, 352.
[114] Jack Neely, "The Night the FBI Collared a Nazi Spy at the YMCA," *Knoxville* (*TN*) *Mercury*, 29 July 2015.

statute and was sentenced to 20 years.[115] He never lost his U.S. citizenship and was released within seven years.[116] He died in 1959.[117]

Significance

Othmer was a strategically insignificant, militarily ineffective patriotic penetration. He was motivated to commit espionage by his devotion to the Nazi Party, and the Abwehr specifically sent him back to the United States because they thought he could blend into American society. Othmer's case was significant because ONI played a minimal role in a case with clear naval equities. The interagency collaboration required for effective counterintelligence was decades away. Militarily, this case was again a failure. The Army eventually neutralized Othmer by excluding him from coastal areas. However, because he did not confess until 1944, the DON had no idea what *time and place advantages* his espionage could have afforded the German Navy over the Allied convoys crossing the Atlantic during the first 18 months of the war. However, the choice of mail as his delivery method likely ensured that his information was operationally obsolete before it arrived in the hands of German naval intelligence.

Lessons Learned

At a more granular level, Othmer's case demonstrates how an asset's mistake—openly joining a Nazi organization—and two mistakes made by an adversary—the Abwehr failing to compartmentalize trainees and using Pyramidon for invisible ink in the United States—resulted in

[115] "Othmer Given 20-Year Term on Charges of Espionage," *Richmond* (*VA*) *Times Dispatch*, 1 August 1944. 7.
[116] "Denaturalization Suit against Othmer Dropped," *Knoxville* (*TN*) *Journal*, 29 September 1944, 12; "Families Cherish Traditions for Keeping the Christmas," *Richmond* (*VA*) *Times Dispatch*, 18 December 1955, 8C; *Report of the Attorney General to the Congress of the United States on the Administration of the Foreign Agents Registration Act of 1938, as Amended* (Washington, DC: Department of Justice, 1952), 89; and Siegfried Othmer, "Stranger in the South," *Medium*, 22 August 2018.
[117] "Obituary: Walter G. Othmer," *Richmond* (*VA*) *Times Dispatch*, 7 August 1959, 17.

significant investigative leads. This case also demonstrated that using simple espionage tradecraft like invisible ink was non-alerting when well-executed. Finally, the Othmer case demonstrated that detailed knowledge of an adversary intelligence service's tradecraft as well as skillful rapport building during subject interviews were key elements to convincing the asset to confess. Othmer's Bund membership was huge indicator. As one fellow Knoxville YMCA resident noted after his arrest, "If he is a spy, he is a dumb one because he made no secret that he favored some of Hitler's policies."[118]

First Soviet Case

The eighth World War II case brief had little to do with the impending war but was a harbinger of the future when it occurred in 1937 because it involved Soviet espionage. It was also unique because the subject remains the only U.S. naval counterintelligence agent ever convicted of espionage. Despite those interesting details, the case also brings up an uncomfortable truth that is still applicable today.

This case occurred in the waterfront area of Long Beach and San Pedro, California. In 1928, the Long Beach Naval Station became the home port for the Navy's second and third aircraft carriers, USS *Lexington* (CV 2) and USS *Saratoga* (CV 3), which were the latest evolution in naval warfare.[119] Just three kilometers away on the same island, several thousand Japanese Americans lived in an isolated community that operated more than 200 fishing boats and worked in the nearby canneries.[120] Using the same ethnic profiling that failed ONI during World War I, U.S. naval counterintelligence targeted the Japanese-American

[118] "Denaturalization Suit against Othmer Dropped," *Knoxville* (*TN*) *Journal*, 29 September 1944, 12.
[119] "USS *Saratoga* (CV-3)," Naval History and Heritage Command, 11 January 2022; and "USS *Lexington* (CV-2)," Naval History and Heritage Command, 11 January 2022.
[120] Hadley Meares. "Off the Coast of San Pedro, a Japanese Community Erased," *Curbed Los Angeles*, 30 March 2018.

fishermen of San Pedro. By the late 1930s, ONI leaders were convinced that Japanese Americans in San Pedro were collecting intelligence about the U.S. Pacific Fleet on behalf of the IJN.[121]

As previously discussed, on 19 February 1942 President Roosevelt signed Executive Order 9066, which authorized the War Department to create areas from which "any or all people" could be excluded to prevent espionage and sabotage.[122]

In contrast to the Eastern Defense Command's requirement that to be excluded, a person's presence must be individually "deemed dangerous," the commanding general of the Western Defense Command, Lieutenant General John L. DeWitt, applied Executive Order 9066 more broadly to include all Americans of Japanese ancestry without regard for any danger they might pose individually. DeWitt noted, "Intelligence services records reflected the existence of hundreds of Japanese organizations [on the West Coast] that were actively engaged in advancing Japanese war aims." Moreover, according to DeWitt, writing in the third person, "his conclusion was in part based upon the interception of unauthorized radio communications which had been identified as emanating from certain areas along the coast. Of further concern to him was the fact that for a period of several weeks following December 7th, substantially every ship leaving a West Coast port was attacked by an enemy submarine. This seemed conclusively to point to the existence of hostile shore-to-ship (submarine) communication."[123]

General DeWitt's account of Japanese submarine attacks along the U.S. West Coast was wildly exaggerated. Nine IJN submarines did pa-

[121] LCdr Kenneth D. Ringle, USN, "Japanese Menace on Terminal Island, San Pedro, California," Office of Naval Intelligence, Counterintelligence Section, 7 February 1942.
[122] "Executive Order 9066: Authorizing the Secretary of War to Prescribe Military Areas."
[123] *Japanese Evacuation from the West Coast, 1942: Final Report* (Washington, DC: Government Printing Office, 1943), vii, 4.

trol the coast during last two weeks of December 1941, but they attacked only 14 ships, sinking one and leaving another a total loss.[124]

Based on this spurious intelligence, DeWitt issued *Public Proclamation No. 4*, which designated the states of Washington, Oregon, California, Montana, Idaho, Nevada, Utah, and Arizona as Military Area No. 1 and ordered all "alien Japanese" and persons of Japanese ancestry to leave within 48 hours. Again, this study demonstrates that, as with the East Coast, West Coast exclusions appear to have had very little influence on espionage. Rather, good intelligence and investigations were the key.[125]

As a result of *Public Proclamation No. 4*, authorities interned all of the Japanese-American residents of the San Pedro fishing village in camps until 1945 to prevent the sabotage and intelligence operations foretold by General DeWitt. While the U.S. government interned the residents, their homes were stripped of valuables and then bulldozed.[126] In reality, not a single Japanese American committed espionage on behalf of Japan. The allegations against them were a series of fabrications and jaundiced observations compounded by analysis suffering from fatal doses of confirmation bias, all of which was built on a foundation of racism. ONI wanted to see the Japanese-American fishermen of San Pedro as spies, so the organization interpreted the available information as signs of espionage where none existed.

This was where the next case started, with ONI chasing ghosts along the California waterfront while another adversary crept up unseen.

---

[124] Bob Hackett and Sander Kingsepp, "Japanese Submarines: Tabular Records of Movements," *Sensuikan!: Stories of Battle Histories of the IJN's Submarines*, accessed 29 December 2023; and "U.S. Ships Sunk or Damaged in Pacific Area during World War II," American Merchant Marine at War, accessed 29 December 2023.

[125] *Public Proclamation No. 4* (San Francisco, CA: Headquarters, Western Defense Command and Fourth Army, 27 March 1942); and American Civil Liberties Union of Northern California Records, Case Files, 1934–1993, Korematsu, Fred, 1942–1946, California Courts 1942–1944, MS-3580_1385, California Historical Society, San Francisco, CA.

[126] Meares, "Off the Coast of San Pedro, a Japanese Community Erased."

1937: Hafis Salich

Background

In 1937, Hafis Salich was a married 33-year-old contract civilian investigator employed by the 11th Naval District, which covered parts of the modern-day Naval Criminal Investigative Service offices of Marine West and Southwest Field Offices. Salich worked as an investigator for the District Intelligence Office, which was based in San Diego and had a branch office in San Pedro, near Los Angeles, where Salich was assigned.[127] A naturalized citizen of the Soviet Union from the Georgian Soviet Socialist Republic, he had been working for ONI for about a year, having been recruited from the Berkeley, California, police department, where he had worked for the previous decade.[128]

Salich was conducting counterintelligence collection operations targeting the Japanese-American fishermen in San Pedro. However, Salich had a gambling problem, was constantly in debt, and, critically, had relatives still living in the Soviet Union.[129]

Initiation and Espionage

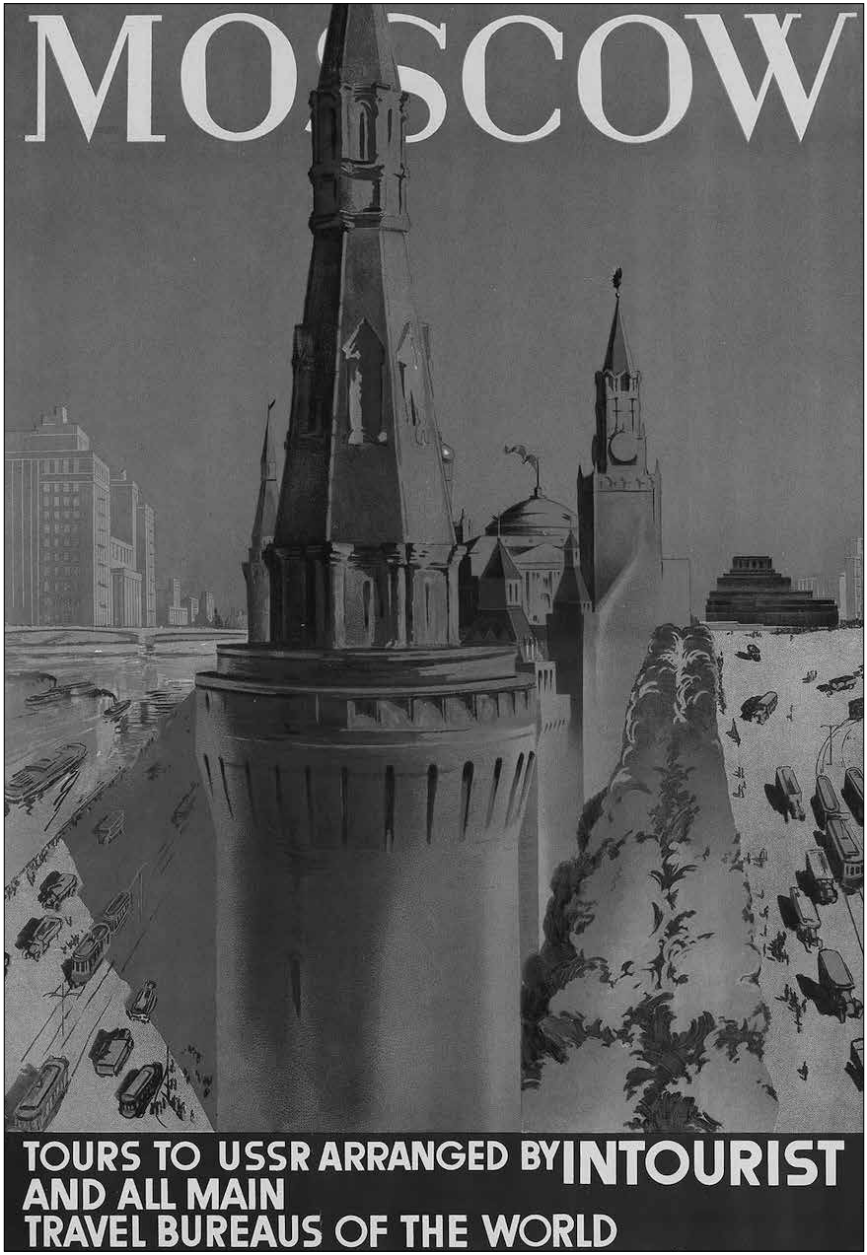
At the same time that Salich began working for U.S. naval intelligence, a Soviet People's Commissariat for Internal Affairs (NKVD) agent named Mikhail Nikolaevich Gorin arrived in the United States to begin working under official cover in the Soviet state-owned import company, Amtorg. Established in 1924, Amtorg served as the Soviet Union's primary trade agent with the United States. However, the

[127] William C. Heimdahl and Edward J. Marolda, *Guide to United States Naval Administrative Histories of World War II* (Washington, DC: Naval History Division, Department of the Navy, 1976), 97.

[128] "Russians Go on Trial as Spies; Sale of Navy Secrets Charged," *Los Angeles Times*, 22 February 1939, 1.

[129] "Navy Officers to Testify in Trio's Espionage Trial," *Los Angeles Times*, 23 February 1939, 6; "Defense Issue to Be Defined," *Los Angeles Times*, 27 February 1939, 4; "Spy Suspect Tells of Deals," *Los Angeles Times*, 1 March 1939, 2; "Sabotage Plot Laid to Japan," *Los Angeles Times*, 2 March 1939, 1; and Capt Ellis M. Zacharias, USN, *Secret Missions: The Story of an Intelligence Officer* (New York: G. P. Putnam's Sons, 1946), 203–5.

Figure 26. Intourist travel agency



Source: Wikimedia Commons.

The Soviet Intourist travel agency was used as a cover by People's Commissariat for Internal Affairs (NKVD) officer Mikhail Gorin in Los Angeles, CA, in 1938.

NKVD soon transferred Gorin to Los Angeles to open a new office of the Soviet state-owned travel agency Intourist.[130] In the 1930s, Soviet intelligence extensively used both Amtorg and Intourist as cover providers that set aside positions for use by the NKVD. In fact, within a year of this case, the NKVD entirely took over Intourist.[131]

Through a mutual acquaintance, Gorin learned that Salich was a former Soviet citizen working for U.S. naval intelligence. Salich, likewise, considered attempting to recruit Gorin. When the two men met, Gorin delivered an ominous letter from the Soviet vice consul in Los Angeles. It related that the authorities in the Soviet Union had checked on Salich's relatives and found that they were doing well. It was a stark threat.[132]

Gorin convinced Salich that they should cooperate, not against the United States but against their common enemy, the Japanese. Salich was in the uncomfortable position of not wanting to admit his gambling problems to the U.S. Navy but probably aware that he should have reported Gorin's implied threat. To solve both problems, in exchange for money to offset his gambling losses, Salich agreed to provide reports on Japanese intelligence activity.[133]

Investigation and Punishment

During 1937–38, Salich sold Gorin approximately 43 classified intelligence reports. Then, in the winter of 1938, Gorin made a critical mis-

[130] "Navy Officers to Testify in Trio's Espionage Trial"; "Defense Issue to Be Defined"; "Spy Suspect Tells of Deals"; "Sabotage Plot Laid to Japan"; and Zacharias, *Secret Missions*, 203–5.
[131] Leonid Maximenkov and Christopher Barnes, "Boris Pasternak in August 1936: An NKVD Memorandum," *Toronto Slavic Quarterly* (Fall 2019): fn5; and Testimony of Ismail Ege before the U.S. Senate Committee on the Judiciary, in *Interlocking Subversion in Government Departments*, pt. 15 (Washington, DC: Government Printing Office, 1953), 1025.
[132] "Spy Case Appeal Contends Data Sold Russia Not Vital," *Los Angeles Times*, 16 February 1940, 12; "Navy Officers to Testify in Trio's Espionage Trial"; "Defense Issue to Be Defined"; "Spy Suspect Tells of Deals"; "Sabotage Plot Laid to Japan"; and Zacharias, *Secret Missions*, 203–5.
[133] "Navy Officers to Testify in Trio's Espionage Trial"; "Defense Issue to Be Defined"; "Spy Suspect Tells of Deals"; "Sabotage Plot Laid to Japan"; and Zacharias, *Secret Missions*, 203–5.

take; he left an envelope in his suit pocket containing notes from a meeting with Salich. Gorin's wife sent the suit to the cleaners, and the pickup driver found the envelope. The driver went through it, and after reading the contents he took it to his supervisor. The supervisor called the Hollywood police, who called Army intelligence, who then called ONI and the FBI.[134]

The police made copies of the notes, and the cleaners returned the originals to Gorin intact. A brief investigation quickly identified Salich. Surveillance observed him typing reports in his office and taking them to meetings with Gorin. Salich's pay from the Soviets totaled $1,700 (approximately $25,000 today).[135] Ironically, Salich's reports were worthless; the fishermen of San Pedro were, as previously described, loyal Americans.

The FBI arrested both Gorin and Salich in December 1938, and in March 1939 they were convicted of violating the espionage statute, with Salich sentenced to four years and Gorin to six years.[136] Salich served less than three years and was permitted to enlist in the U.S. Army. He served faithfully throughout World War II and received amnesty in 1946.[137] Gorin, with the full weight of the Soviet government—now a U.S. ally—behind him, appealed his conviction and won. In 1941, he was released and deported.[138]

[134] "Navy Officers to Testify in Trio's Espionage Trial"; "Defense Issue to Be Defined"; "Spy Suspect Tells of Deals"; "Sabotage Plot Laid to Japan"; and Zacharias, *Secret Missions*, 203–5.
[135] "Navy Officers to Testify in Trio's Espionage Trial"; "Defense Issue to Be Defined"; "Spy Suspect Tells of Deals"; "Sabotage Plot Laid to Japan"; and Zacharias, *Secret Missions*, 203–5.
[136] "Russian Convicted Here as Spy Files Plea for Probation," *Los Angeles Times*, 21 March 1939, 14; and "Russians Convicted as Spies; Wife of One Acquitted by Jury," *Los Angeles Times*, 11 March 1939, 1.
[137] "Convicted Spy Wins Amnesty for War Duty," *Los Angeles Times*, 8 June 1946, 1.
[138] James Young, "State Department Appeasement Freed Convicted Russian Spy," *Miami* (*FL*) *News*, 29 March 1946, 15-A.

Significance

The Salich case was fully successful militarily. The DON was aware of the full extent of the espionage that occurred and was able to determine that the Soviets did not gain an *unexpected advantage* from it. Even though the information compromised was nearly useless, the case was significant because it was the first instance of Soviet espionage that targeted the U.S. Navy. ONI rightfully emphasized Japan as its chief adversary at the time, but this case should have been a warning.

Lessons Learned

Salich was a classic recruitment-in-place because the NKVD agent met him through a routine encounter. The NKVD then assessed Salich for his vulnerabilities and access to sensitive information and recruited him to provide ongoing access to that sensitive information. A positive aspect of this case was the existence within Southern California of a pocket of interagency cooperation between service counterintelligence agencies and the FBI. Moreover, ONI's ability to muster physical surveillance assets, admittedly within its office, was vital to quickly resolving this case.

The First Espionage Interdiction—Almost

The ninth World War II case brief was somewhat different than the previous eight, as it was the first time that a naval-related spy failed in their attempt to become a spy but was still caught. This was through no great effort by U.S. counterintelligence—it was just luck—but the case resulted in a partial understanding of the *advantage* gained by the Japanese. However, once the allegation was made, the FBI did a good job investigating and the case resulted in a conviction. Creating an effective counterintelligence net in the United States to catch would-be

spies would take another few decades. Unfortunately, ONI's role remained a distraction rather than a help.

Another point that this case highlights is a concept mentioned in the Kuehn case in Hawaii that could have application today: that the closer Japan came to attacking the United States, the more its intelligence collection shifted from technical information to operational information. While the Japanese directed Kuehn to obtain operational information in 1935, they rejected this would-be spy with technical information in 1938.

That was the situation described here, that a would-be spy was inspired to sell sensitive information to a looming adversary while U.S. counterintelligence agencies struggled to cooperate with one another.

1938: Karl A. Drummond

Background

In May 1938, Karl A. Drummond was a 21-year-old inspector at the former Northrop Corporation, renamed the El Segundo Division of the Douglas Aircraft Company, in Los Angeles, which led development of Douglas dive bomber and attack aircraft for the U.S. military. These are the same companies that, 40 years later, designed and built the U.S. Navy and Marine Corps' McDonnell Douglas F/A-18 Hornet fighter/attack aircraft, versions of which are still in use today.[139] Drum-

[139] "Douglas Aircraft Company Long Beach Plant, 2001," Historic American Engineering Record, Pacific Great Basin Support Office, National Park Service, U.S. Department of the Interior, San Francisco, CA; "F/A-18 A-D Hornet," Naval Air Systems Command, accessed 17 November 2023; and "F/A-18E/F Super Hornet," Naval Air Systems Command, accessed 17 November 2023. Note: John K. Northrop left the Douglas Aircraft Company in 1927, joined the Lockheed Aircraft Corporation, and had gone on to start his own company, but he returned to Douglas in 1932 to run the Northrop Corporation, a majority-owned subsidiary that he and Donald W. Douglas established in El Segundo. Northrop led development for Douglas of dive and attack bomber planes for the U.S. military. In 1938, Douglas acquired the remaining interest in Northrop and changed the name to the El Segundo Division of the Douglas Aircraft Company. Northrop left Douglas and founded the Hawthorne-based company Northrop Aircraft Incorporated in 1939. After being denied a crucial line of credit to fill waiting orders, Douglas made the decision to take on a partner. The result was the merger of Douglas Aircraft and the McDonnell Corporation in early 1967, renamed the McDon-

mond had worked for Northrop for a year, having joined his brother in California from their home state of Kansas.[140]

Vee Dee Drummond, five years older than Karl, was a married former U.S. Navy sailor employed at North American Aircraft in the Ingleside area of Los Angeles. The older Drummond had a problem; his wife was critically ill and he needed money for her treatment. The younger Drummond, conversely, was already on probation after a forgery and burglary conviction back in Kansas.[141]

Northrop was working on an important defense contract for the U.S. Navy to produce the BT-1 dive bomber, the precision-guided munition of the day. The technique involved plunging the aircraft down at a steep angle (70 degrees) and then releasing a bomb at low altitude so that it dropped directly onto the target. The Navy was perfecting this technique and creating specialty aircraft that would lead the world in naval dive-bombing. The BT-1 was the forefront of naval aviation, and its successor, the SBD Dauntless, would play a critical role in defeating the IJN just three years later.[142]

Initiation and Espionage

Karl Drummond, despite his job at Northrop, was still a thief at heart. He stole books from his coworkers and tools from the company. Then,

---

nell Douglas Corporation. The F/A-18 A-D Hornet was built by McDonnell Douglas with Northrop a major subcontractor. The F/A-18 Hornet remains the workhorse of Marine Corps tactical aviation and supports operational deployments around the globe. It will serve as the Marine Corps' primary bridging platform to the F-35 until its planned sundown in 2030. The F/A-18 E and F Super Hornet were rolled out at McDonnell Douglas (now a part of Boeing) in 1995.

[140] "Karl Allen Drummond," Federal Bureau of Investigation, File # 65-1080, author's records, hereafter Drummond FBI file; and "Aircraft Worker Accused as Spy," Associated Press, 1 December 1938.

[141] Drummond FBI file.

[142] John Rickard, "Northrop BT-1," Military History Encyclopedia on the Web, 15 June 2007; Barrett Tillman, "The Plane that Won the War," *Naval History* 31, no. 1 (February 2017); Gordon Swanborough and Peter M. Bowers, *United States Navy Aircraft since 1911* (London: Putnam, 1979), 167–69; and *Battles of Coral Sea and Midway* (London: Admiralty Naval Staff, 1952), 14, 39.

Figure 27. BT-1 dive bomber

Source: Naval History and Heritage Command, Washington, DC.

In 1938, Karl A. Drummond attempted to compromise the design of the BT-1 dive bomber, which was the prototype for the Douglas SDB Dauntless.

one day, he saw a chance to steal something he perceived to be much more valuable. In May 1938, he stole 14 blueprints and 150 photographs of the BT-1 by smuggling them out of the plant under his sweater. He apparently did not have a plan; he just thought someone would pay for them. While lacking a formal classification, Northrop and Navy officials described the blueprints and photographs stolen by Drummond as "highly confidential."[143]

[143] Drummond FBI file.

Drummond immediately showed the blueprints and photographs to his brother, who, knowing that Japan was a likely adversary of the United States, saw an opportunity to get his wife the medical care she needed. With the Japanese threat looming in every newspaper, the two brothers decided that the Japanese were likely to pay for the information. They first tried to find a Japanese buyer by boarding a Japanese merchant ship at Long Beach. They noticed that Douglas DC-3 airliners were being loaded onto the ship and thought the captain might have a Japanese contact interested in aircraft. But the captain did not speak English, and so the brothers departed.[144]

Next, Vee Dee Drummond suggested that they try to sell the items to the Japanese consulate in Los Angeles. The Japanese vice consul did not know what he was looking at, nor was he was particularly interested in espionage against the United States, and so he dismissed the brothers. Undeterred, the Drummonds visited the vice consul's house that evening. While the future of naval aviation eluded the vice consul, he was aware that Northrop was shipping aircraft to the Nationalist Army of the Republic of China. To deflect the brothers, the vice consul asked them to get him information about the BT-9 trainer aircraft, made by Vee Dee's company, North American, that were being sold to the Republic of China Air Force (ROCAF).[145]

The vice consul also suggested that the Drummonds could try to sell the blueprints and photographs to the representative of the Japanese Showa Aircraft company, who was visiting Los Angeles at the time. The brothers went to his hotel, but he too rejected the BT-1 information and asked for information about aircraft being sold to the ROCAF. Finally, the vice consul allegedly also referred the Drummonds to a prominent Japanese-American lawyer, who also rejected

[144] Drummond FBI file.
[145] Drummond FBI file.

the blueprints but asked for information about the aircraft sales to the ROCAF.[146]

Investigation and Punishment

In the meantime, Karl Drummond's thieving caught up with him. In June 1938, Northrop fired him for his petty thefts. He was convicted and returned home to Kansas on probation. Vee Dee, meanwhile, met the Japanese vice consul another time and earned $20 ($300 today) for BT-9 export information, but then he had a bout of conscience. He told his supervisor at North American about his contacts with the Japanese but only revealed the ROCAF aircraft compromises, not the stolen BT-1 blueprints and photographs. The supervisor contacted ONI.[147]

Without coordinating with the FBI, ONI decided to run Vee Dee Drummond as a double agent against the Japanese and began to use him to feed disinformation. After a month, Drummond had another bout of conscience and told ONI about the BT-1 blueprints and photographs as well as his and his brother's attempts to sell them to the Japanese consulate and the Showa Aircraft representative. At that point, ONI shut down the double agent operation and called the FBI. The investigation confirmed much of what Vee Dee Drummond said. However, Karl Drummond claimed that the entire episode was a patriotic attempt to expose the poor security at defense contractors. At the trial, it was brother versus brother, and in the end the judge found Vee Dee Drummond's version of events more believable.[148]

In exchange for his testimony, the DOJ did not charge Vee Dee Drummond. However, in December 1938, the court found Karl Drummond guilty of violating the espionage statute and sentenced

[146] Drummond FBI file.
[147] Drummond FBI file.
[148] Drummond FBI file.

him to two years.[149] He was released and found work at another aviation defense contractor, Consolidated Aircraft Company. However, when Consolidated Aircraft submitted him for a security clearance, the Army found the record of his espionage conviction and the company fired him.[150]

The FBI launched a long investigation of the Japanese-American lawyer but found no evidence to support Vee Dee Drummond's allegation. When interviewed, the lawyer denied ever meeting the Drummonds. Despite the lack of evidence, the U.S. government interned the lawyer for five years after the Japanese attack on Pearl Harbor.[151]

What the FBI and ONI missed was the Showa Aircraft representative's actual mission in the United States. Overtly he was there to purchase three DC-3s, the planes the Drummonds saw being loaded in Long Beach, and the manufacturing rights and equipment. However, the DC-3 was dual-use. In peacetime, it was used as a passenger and cargo plane, but in wartime it was the primary mover of paratroopers and cargo. The Japanese had falsified the end user certifications, and the actual customer was the IJN. Despite investigating the Drummond case, the FBI and ONI completely missed the purchase. Showa Aircraft built nearly 500 of these planes, code-named "Tabby" by the Allies, which the IJN used throughout the war.[152]

During the next few years, Douglas Aircraft modified and improved the BT-1 dive-bomber that the Japanese did not want information about. The result was the SBD Dauntless that the U.S. Navy used to sink five IJN aircraft carriers during the battles of the Coral Sea and Midway and turn the tide of World War II in the Pacific.[153]

---

[149] Drummond FBI file.
[150] Drummond FBI file.
[151] Drummond FBI file.
[152] Mark Chambers, *Wings of the Rising Sun: Uncovering the Secrets of Japanese Fighters and Bombers of World War II* (New York: Osprey, 2018), 258–59.
[153] "Douglas SBD-1 Dauntless," Flying Leathernecks Historical Foundation, 22 March 2020.

Significance

The 1938 Drummond case negatively demonstrated Ken Kotani's theory of a shift in collection from technical to operational information as war approached. The Japanese were no longer trying to improve their systems—they were preparing to fight a war with what they had. Unfortunately, U.S. intelligence did not recognize this trend at the time. On the positive side, the Drummond case was the first ONI interdiction of a would-be spy before any significant compromise occurred. Admittedly, part of ONI's success was due to Japanese incompetence, in that they rejected what should have been crucial information about U.S. naval dive bombers. Classic financial volunteers, the Drummond brothers' case was largely a military success because the FBI investigation assured the DON that the Japanese did not receive the BT-1 dive bomber blueprints. Any *manner advantage* gained through the Drummonds' treason was *known*.

Lessons Learned

Unfortunately, the Drummond case also points out a litany of DON failures. After the Farnsworth case, this was the second known instance of sloppy security at a Navy contractor and should have led to a more thorough review of contractors' employees. Perhaps naval counterintelligence would have caught Othmer earlier. This was also the third time that naval counterintelligence attempted and failed to conduct a reactive double agent operation without thoroughly investigating the situation. Finally, the case should have highlighted the successful Japanese technology diversion operation, but both the FBI and ONI missed the cues that the Drummond case exposed.

Big Apple Espionage

The 10th World War II case brief returns to the scene of the Duquesne Spy Ring in New York City. Like Othmer in Norfolk, this case was

handled by the Abwehr's Nest Bremen, which wisely eschewed the use of the double agent radio network established by the FBI in May 1940. Instead, Nest Bremen relied on the mail, which meant that once the FBI had rounded up the Duquesne Spy Ring, only two German assets continued to report on maritime activities from the East Coast of the United States, Othmer in Norfolk and the subject of the next case brief in New York. Like Othmer in Norfolk, this other asset had a ringside seat to the fruits of the Lend-Lease Act in New York, as British Royal Navy warships underwent repairs at the Brooklyn Navy Yard and increasing amounts of lethal aid and food were shipped from New York Harbor to Europe.[154]

1939: Simon Emil Koedel

Background

In 1939, Simon Emil Koedel was a 58-year-old film projectionist at the Lyric Theater in Manhattan. He was born in Wurzburg, Germany, in 1881, emigrated to the United States in 1906, and was naturalized in 1912.[155] He reportedly served in the U.S. Army from 1908–11, rising to the rank of corporal, and allegedly served in the Imperial German Army as a captain during World War I.[156]

Initiation and Espionage

In 1939, Koedel volunteered to spy for the Abwehr by mail using his home address in New York. Nest Bremen chief commander Erich

[154] Williamson, "Industrial-Grade Generosity;" and "Shipping Increase for Port Is Listed," *New York Times*, 7 July 1940, 8S.
[155] "Summary of War Room Traces in PT/601785," Records of the [British] Security Service, Bischoff, Johannes W., Case PF 601785, Volume 1, British National Archives, KV-2-2749), 7, 28 electronic file; and "Girl Denies Spying, Held in $25,000 Bail on U.S. Charge," *St. Louis* (*MO*) *Globe-Democrat*, 24 October 1944.
[156] "German Ex-Officer Held as Nazi Spy," *New York Times*, 24 October 1944.

Figure 28. SS *Coamo* departs New York Harbor

Source: Library of Congress, Washington, DC.

The steam passenger ship SS *Coamo* departs New York Harbor in December 1941. One year later, the ship was torpedoed and sunk by a German submarine in the mid-Atlantic.

Pheiffer received the offer and immediately accepted by mail, tasking Koedel with reports on shipping in New York harbor.[157]

Pheiffer handed the Koedel case over to his assistant, Sonderführer Johannes Bischoff, a cotton broker turned Abwehr case officer. Koedel did not receive regular payments but asked that an unidentified amount be set aside for him for after the war. Additionally, Koedel received a total of $600 in 1939–40 from Bischoff's cousin in Texas.[158] Koedel's foster daughter, Marie, a 21-year-old elevator operator, helped him

[157] "Interim Report in the Case of Erich Pheiffer," 34, 13 electronic file.

[158] "Exhibit List," Records of the [British] Security Service, Bischoff, Johannes W., Case PF 601785 Volume 1, British National Archives, KV-2-2749, 4 electronic file; and "Interim Report in the Case of Erich Pheiffer, appendix 4: "War Establishment of Abwehrnebenstelle Bremen in 1939/40," KV-276_3, 35. Note: a *Sonderführer* was a uniformed civilian commissioned due to their special qualifications required by the German military.

Figure 29. U.S. convoy departs New York Harbor

Source: Naval History and Heritage Command, Washington, DC.

In February 1942, a convoy with the second contingent of U.S. Army units dispatched to Europe during World War II departs New York Harbor, overwatched by a Navy blimp from Naval Air Station Lakehurst, NJ. The ship in the foreground, USS *Neville* (AP 16), has the U.S. Army's 34th Division signal and military police companies embarked.

gather information around the port.[159] The Koedels observed the port of New York with binoculars from aboard ferry boat transits and elicited information from crewmembers ashore. The pair also attempted to elicit information by mail from defense agencies and contractors.[160]

Using what British intelligence described as "guarded language," most likely simply obscuring the true purpose of the information ex-

[159] "Summary of War Room Traces in PT/601785," 7, 28 electronic file; and "Daughter Denies Spying with Father, Is Held on Bail," *Richmond* (*VA*) *Times-Dispatch*, 24 October 1944.
[160] "German Ex-Officer Held as Nazi Spy."

change, the Abwehr and Koedel passed intelligence requirements and collection exclusively by mail. Most of Koedel's reports consisted of twice monthly annotated shipping lists from U.S. newspapers. However, one especially good report, commended by Abwehr Headquarters in Berlin, provided the composition of a convoy, and pinpointed its assembly area off the coast with geocoordinates. Koedel received a special bonus for that information. Through his job as a projectionist, Koedel also had access to clips from U.S. Army instructional films, which he forwarded to the Abwehr.[161]

Investigation and Punishment

Throughout October 1939–October 1941, Koedel provided information to the Abwehr via the same two accommodation addresses used by Othmer. Like Othmer, Koedel ceased operations when the United States entered World War II in December 1941.[162] Probably based on his alleged service in the Imperial Germany Army in World War I, Koedel, like Othmer, was excluded from the eastern seaboard by the Eastern Defense Command in June 1943 and moved to West Virginia. Then, in May 1944, an Abwehr agent interned in the United States revealed the identity of his own case officer, Bischoff, who also handled Koedel and Othmer. With Bischoff's name, the FBI quickly tracked down his cousin and the payments to Koedel. Koedel and his foster daughter were arrested in October 1944.[163] Investigators also located letters asking about U.S. ship departures from "German military officials," presumably Pheiffer or Bischhoff, in the Lyric Theater where Koedel had worked. Koedel pled guilty under the Espionage Act and

[161] "Interim Report in the Case of Erich Pheiffer," 39–40, 18–19 electronic file.
[162] "Summary of Information Obtained from Bischoff," 7, 17 electronic file; "Summary of War Room Traces in PT/601785"; and "Interim Report in the Case of Erich Pheiffer," appendix 21, 76, 22 electronic file.
[163] *History of the SIS Division*, 352.

was sentenced to 15 years.[164] Marie refused to plead guilty but was convicted and sentenced to seven and a half years.[165]

Significance

The Koedel case was an outlier among those considered in this study—the sole *patriotic volunteer*. Strategically insignificant and militarily ineffective, he had no apparent impact on the course of the Battle of the Atlantic but was caught years too late.

Lessons Learned

The Griebl, Koedel and Othmer cases are all German demonstrations of Kotani's theory that Japanese intelligence collection shifted from technology to operational information as war became a higher probability. Additionally, the Koedel case was unique because he and his handlers never met and he received no training in intelligence tradecraft. The tradecraft used was sloppy but effective given the low level of scrutiny by U.S. counterintelligence at the time. The critical mistake that eventually led to Koedel's arrest was the Abwehr's lack of compartmentation between operations. Providing the same Abwehr accommodation addresses and revealing the true identity of the Abwehr case officer to several different operatives was the undoing of the Koedel case.

The Shooting Starts

The 11th World War II case brief does not involve an American stealing the DON's secrets but was instead about a foreign agent who, acting alone, set the stage for the U.S. Navy's defeat at Pearl Harbor on 7 December 1941. This case was the second-most egregious example in

[164] "Koedel Halts Spy Plot Trial to Plead Guilty," *Brooklyn* (*NY*) *Daily Eagle*, 15 February 1945.
[165] "Koedel Receives Term of 15 Years as Spy," *Evening Star* (Washington, DC), 1 March 1945, B1.

Figure 30. Imperial Japanese Navy chart of Pearl Harbor

Source: Naval History and Heritage Command, Washington, DC.

A chart of Pearl Harbor, HI, recovered from an Imperial Japanese Navy aircraft downed during the attack on 7 December 1941. Titled "Report on Positions of Enemy Fleet at Anchorage A," the chart accurately identifies U.S. Pacific Fleet mooring locations and is an exemplar of the high quality operational/tactical intelligence gathered by the Japanese in Hawaii.

---

this study of a U.S. naval counterintelligence failure to ensure that an adversary's *time, place, and manner advantage was not unexpected.*

With both Rutland and Kuehn underperforming in Hawaii and Japan's relations with the United States plummeting, Japanese naval intelligence was hard pressed for current, accurate information to plan the IJN's long-contemplated strike against Pearl Harbor. Rather than continue to rely on foreign assets that could blend with the U.S. population or try to recruit a Japanese American, the Japanese took a risk and opted for one of their own.

Unlike all previous espionage conducted against the U.S. Navy, this case involves directly tracking the movement of U.S. Navy ships to target them for destruction, a fact confirmed after the attack. A chart taken from a Japanese plane shot down during the raid clearly marks each ship in the harbor. The chart, titled in Japanese, "Report on positions of enemy fleet at anchorage A," identifies ship mooring locations.[166] The information to make this chart was precise and could only have come from direct observation of the harbor.

This case brief began with Japan nearly blind to the U.S. military buildup in Hawaii yet determined to conduct a surprise attack there. U.S. military counterintelligence and the FBI were attempting to blanket the territory (Hawaii was not yet a state) but were doing so in isolation, so no one organization could effectively cover the few existing targets. There were only two Japanese intelligence collectors on Oahu, both of whom were known to ONI and the FBI. As in California, U.S. naval counterintelligence wasted scarce resources targeting loyal Japanese Americans.[167]

1940: Takeo Yoshikawa

Background

In 1941, Takeo Yoshikawa was a 27-year-old IJN naval aviator ensign grounded due to a chronic illness and assigned under diplomatic cover to the Japanese consulate in Honolulu, Hawaii, under the alias Tadashi Morimura. His mission was to provide intelligence on the U.S. Pacific Fleet, which had just moved from California to Pearl Harbor.[168]

---

[166] "Chart of Pearl Harbor," Naval History and Heritage Command, accessed 24 November 2020.

[167] Erin Blakemore, "After Pearl Harbor, Hawaii Spent Three Years under Martial Law," History Channel, 23 August 2019.

[168] Takeo Yoshikawa, with LtCol Norman Stanford, USMC, "Top Secret Assignment," U.S. Naval Institute *Proceedings* 86, no. 12 (December 1960); Roger Naylor, "Pearl Harbor Spy Was Detained at Triangle T Ranch," Azcentral, 17 July 2015; and VAdm Homer N. Wallin, USN (Ret), *Pearl Harbor: Why, How, Fleet Salvage and Final Appraisal* (Washington, DC: Naval History Division, 1968), 42–43.

Figure 31. Takeo Yoshikawa

Source: Courtesy of the *Hawaii Times* Photo Archives Foundation and the Hoji Shinbun Digital Collection, Hoover Institution.

Imperial Japanese Navy ensign Takeo Yoshikawa in March 1941.

The IJN did not have professional intelligence officers. Instead, line officers rotated to intelligence duty between tours at sea and other duties. Due to his illness, Yoshikawa stayed ashore and spent two years studying the U.S. Navy. After he was medically retired, the Japanese Navy recalled him to limited duty and permanently assigned him to the American desk in naval intelligence. During the next four years, Yoshikawa, an English linguist, became the IJN's subject matter expert on the U.S. Navy.[169]

Assigned to the *3d Division* (Intelligence) of the Imperial Japanese Navy General Staff, Yoshikawa was one of only about 30 officers de-

[169] Yoshikawa and Stanford, "Top Secret Assignment."

voted to intelligence within the IJN. Relying almost entirely on open sources, Yoshikawa focused on the U.S. Navy bases on Guam, in the Philippines, and at Hawaii and became familiar with every ship, aircraft, and weapon in the U.S. Fleet.[170]

Initiation and Espionage

While Japanese naval intelligence had two agents, Rutland, and Kuehn, focused on Hawaii, neither had lived up to expectations. Rutland remained in California, while Kuehn forwarded useless gossip and newspaper clippings. With the decision to attack Pearl Harbor already taking shape in late 1939, the Japanese needed a reliable, dedicated expert on Oahu, and Yoshikawa was the man for the job.[171]

In 1940, the IJN gave Yoshikawa the Hawaii assignment. He took the Foreign Service English test and received an appointment as a junior diplomat under his alias, Morimura. Japanese naval intelligence elected diplomatic cover so that he could use the consulate's radio transmitter to submit reports. They feared, correctly, that U.S. naval counterintelligence would easily have discovered a clandestine radio transmitter. Japanese naval intelligence briefed only the vice consul on Yoshikawa's true name and affiliation.[172] Yoshikawa did not replace a departing diplomat; his position was allegedly an addition to cope with a large number of Japanese Americans renouncing their Japanese citizenship.[173] Despite these precautions, it was a small post, and it soon became evident to the other consulate employees that Yoshikawa's unusual hours meant that something was going on.[174]

---

[170] Yoshikawa and Stanford, "Top Secret Assignment."
[171] Yoshikawa and Stanford, "Top Secret Assignment."
[172] Yoshikawa and Stanford, "Top Secret Assignment."
[173] "Tadashi Morimura: Japanese Consulate General Swamped with Japanese Nationality Renunciations," *Nippu Jiji*, 10 March 1941, 3; and Yoshikawa and Stanford, "Top Secret Assignment."
[174] Robert B. Stinnett, *Day of Deceit: The Truth about FDR and Pearl Harbor* (New York: Free Press, 2000), 83–118.

Using his alias, Yoshikawa arrived in Honolulu in March 1941, nine months before the surprise attack on Pearl Harbor. Because of the large Asian population in Hawaii, he found that he could move quite easily around the island, but he also discovered that the Japanese Americans there were loyal Americans. He felt that any attempt to involve local Japanese Americans would jeopardize rather than assist his mission. While Yoshikawa did not know the specifics of the plan to attack Pearl Harbor, he knew that facilitating such a plan was the reason for his mission.[175]

As a former naval aviator, Yoshikawa rented planes at John Rodgers Airport (modern-day Kalaeloa Airport) and routinely flew over Oahu's military bases. He walked through Pearl City nearly every day to make observations of the East and Middle Lochs and across Ford Island to Battleship Row. He would also hike through the agricultural fields in the hills above Aiea, now covered with subdivisions, to look down into the harbor. But his favorite and most productive observation point was the Shuncho-ro Tea House, now called the Natsunoya Tea House, on Makanani Drive in Honolulu.[176] From an upstairs private function room, with the aid of a telescope, he could read the hull numbers of ships and track the movements of the Pacific Fleet in relative comfort and security.[177]

In September, the Japanese consulate received a message for Yoshikawa with instructions to begin identifying exactly where in the harbor each ship was moored. He now knew the attack was coming.[178] In late November, just days before the attack, a Japanese naval intelligence officer arrived in Honolulu under cover as a crew member of a

[175] "Tadashi Morimura: Japanese Consulate General Swamped with Japanese Nationality Renunciations."
[176] Will Deac, "Takeo Yoshikawa: World War II Japanese Pearl Harbor Spy," *World War II* (May 1997); and Lynn Cook," Teahouse of Intrigue," *HanaHou!: The Magazine of Hawaiian Airlines* (August/September 2011).
[177] Yoshikawa and Stanford, "Top Secret Assignment."
[178] Yoshikawa and Stanford, "Top Secret Assignment."

freighter. Despite multiple U.S. counterintelligence agencies focused on visiting ships' disembarking passengers, the intelligence officer delivered, via the vice consul, a list of 97 specific intelligence requirements for Yoshikawa. He answered them the same day and passed his report, along with photographs and other reports, to the intelligence officer aboard the freighter, which departed the next morning.[179] Soon, the IJN required Yoshikawa to send daily reports detailing the Pacific Fleet presence in Pearl Harbor.[180]

Investigation

Both the FBI and ONI had identified Yoshikawa as a suspected intelligence officer, but their operations were uncoordinated and neither had access to the signals intelligence that might have focused their efforts. With only a handful of agents each, their uncoordinated operations meant that they could not cover Yoshikawa well enough to determine exactly what he was doing. Further, like the ONI analysts who had examined signals intelligence reporting about the consulate's activities, both the FBI and ONI believed that the much larger threat was sabotage by Japanese Americans. Racism, incompetence, and bureaucratic infighting ensured that Yoshikawa was able to continue gathering and transmitting intelligence unmolested.[181]

When the Japanese attack occurred on the morning of 7 December, Yoshikawa was eating breakfast. He and the vice consul began their emergency destruction of records almost immediately, but within an hour, the Honolulu police and the FBI detained him, leaving intact the message that would later convict Kuehn. Yoshikawa never broke cover, and the United States eventually repatriated him with the other

[179] Yoshikawa and Stanford, "Top Secret Assignment"; and Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York: Penguin, 1981), 316–19.
[180] Yoshikawa and Stanford, "Top Secret Assignment."
[181] Stinnett, *Day of Deceit*, 83–118.

Japanese diplomats.[182] He worked for Japanese naval intelligence as an analyst for the rest of the war.[183]

After the war, Yoshikawa went into hiding briefly to avoid arrest by U.S. forces. He started a business and was briefly a celebrity in the United States in the early 1960s, when his role in the attack on Pearl Harbor became public knowledge. However, his role in the war made him unpopular in Japan. Yoshikawa died in 1993.[184]

Significance

While he never gained direct access to the U.S. Navy, like Othmer collecting for the Germans in Norfolk, Yoshikawa was a patriotic penetration because he entered the U.S. territory of Hawaii for the purpose of gathering intelligence for Japan. For the DON, the Yoshikawa case was an utter failure. Both the Kuehn and Yoshikawa cases demonstrate that while U.S. naval counterintelligence was aware of their activities, it was unable to provide an accurate appraisal of the *time, place, and manner advantage* that the IJN enjoyed over the U.S. Pacific Fleet due to espionage. In general terms, for U.S. Navy leaders the significance of the Yoshikawa case was the lesson that attempting to keep ship movements in and out of ports a secret was close to futile.

Lessons Learned

Because the Yoshikawa case was such a failure, it offered several lessons for naval counterintelligence practitioners. At the broadest level, it demonstrated the importance of both integrating signals intelligence into counterintelligence investigations and the criticality of ensuring that sufficient surveillance assets were available. For counterintelligence analysis, the Yoshikawa case demonstrated how confirmation

[182] Naylor, "Pearl Harbor Spy was Detained at Triangle T Ranch."
[183] Yoshikawa and Stanford, "Top Secret Assignment."
[184] Ron Laytner, "The Rising Sun Never Shines for Pearl Harbor Spy," *Chicago Tribune*, 1 December 1979, 13; and Naylor, "Pearl Harbor Spy Was Detained at Triangle T Ranch."

bias can be a fatal fault. At the tactical level of individual investigators and their immediate leadership, the Yoshikawa case demonstrated the absolute requirement for interagency cooperation.

The Last Hurrah

The 12th and final World War II case brief was an odd one. As war approached, Japanese naval intelligence scrambled to find stay-behind assets, agents established in the event of circumstances under which normal access would be denied, to report on issues within the United States after hostilities commenced.[185] They only managed to find one and made a tremendous blunder. U.S. counterintelligence quickly neutralized all other Japanese intelligence assets in the country soon after the attack on Pearl Harbor but missed this rather unusual case.

That was where this case started—while most of the nation's attention was on the kinetic conflict and countering enemies overseas, a middle-aged woman and her ailing husband began touring the United States on a mission for Japanese naval intelligence.

1941: Velvalee M. Dickinson

Background

In 1941, Velvalee M. Dickinson was a married 48-year-old owner of a collector-quality doll shop on Madison Avenue in New York and a most unlikely Japanese spy. However, in the months following the attack on Pearl Harbor she tried, but failed, to be the primary source of intelligence for Japanese post-attack battle damage assessment.[186]

---

[185] Col Mark L. Reagan, USA (Ret), ed., *Counterintelligence Glossary: Terms and Definitions of Interest for Counterintelligence Professionals* (Washington, DC: Department of Defense, 2014), 302.

[186] "Velvalee Dickinson," Federal Bureau of Investigation, File # 65-11186, author's records, hereafter Dickinson FBI file.

Figure 32. Velvalee Dickinson

Source: "Velvalee Dickinson, the 'Doll Woman'," Federal Bureau of Investigation, n.d.
Velvalee Dickinson, 1944.

Dickinson and her husband, Lee, first encountered Japanese culture in 1928. Lee was a produce broker in San Francisco and, despite the racial prejudice of the time, did business with Japanese American farmers from around the city. The Dickinsons became well acquainted with Japanese society in San Francisco and within a few years were regulars at events at the Japanese consulate and the Japan-America Society.[187]

In 1933, a Japanese training squadron consisting of the cruisers IJN *Iwate* (1900) and *Yakumo* (1899) visited the West Coast of the United States, including a stop in San Francisco. Hundreds of Japanese officers, sailors, and naval cadets toured the city, and during the fes-

[187] Dickinson FBI file.

tivities the Dickinsons met the Japanese assistant naval attaché, Ichiro Yokoyama.[188]

During the 1930s, the United States and much of the world were struggling through an economic calamity known as the Great Depression, with farmers defaulting on their loans, businesses closing, and unemployment reaching unprecedented heights.[189] By 1935, the disaster reached the Dickinson's produce brokerage. They closed, and Lee took a federal government job in Washington, DC. When the couple arrived in the capital, they rented an apartment in the Alban Towers, the home and office of the Japanese naval attaché.[190] The Dickinsons were living there while Farnsworth and Thompson were selling classified U.S. Navy information to the Japanese naval attaché in the same building.

In 1937, Lee's health began to fail, and he had to stop working. Velvalee's doll hobby became their main source of income. They moved to New York, where she attempted to open a fashionable doll shop on Madison Avenue. There, she continued socializing with Japanese society and frequently visited the Japanese consulate.[191]

Initiation and Espionage

In 1940, Yokoyama returned to the United States as the Japanese naval attaché. Just one month before the attack on Pearl Harbor, Yokoyama approached the Dickinsons with a proposition. In return for $25,000 ($375,000 in today's money), they would provide intelligence to the

[188] Dickinson FBI file; "IJN *Iwate*: Tabular Record of Movement," Imperial Japanese Navy Page, accessed 19 November 2023; "Men of 2 Japanese Ships to Be Feted," *San Francisco (CA) Examiner*, 13 April 1933, 13; "Japan Cadets See 'Ironside' in Frisco Bay," *Japan-California Daily News*, 14 April 1933, 8; "Touring Middies Heckled by Students," *Province* (Vancouver, BC), 15 April 1933, 3; "Japan Training Ships Here Soon," *Honolulu* (*HI*) *Star-Bulletin*, 17 April 1933, 34; and "Japanese Attaché Here," *El Paso (TX) Times*, 25 April 1933, 2.
[189] Dani Rodrik, *The Globalization Paradox: Democracy and the Future of the World Economy* (New York: W. W. Norton, 2011), 45.
[190] Dickinson FBI file.
[191] Dickinson FBI file.

IJN via coded letters. Yokoyama provided the Dickinsons with a code and an accommodation address in Argentina.[192]

One month later, Pearl Harbor was attacked and the Dickinsons made trips from Bremerton, Washington, to Mare Island, California, in January and June 1942. They would have been able to observe battle damage repairs being completed on two battleships at Puget Sound Navy Yard, on another battleship at San Francisco, and on a cruiser and destroyer at Mare Island Naval Shipyard.[193] At Puget Sound and Mare Island, the couple noted the repair of U.S. Navy ships damaged at Pearl Harbor. Velvalee dutifully typed letters using the Japanese code to let the Japanese know the extent of the damage done. Then she mailed them off to Argentina. However, after Lee died in 1943, his wife destroyed the code, stopped making collection trips, and never sent another coded letter.[194]

In Argentina, the accommodation address was at 2563 O'Higgins Street in Buenos Aires, the home of a Japanese and Nazi sympathizer who was an informant for the Japanese naval attaché in Argentina. Theirs seemed like a perfect plan, except for one problem—someone got the address wrong. The address that Velvalee Dickinson was using

[192] Dickinson FBI file.

[193] "USS *Shaw* during the Pearl Harbor Attack," Naval History and Heritage Command, accessed 22 November 2023; "Salvage Work on USS *Nevada*," Naval History and Heritage Command, accessed 23 November 2023; "Salvage Work on USS *California*," Naval History and Heritage Command, accessed 23 November 2023; "USS *Tennessee* (BB-43), 1920–1959," Naval History and Heritage Command, accessed 23 November 2023; "USS *West Virginia* (BB-48), 1923–1959," Naval History and Heritage Command, accessed 23 November 2023; and "*Pennsylvania* III (Battleship No. 38), 1916–1946," Naval History and Heritage Command, accessed 23 November 2023. Note: USS *Shaw* (DD 373) was repaired and modernized at the Mare Island Naval Shipyard beginning in February 1942; this coincided with Dickinson's trip. USS *Helena* (CL 50) was repaired and modernized at the Mare Island Naval Shipyard in December 1941–July 1942; this coincided with Dickinson's trip. USS *Nevada* (BB 36) was repaired and modernized at Puget Sound Navy Yard in the summer and fall of 1942; this coincided with Dickinson's trip. USS *Tennessee* (BB 43) was repaired and modernized at Puget Sound Navy in December 1941–February 1942; this coincided with Dickinson's trip. USS *Pennsylvania* (BB 38) was repaired and modernized in San Francisco during several yard periods in January 1942–February 1943; this coincided with Dickinson's trip.

[194] Dickinson FBI file.

was 1414 O'Higgins Street, so postal authorities returned all her letters to the sender.[195]

Investigation and Punishment

Probably unknown to the Dickinsons and Yokoyama, British intelligence was operating several imperial censorship stations that examined all mail going to and from Latin America. The Allies required that both airmail and ships carrying mail to and from the Western Hemisphere stop in the British colonies of Bermuda and Trinidad. These censorship stations employed thousands of people who screened millions of pieces of mail every day. Beyond the censors, these stations employed chemists and cryptographers to reveal invisible ink messages and break codes. These censors helped identify at least six espionage agents during World War II.[196]

While Dickinson's outbound letters made it past the censors, the "return to sender" letters did not. In 1943, the British cryptographers at the Trinidad censorship station identified the odd language used in Dickinson's letters as an open code, which substitutes innocuous-looking words or phrases to disguise the intended meaning. The code Dickinson used was based on the word *doll* meaning *ship*. A "doll hospital" signified a naval shipyard, a "Siamese" doll signified aircraft carriers, "Old English dolls" were Royal Navy ships, a hula skirt on a doll represented a ship that had been at Pearl Harbor during the attack, and "Mr. Shaw" referred to USS *Shaw* (DD 373).[197] The British thought the code referred to pornography. British intelligence forwarded copies of the letters to the FBI which, with the help

[195] Dickinson FBI file.
[196] *A Report on the Office of Censorship* (Washington, DC: Office of Censorship, 1945), 20–21, 45, 48–49.
[197] *Basic Cryptologic Glossary* (Washington, DC: National Security Agency, 1955), 24.

of U.S. Army cryptographers, identified them as coded language referring to U.S. Navy ships.[198]

Before the FBI could react to the British tip, they received several more complaints about strange letters about dolls returned from Argentina with return addresses of people who did not send them. The FBI opened an investigation in 1944. As the FBI received more letters, it became clear that the "senders" had one thing in common: they were all customers of Dickinson's Doll Shop.[199]

After attempting to connect Dickinson to the letters by comparing typewriters at hotels and in the Dickinson's home, the FBI arrested Dickinson in 1944. She confessed to knowing about the scheme and typing the letters but claimed that her deceased husband was behind the whole thing. The FBI investigation refuted the claim, showing he was mentally impaired in 1941 and could not have made the deal with Yokoyama.[200]

Dickinson pled guilty to violating censorship laws. She was sentenced to 10 years and served 6. She reportedly emerged from prison mentally unstable and disappeared in 1954.[201]

Significance

Dickinson was what can be termed an *ideological volunteer*. The cases in this study suggest that subjects such as Dickinson were ideological because they adopted a foreign culture as their own, generally one highlighted in the news at the time. Ideological volunteers tended to locate the nearest "official" representative and attempted to be of service, including espionage. Dickinson was difficult to detect because she was already in a relationship with a foreign culture before the espionage relationship began.

---

[198] Dickinson FBI file.
[199] Dickinson FBI file.
[200] Dickinson FBI file.
[201] Dickinson FBI file.

The Dickinson case was another military failure. While the FBI eventually neutralized Dickinson, she successfully gathered intelligence about the DON which, but for the handler's mistake, would have provided the Japanese with an *unexpected manner advantage* by warning the IJN about which U.S. warships would soon be back in action. The failure was exacerbated by the fact that even after the FBI received the first letters, it appears that they did not involve ONI despite obvious Navy equities.

Lessons Learned

The Dickinson case demonstrated the difficulty of attempting to conduct espionage during a high-intensity conflict when the authorities often suspend some civil liberties, even within democracies. Due to restrictions such as censorship and private radio transmitter bans, communicating intelligence from an asset to their handler was often slower and more laborious. The explosion of mobile telephone encrypted communications applications over the past decade has changed that dynamic. Delays can negate the utility of perishable information, and complex communication procedures increase the likelihood of compromise. In the Dickinson case, both happened. Finally, as with several cases during World War I, the Dickinson case demonstrates the benefits of exchanging counterintelligence leads with allies.

The Failure of U.S. Naval Counterintelligence, 1919–45

During the two decades between the world wars, 12 different people were known to have spied on the U.S. Navy—8 for Japan, 3 for Germany, and 1 for the Soviet Union. The assets spying for Japan compromised the designs of some of the latest U.S. naval warfare innovations and tracked the activities of the fleet. Similarly, the assets spying for Germany compromised an array of warship designs and technical

information and tracked U.S. assistance to its allies. All told, ONI's counterintelligence efforts failed the DON because Japan achieved potentially campaign-winning *unexpected time, place, and manner advantages* over the U.S. Pacific Fleet. Conversely, Germany achieved only minor *manner advantages* that do not appear to have had any effect on the outcome of the Battle of the Atlantic.

The Rutland, Farnsworth, Thompson, and Yoshikawa cases for Japan and the Griebl, Othmer, and Koedel cases for Germany combine to illustrate the trend in naval intelligence collection from *manner advantages* to *time and place advantages* highlighted by historian Ken Kotani in 2009. Through information collected from open sources and these agents, the Japanese and German navies would have learned of the rapid advances in U.S. naval aviation and should have understood how critical that U.S. Navy *manner advantage* would be in the upcoming conflict. The interwar period more clearly demonstrates a potential pattern first discerned during World War I: the tendency for potential naval adversaries to first focus espionage on technical issues, *manner advantages*, followed by a focus on tactical issues, *time and place advantages*. While clear in hindsight, the capacity to use this pattern—dubbed the "Kotani-shift" in this study—to predict a conflict in the future remains a question.

However, even the best intelligence was useless if operating forces ignored it. The behavior of the Japanese leadership in the final days before the attack on Pearl Harbor illustrates the perils of ignoring friendly *time and place advantages*. Since 1936, the Japanese Naval War College had recommended a surprise attack on Pearl Harbor, but only if U.S. aircraft carriers were present. They understood that aircraft carriers were the biggest threat to Japan, and so clearly the carriers should be the target of an attack on Pearl Harbor. However, the day before the attack, with the Japanese strike force still hundreds of kilometers from Hawaii, Yoshikawa reported that the carriers were not in port. The IJN

leadership ignored the intelligence and blindly carried out a plan that would not only fail to achieve its single objective but would also plunge their country into a war that they ultimately lost.

World War II was also a demonstration of a second potential pattern first seen in World War I, that espionage within the United States dropped off dramatically once the nation became engaged in a high-intensity conflict and martial law suspended some civil liberties. As a result of those restrictions, espionage became riskier and more complex, resulting in fewer volunteers, greater caution among established assets, and more mistakes in tradecraft.

This pattern has several implications for future U.S. naval counterintelligence operational prioritization. Most importantly, investments in counterintelligence personnel and infrastructure must precede a conflict before a potential adversary acquires an *unexpected advantage* through espionage. Equally important, naval counterintelligence practitioners must have both the capability to identify potential future adversaries and the institutional freedom to pursue espionage allegations involving any potential adversary.

Lessons Learned

The World War II period generated several bedrock lessons learned for the DON. First, the department suffered for a lack of trained and experienced counterintelligence investigators and plentiful surveillance assets. Second, attempts to turn espionage suspects into double agents through the use of threats were unsuccessful. Third, signals intelligence was a vital source of counterintelligence leads, and naval counterintelligence should have fully incorporated it into the overall counterintelligence effort. Fourth, counterintelligence investigators needed a detailed understanding of their adversary which relied on unbiased, effective analysis.

Of note, while examination of current events should not rely too heavily on historical parallels, Japanese naval intelligence activities in the years leading up to World War II may be able shine a light on future events. Like Japan in the 1920s and early 1930s, the PRC targeted U.S. Navy technology for decades from the 1980s on to slowly build up its naval forces. Moreover, like Japan in the 1920s, the PRC in the 2020s has sought U.S. and allied military aviation experience to train its own air forces.

In the latter half of the 1930s, Japan shifted its intelligence collection toward operational information and finally attacked the United States in 1941. More recently, in 2020 the PLA Navy for the first time crossed the International Date Line to conduct unilateral training approximately 435 kilometers south of Midway. As with the Japanese prior to the attack on Pearl Harbor, a shift in PRC intelligence targets during the 2020s could be a harbinger of the future.[202]

[202] "Recent Insider Threat Cases," Director of National Intelligence, accessed 11 October 2020; Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies"; Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, 8 June 2018; Xuanzun Liu, "Chinese Naval Fleet Wraps up Far Sea Exercise Deep in Pacific Ocean," *Global Times*, 26 February 2020; and Wen Chu, "Approaching Hawaii, What Is the Low-key Training Intention of China's Cutting-edge Fleet," *DWNews*, 21 February 2020.

Chapter 3
Early Cold War Case Briefs, 1946–1979

After the arrest of Velvalee Dickinson in 1941, the U.S. Navy was espionage-free for more than a decade despite the increase in tensions between the United States and the Soviet Union. The Cold War officially began in 1947 as the former Allies of World War II divided the world into spheres of influence. The tensions forced almost every country in the world to choose between the Soviet Union or the United States, and a long string of conflicts erupted because of or were influenced by those affiliations. Mostly, these conflicts involved independence for European colonies, such as the wars in Vietnam, or settling old disputes unresolved by World War II, such as the Korean War.[1]

All of these conflicts involved the U.S. Department of the Navy (DON). In Korea, the Navy and Marine Corps' amphibious invasion at Inchon, South Korea, in September 1950 turned the tide of the war.[2] In Vietnam, Marine ground forces, Navy riverine forces, and carrier

[1] Arthur Schlesinger Jr., "Origins of the Cold War," *Foreign Affairs* 46, no. 1 (October 1967): 22–52, https://doi.org/10.2307/20039280.

[2] "Inchon Landing (Operation Chromite)," Naval History and Heritage Command, accessed 20 May 2021; Lynn Montross and Capt Nicholas A. Canzona, USMC, *U.S. Marine Operations in Korea, 1950–1953*, vol. 2, *The Inchon Seoul Operation* (Washington, DC: Historical Branch, G-3, Headquarters Marine Corps, 1955), 296–97; and LtCol Pat Meid, USMCR, and Maj James M. Yingling, USMC, *U.S. Marine Operations in Korea, 1950–1953*, vol. 5, *Operations in West Korea* (Washington, DC: Historical Division, Headquarters Marine Corps, 1972), 478.

aviation all played significant roles.[3] Despite that, little espionage was involved. Instead, in Vietnam particularly, naval counterintelligence focused heavily on force protection to thwart asymmetric attacks in areas such as Saigon and Da Nang.[4]

While the United States' primary adversary throughout the Cold War was the Soviet Union, for the first 13 years of the conflict, Soviet intelligence paid limited attention to the U.S. Navy. The Navy posed little strategic threat to the Soviet Union because it had no role in strategic nuclear weapons deployment until 1960.[5] Despite that, Soviet intelligence maintained an operational interest in the Navy and would not turn away any *time, place, or manner advantages* that presented themselves.

That was where the first Cold War case brief began, 12 years after the end of World War II and 10 years after the beginning of the Cold War. A sailor working with classified information at the U.S. Navy headquarters in London was heavily in debt and looking for a way out.

1957: Nelson C. Drummond

Background

In 1957, Nelson C. Drummond was a married 29-year-old yeoman first class assigned to the headquarters of U.S. Naval Forces Eastern Atlantic and Mediterranean in London (now known as U.S. Naval Forces

[3] "U.S. Naval Forces in Vietnam and Southeast Asia," Naval History and Heritage Command, accessed 20 May 2021; Maj George R. Dunham, USMC, and Col David A. Quinland, USMC, *U.S. Marines in Vietnam: The Bitter End, 1973–1975* (Washington, DC: History and Museums Division, Headquarters Marine Corps, 1990), 266–67; and Edward J. Marolda, *By Sea, Air, and Land: An Illustrated History of the U.S. Navy and the War in Southeast Asia* (Washington, DC: Naval Historical Center, Department of the Navy, 1994), 70–118, 162–214.

[4] Richard A. Mobley and Edward J. Marolda, *Knowing the Enemy: Naval Intelligence in Southeast Asia* (Washington, DC: Naval History and Heritage Command, 2015), 80–81.

[5] Randy Papadopoulos, "Selling a Strategy: Acquiring a New Role and Paying for It," Naval History and Heritage Command, 19 March 2021.

Figure 33. Nelson C. Drummond

Source: *FBI Annual Report 1964* (Washington, DC: Federal Bureau of Investigation, 1964), 25.

U.S. Navy yeoman Nelson C. Drummond.

Europe and Africa Command in Naples, Italy). Due to a variety of personal problems, he was chronically short of money.[6]

Initiation and Espionage

In August 1957, Drummond allegedly called the Soviet embassy in London from a pay phone and offered his services. After Drummond identified himself, the Soviets said that they were not interested and hung up. Drummond then attempted to hold up a store but was scared off. A few days later, he claimed to have encountered a Soviet military intelligence officer (Main Intelligence Directorate, or GRU) on the street who threatened to expose his robbery attempt if he did not

[6] *Espionage* (Washington, DC: Naval Investigative Service, 1989), 8; "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)," U.S. Court of Appeals for the Second Circuit, 26 May 1965; and Pierre J. Huss and George Carpozi Jr., *Red Spies in the UN* (New York: Coward-McCann, 1965), 215–39.

cooperate with them and commit espionage. The GRU officer offered Drummond cash for classified documents.[7]

For the next five years, Drummond stole classified documents and sold them to the Soviets. On one occasion, short funds, Drummond even openly sought out his handler at the Soviet embassy in London. In 1958, the U.S. Navy's Office of Naval Intelligence (ONI) investigated and polygraphed Drummond after he was reportedly seen with a Soviet diplomat in London. However, his Soviet handlers had warned Drummond of the ONI investigation and suspended his operations.[8]

Later that year, Drummond transferred to the destroyer USS *Caperton* (DD 650) in Newport, Rhode Island. During his tour, *Caperton* made a deployment to the Mediterranean prior to decommissioning.[9] In 1960, Drummond transferred ashore to Mobile Electronic Technical Unit 8 (METU 8) in Newport. The METU was an electronics repair unit staffed by subject matter experts who traveled to ships and stations throughout the Atlantic region to repair sensitive shipboard electronic sensor and weapons systems. During this time, Drummond's Soviet handlers supplied him with espionage tradecraft such as hollowed-out magnets, miniature cameras, flash paper, and invisible writing materials. Drummond regularly sold the Soviets classified documents from *Caperton* and METU 8.[10]

According to an ONI publication in 1963, "There is accumulated evidence gathered from [Drummond's] co-workers and associates that because of his expensive vices he was always in debt and borrowed

[7] "Drummond, Nelson Cornelious," Office of Naval Intelligence, 1971, cited portion declassified by the Naval Criminal Investigative Service (NCIS) per NCIS Memo 3850 Ser 22/21U0253, 19 August 2021; "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)"; and Huss and Carpozi, *Red Spies in the UN*.
[8] "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)"; and Huss and Carpozi, *Red Spies in the UN*.
[9] "H.G. States Is Serving aboard USS *Caperton*," *Helena (OK) Star*, 2 July 1959.
[10] "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)"; and Huss and Carpozi, *Red Spies in the UN*.

money constantly."[11] Living beyond his means, Drummond received payments averaging $500 ($4,000 today) for each delivery of classified documents, which he used to repay his heavy personal debts. On several occasions, Drummond openly sought out his Soviet handlers at the Soviet United Nations Mission and even at one GRU officer's apartment. In November 1961, on demand, Drummond received a special payment of $6,000 ($50,000 today) from his Soviet contact and used the funds to purchase the Havana Bar and Grill at 12 Oak Street in Newport.[12]

Investigation and Punishment

At that same time, Drummond's Soviet handlers in New York were working alongside another GRU officer named Dmitiri Polyakov. In November 1961, disillusioned with the Soviet government, Polyakov volunteered to the U.S. Federal Bureau of Investigation (FBI). Given the code name Top Hat, Polyakov would spy on the GRU for the United States for the next 20 years. One of his first reports was about a document that Drummond had sold.[13] Both FBI spy Robert Hanssen and U.S. Central Intelligence Agency (CIA) spy Aldrich Ames later betrayed Polyakov, and the Soviets executed him in 1988.[14]

As a result of Polyakov's tip about the document, the FBI and ONI identified Drummond in June 1962 and began surveillance in August. One evening in late September, after METU 8 had secured for the day, agents monitoring Drummond's office through closed-circuit television (CCTV) observed him removing papers from a classified file and

[11] *FBI Annual Report, Fiscal Year 1964* (Washington, DC: Federal Bureau of Investigation, 1964), 24–25; and *Guide for Security Orientation, Education and Training* (Washington, DC: Office of Naval Intelligence, 1965), paragraph 0505.
[12] "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)"; and Huss and Carpozi, *Red Spies in the UN*.
[13] Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (New York: Farrar, Straus and Giroux, 2015), 224–25; and *Espionage*, 8.
[14] Erin Blakemore, "The Spy Who Kept the Cold War from Boiling Over," History Channel, 15 July 2019.

placing them in his bag. He then drove to a diner in Larchmont, New York. The FBI waited until Drummond and his Soviet handler were together in Drummond's vehicle and then arrested them both, along with the Soviet handler's driver. The FBI found eight classified documents on the car seat between Drummond and his handler.[15] Drummond later admitted that he had passed so many documents to the Soviets that he could not accurately account for all of them.[16]

Drummond was tried in federal court for violations of the espionage statute. His first trial resulted in a hung jury, but he was convicted in the second trial and sentenced to life. Drummond served 10 years before being released.[17]

Significance

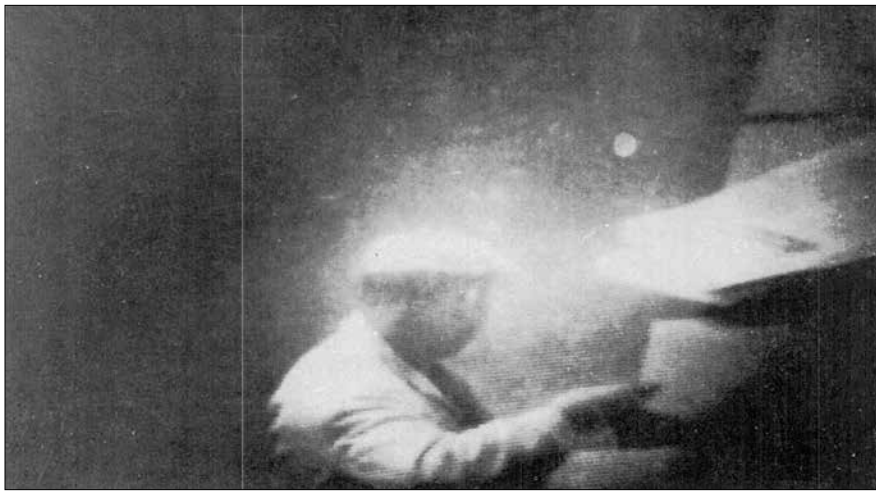
Drummond was another financial volunteer because he sought out the Soviets to solve his debt problems. Militarily, this was another failure, as Drummond compromised an alarming number of the DON's weapons and sensors over several years before the FBI identified him. Even after the FBI arrested Drummond, the full extent of the compromise could not be determined. Consequently, for years the DON could never be certain if the Soviet Navy had achieved an *unexpected manner advantage* over the U.S. Navy.

Lessons Learned

The Drummond case presented a series of firsts. He was the first active-duty U.S. Navy sailor convicted of espionage. He was also the only DON espionage subject considered in this study known to have

[15] *Espionage*, 8.
[16] "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)"; and Huss and Carpozi, *Red Spies in the UN*.
[17] "United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)"; "Drummond Gets Life Sentence," *Baltimore* (*MD*) *Sun*, 16 August 1963, 7; "Drummond, Nelson Cornelious"; and "Drummond, born in 1928," LocateAncestors.com, accessed 2 March 2021.

Figure 34. Drummond committing espionage



Source: *FBI Annual Report 1964*
(Washington, DC: Federal Bureau of Investigation, 1964), 25.
Nelson C. Drummond removing classified documents to sell to Soviet agents.

successfully lied through a polygraph exam. His was the first DON espionage case predicated on information derived from the penetration of an adversary intelligence service. Those leads were often the only way to detect an espionage operation once the adversary applied the tradecraft necessary to securely meet and exchange information and money. Drummond's case was also the first DON espionage case to use CCTV to surveil a subject in the workplace. Finally, his was the first DON case in which naval counterintelligence and the FBI worked together seamlessly. That cooperation would be the key to solving dozens more espionage cases during the next 50 years.

Nuclear Threats

As mentioned earlier in this chapter, for the first 13 years of the Cold War Soviet intelligence had little strategic interest in the U.S. Navy. In 1960, the first successful launch of the nuclear-armed UGM-27 Polaris

Figure 35. Holy Loch, Scotland

Source: Wikimedia Commons.

In March 1961, U.S. Navy submarine tender USS *Proteus* (AS 19) and ballistic missile submarine USS *Patrick Henry* (SSBN 599) conducted the first refit at Site-1 in Holy Loch, Scotland.

submarine-launched ballistic missile (SLBM) compelled Soviet intelligence to focus more attention on the new and dangerous threat posed by U.S. ballistic missile submarines (SSBN). The Polaris could carry a nuclear warhead from under the water out to a range of 1,500 nautical miles and later 2,500 nautical miles. Polaris was a disruptive technology that caused a major shift in the international nuclear balance because it put most of the Soviet Union within range of U.S. nuclear missiles that could be launched from undetectable launch sites just off the coast.[18]

[18] Adm Ignatius J. Galantin, USN (Ret), *Submarine Admiral: From Battlewagons to Ballistic Missiles* (Chicago: University of Illinois Press, 1995), 231, 239, 241; "Submarine Weapons: Ballistic Missiles," Smithsonian Institution, accessed 16 March 2021; *Forty-One for Freedom: A Fleet Is Built* (Washington, DC: U.S. Department of the Navy, 1968), approx. 20 mins.; and John M. Watson, "The Origin of the APL Strategic Systems Department," *Johns Hopkins APL Technical Digest* 19, no. 4 (1998).

The "nuclear balance" theory on which peace rested held that neither side would use nuclear weapons first because if either side detected bombers or missiles heading their way, they could launch a retaliatory strike, and both sides would destroy each other.[19] Donald Brennan, a former president of the Hudson Institute, ironically called the theory "mutual assured destruction" or "MAD" in a *New York Times* editorial in 1971. Polaris shortened the time for a first strike so much that the Soviets would not have had time to retaliate, leaving them defenseless. As a result, with little notice and no ability to locate Polaris-equipped submarines, U.S. Navy subsurface operations went from a minor to a critical Soviet intelligence collection target as the Soviets sought an immediate *time, place, and manner advantage* over this new threat.[20]

As soon as the first Polaris-equipped submarines were ready for deployment, the U.S. Navy began continuous SSBN patrols off the coast of the Soviet Union. To maximize this effort, the Navy repaired and refitted submarines and swapped their crews at a base along Scotland's Holy Loch called "Site One."[21] This made Holy Loch a major Soviet intelligence target. By observing the movements of SSBNs at Holy Loch, the Soviets hoped to be able to queue other collectors to locate them so that the Soviet Navy could position its own assets to destroy the SSBNs if required.[22]

As with Japanese interest in new U.S. aircraft carrier technology and techniques in the 1930s, there is little evidence to suggest that U.S. naval counterintelligence understood the massive shift in the threat from Soviet intelligence once SSBN patrols commenced off the coast of the Soviet Union.

---

[19] *Forty-One for Freedom: A Fleet Is Built*; and *The Submarine, Part II: Backgrounds, Characteristics and Missions of Nuclear Powered Submarines* (Washington, DC: U.S. Department of the Navy, 1971), approx. 29 mins.
[20] Donald G. Brennan, "Strategic Alternatives I," *New York Times*, 24 May 1971.
[21] Galantin, *Submarine Admiral*, 231, 239, 241.
[22] Harry Houghton. "I Betrayed My Country—And the Woman I Love: The Lonsdale Spy Ring," *Ottawa* (*ON*) *Citizen*, 9 September 1961, 41.

That was where the second Cold War case brief began, with Soviet intelligence agents attempting to track SSBNs from Holy Loch in Scotland in an urgent bid to realign the nuclear balance. U.S. naval counterintelligence, detached from ONI in 1966 and now called the Naval Investigative Service (NIS), was there but was reliant on British counterintelligence.

1967: Garry L. Ledbetter

Background

In 1967, Garry L. Ledbetter was a married 25-year-old shipfitter second class aboard the submarine tender USS *Simon Lake* (AS 33), which had arrived in Holy Loch a few months earlier to service the Polaris-equipped SSBNs deploying from there. A submarine tender had been stationed at Site One since March 1961 to reduce the two-week round trip back to the East Coast of the United States. USS *Proteus* (AS 19) arrived on 3 March 1961, and USS *Patrick Henry* (SSBN 599) arrived on 9 March, mooring alongside *Proteus*.[23]

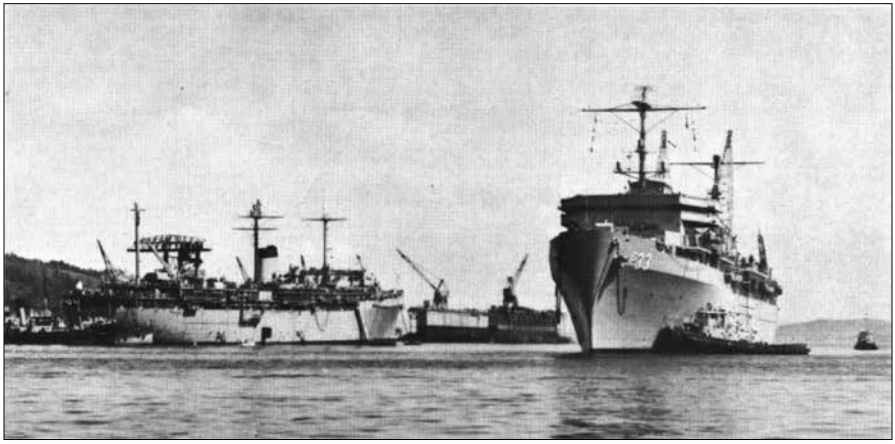
Months before the U.S. Navy arrived, Soviet intelligence had already begun placing assets in the Holy Loch area to observe the movements of the SSBNs operating from there.[24]

---

[23] Brian Lavery, "The British Government and the American Polaris Base in the Clyde," *Journal for Maritime Research* 3, no. 1 (2001): 130–45, https://doi.org/10.1080/21533369.2001.9668315; "U.S. Sailor Convicted of Charge," *Daily Herald* (Provo, UT), 27 August 1967; Gary Flynn, "U.S. Submarine Base: Site One, Holy Loch, Scotland," AboutSubs.com, accessed 16 February 2016; "Deck Log Book, USS *Proteus* (AS 19), 1–31 March 1961," Record Group (RG) 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Proteus* (AS 19)–March 1961, NAID: 203382218, National Archives and Records Administration, College Park, MD, 13; "Deck Log Book, USS *Patrick Henry* (SSBN 599) 1–31 March 1961," RG 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Patrick Henry* (SSBN 599)–March 1961, NAID: 218495306, NARA, 20; and "Deck Log Book, USS *Simon Lake* (AS 33) 1–31 July 1966," RG 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Simon Lake* (AS 33)–July 1966, NAID: 215129454, NARA, 44.

[24] Houghton, "I Betrayed My Country—And the Woman I Love."

Figure 36. USS *Simon Lake* (AS 33)



Source: *All Hands* (October 1966): 35.

U.S. Navy shipfitter second class Garry L. Ledbetter's ship, USS *Simon Lake* (AS 33), arriving in Holy Loch, Scotland, in July 1966.

Initiation and Espionage

Six years later, in 1967, the Soviet surveillance operation continued with the dispatch of a 26-year-old East German ship's cook named Peter Dorschel. Recruited earlier that year by Soviet agents in East Germany, Dorschel moved to Dunoon, Scotland, to observe the nearby Site One and elicit information from U.S. sailors. The Soviets tasked Dorschel with notifying them of the movement of SSBNs in and out of Holy Loch by letter using an open code involving different colored pencils and numbers for each of the submarines based there.[25] Dorschel, however, was unable to gather much information and turned in desperation to a local bookmaker named William MacAffer for help.[26]

[25] "Holy Loch Spy Gets Seven Years," *Birmingham* (*UK*) *Evening Mail and Despatch*, 23 June 1967, 1.

[26] "Seven Years for 'Little Fish' Spy," *Guardian*, 24 June 1967, 3; and "E. German Gets 7 Yrs. as Polaris Sub Spy," *Evening Journal*, 23 June 1967, 26.

Ledbetter, who was carrying on an extramarital affair with MacAffer's sister, sold MacAffer a restricted training manual to sell to Dorschel.[27]

Investigation and Punishment

At the same time, MacAffer reported Dorschel to the British authorities, and it became clear that a U.S. sailor was involved. U.S. Navy officers in Holy Loch called NIS, and agents quickly identified Ledbetter. During questioning by NIS, Ledbetter confessed.[28]

Ledbetter was court-martialed aboard *Simon Lake* in August 1967 and convicted of Uniform Code of Military Justice violations regarding unauthorized disclosure. He was sentenced to six months and a bad conduct discharge.[29] Dorschel pled guilty to violating the British Official Secrets Act and was sentenced to seven years, but he only served three and was deported.[30] Though MacAffer was also charged with violating the Official Secrets Act, the charges against him were dropped.[31]

Significance

Ledbetter represents a recruitment-in-place because Dorschel sought him out specifically for the information he might be able to access. Thanks to MacAffer, this case was militarily effective. British and U.S. authorities revealed the full scope of the compromise before Ledbetter

[27] "Seven Years for 'Little Fish' Spy"; "MacAffer Says He Spied for Britain and U.S.," *Glasgow* (*UK*) *Herald*, 6 September 1967, 7; "Couple Wed in Woodlawn EUB Church," *Bucyrus (OH) Telegraph-Forum*, 23 March 1961, 4; "Notice for Service of Summons by Publication in Common Pleas Court of Crawford County, Ohio," *Bucyrus (OH) Telegraph-Form*, 2 December 1967, 11; "Sailor Denies Anti-Security Allegations," *Arizona Daily Star*, 25 August 1967, 15; and "Dorschel Gives Evidence in Camera," *Guardian*, 25 August 1967, 16.

[28] "Midnight Questions on Polaris," *Guardian*, 26 August 1967, 12.

[29] "Deck Log Book, USS *Simon Lake* (AS 33) 1–31 August 1967," RG 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Simon Lake* (AS 33)–August 1967, NAID: 215545799, NARA, 49–53; and "U.S. Sailor Convicted of Charge," *Daily Herald* (Provo, UT), n.d.

[30] "Seven Years for 'Little Fish' Spy"; and "Spy's Wife Awarded Decree," *Guardian*, 23 October 1970, 7.

[31] "Charge under Secrets Act Dropped," *Guardian*, 6 September 1967, 3.

could do any serious damage. The Soviets did not achieve an *unexpected manner advantage*. They did, however, achieve an *unexpected time and place advantage* because, in theory, Dorschel should have been reporting the movements of the SSBNs at Holy Loch. However, readers will recall that shore establishment espionage was often of tertiary importance, with the most glaring exception being the Yoshikawa case at Pearl Harbor. If the Soviet Union and the United States had been close to war, Dorschel's espionage could have been strategically significant.

Lessons Learned

Ledbetter was the DON's first overseas espionage case and NIS's close cooperation with British counterintelligence was a success. This case was also the first time that naval espionage involved a criminal acting as an intermediary between a subject and a foreign intelligence service. Similar cases would follow. Finally, Ledbetter was the first Soviet espionage targeting the U.S. Navy's SSBNs and should have initiated a reevaluation of the DON's counterintelligence operational priorities that might have prevented the damage caused by a different soon-to-begin SSBN case.

A Serious Blow

Just a few months after news of the Soviet intelligence failure at Holy Loch broke, another submarine espionage case began. The Soviets still could not locate U.S. SSBNs, and now U.S. and British counterintelligence had interrupted their surveillance of Site One. They were at a critical *time and place disadvantage*.

One of the best kept secrets of World War II was the Allied effort to break the German code machine called Enigma. Among other triumphs, reading coded German radio messages helped the Allies find and sink 95 percent of the German submarine fleet and win the Battle of the Atlantic. An even closer held secret was the fact that the key to

unlocking the code was a German spy, Hans Thilo Schmidt. Schmidt's brother was friends with the director of the office that created the codes and who hired his friend's brother out of pity. Schmidt squandered his salary, and when he ran out of funds in 1931, he walked into the French embassy in Berlin and volunteered to spy. Schmidt sold the French the Enigma operating manual and about eight months of the code settings. With that information, during several years, the Allies were able to break the code.[32]

That was where the next case brief began, with the Soviets desperate to find U.S. SSBNs and a senior radioman troubled at home.

1967: John A. Walker

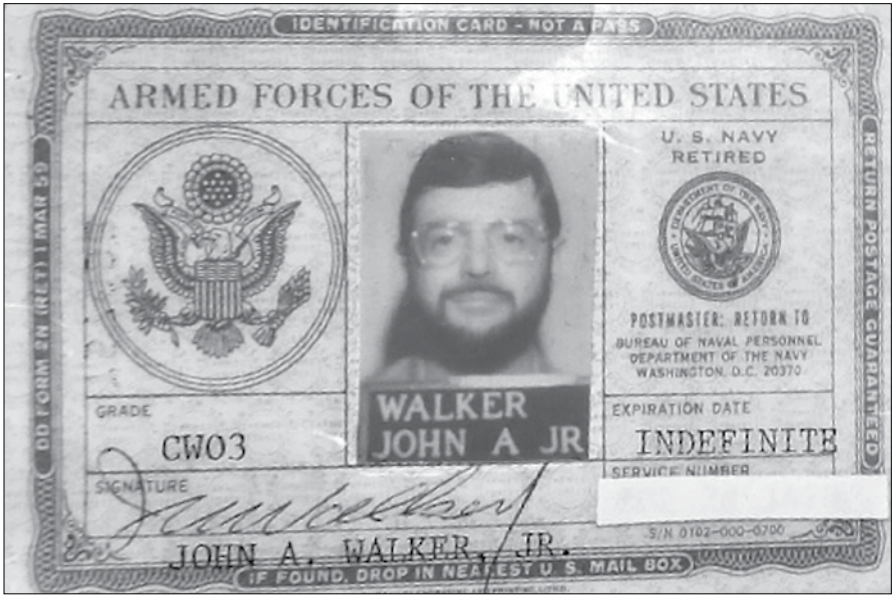
Background

It all started with a bar. In 1966, John A. Walker was a married 29-year-old U.S. Navy chief radioman with 11 years of service, and he was already starting to look toward retirement. Along with Bill Wilkinson, a shipmate from USS *Simon Bolivar* (SSBN 641), home ported in Charleston, South Carolina, he invested his life savings into a single-story cinderblock house on U.S. Route 78 in Ladson, South Carolina. The location seemed perfect for a bar, right across the street from a General Electric Plant and just down the road from the Naval Weapons Station.[33]

Then the plan started to fall apart. Wilkinson backed out and took his money, the renovation expenses ran over budget, and Walker had not counted on the taxes. Before it even opened, Walker's mistakes doomed the "Bamboo Snack Bar."[34]

[32] Jennifer Wilcox, *Solving the Enigma: History of the Cryptanalytic Bombe* (Washington, DC: Center for Cryptologic History, National Security Agency, 2015).
[33] Pete Earley, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1988), 54–55; "Property of Convicted Spy to Be Sold at Public Auction," *Index Journal* (Greenwood, SC), 5 February 1987, 17; and "Walker with Wilkinson," Associated Press, 1965.
[34] Earley, *Family of Spies*, 70–71.

Figure 37. John A. Walker identification card



Source: Federal Bureau of Investigation.

U.S. Navy chief radioman John A. Walker's retired Navy identification card.

Then, in 1967, Walker received a promotion to chief warrant officer and was transferred to serve as a communications watch officer at commander, Submarine Force Atlantic in Norfolk, Virginia. He was responsible for four classified radio networks broadcasting messages to deployed SSBNs. Walker was a geographic bachelor; his wife and children lived in a trailer behind the bar, which she tried to run at a profit. Faced with the severe financial pressure, both he and his wife were drinking heavily and having extramarital affairs.[35]

Initiation and Espionage

By that summer, Walker was close to despair. He contemplated suicide, but then a late-night bull session with some fellow radiomen about sell-

[35] Maj Laura J. Heath, USA, "An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967–1974, as Exploited by CWO John Walker" (thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2005).

ing classified information to the Soviets gave him an idea. He decided his way out was to commit espionage. It was a desperate move, and he later explained that he expected the FBI to catch him immediately.[36]

In October, Walker stole a settings list for the KL-47 cryptographic device. This machine was a direct descendant of the German Enigma and was the most widely used device in the U.S. military at the time.[37] He walked out of the communications center with it and drove to the Soviet embassy in Washington, DC.[38]

The FBI should have caught Walker right there, but there is no record that their surveillance noticed his approach to the embassy. By the 1960s, the FBI had established an observation post in an office of the National Geographic Society's headquarters across the street. From behind the magnolia trees on the southwest corner of the building, the FBI would have had a perfect view of Walker as he paced up and down the street and then dashed through the vehicle gate.[39] However, the placement of the FBI observation post limited surveillance of the embassy; they could only photograph the faces of people leaving, not entering, explaining how they missed Walker.[40] An alternative theory was that Walker volunteered earlier at an overseas Soviet embassy.[41]

Inside the embassy, Soviet staff took Walker to speak with the veteran Committee for State Security (KGB) security officer, who was responsible for the initial debriefs of walk-ins. Using an older officer in this way ensured that double agents could not expose newly assigned case officers. The security officer took some convincing but eventually

[36] Earley, *Family of Spies*, 14–16, 58–59.
[37] *A History of U.S. Communications Security Post World War II* (Washington, DC: National Security Agency, 1973), 77–82. Declassified in 2011.
[38] Earley, *Family of Spies*, 60–62.
[39] Robert M. Poole, *Explorer's House: National Geographic and the World It Made* (New York: Penguin, 2004), 216–17.
[40] Nigel West, *Historical Dictionary of Cold War Counterintelligence* (Lanham, MD: Scarecrow Press, 2007), 284.
[41] Heath, "An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System," 56–57.

believed that Walker was selling genuine cryptographic material. The Soviets paid Walker for the material, gave him recontact instructions, and then, avoiding the FBI across the street, drove him back to his car using an extensive surveillance detection route. Walker then drove back to Norfolk.[42]

For the next two years, Walker provided the Soviets with a steady supply of cryptographic material using dead drops in the Washington, DC, area. He paid off his debts and spent money freely. In April 1968, he finally leased the bar in South Carolina to someone else and his family joined him in Norfolk. It was not long before his wife became suspicious, found evidence of his espionage, and confronted him. He confessed and she did nothing. Then, in 1969, Walker transferred to a Navy radio school in San Diego, California, where he lost access to classified information. The Soviets reduced his pay.[43]

In 1971, Walker transferred to the combat stores ship USS *Niagara Falls* (AFS 3), home ported in San Diego, where he again had access to cryptographic material. He continued to deliver the material at dead drops in the Washington, DC, area. Walker transferred back to Norfolk in 1974 and retired in 1976. His family left him and moved to Maine.[44]

Fearing the loss of income after retirement, Walker recruited a former colleague from the radio school, Jerry A. Whitworth.[45] Whitworth continued to provide Walker access to cryptographic material for the next three years. The espionage weighed heavily on Whitworth. He took early retirement in 1983 to end his involvement and in 1984 wrote three anonymous letters to the FBI outlining the plot and requesting immunity.[46]

---

[42] Earley, *Family of Spies*, 63–67.
[43] Earley, *Family of Spies*, 68–72, 76–77, 78–80, 84–85.
[44] Earley, *Family of Spies*, 98, 104–5, 106–9, 143–44.
[45] Earley, *Family of Spies*, 129–35.
[46] Earley, *Family of Spies*, 146–62, 168–69, 174, 271, 279–83.

Walker, meanwhile, kept the money flowing by recruiting first his brother Arthur, a retired Navy officer turned contractor, and then his son Michael, now in the Navy, to maintain his access to classified information. However, neither had access to cryptographic material. By now, Walker was making trips overseas to meet his Soviet handlers.[47]

Investigation and Punishment

In July 1984, Walker's estranged wife visited him in Norfolk and saw how well he was living. She demanded money or she would finally report him. Mistakenly convinced that she knew her son was now involved and that she would not incriminate him, Walker refused to pay her. She returned to Cape Cod, where she now lived, and in November 1984 called the FBI.[48] Walker's failure to keep his own secret was his downfall, as his wife, brother, son, and colleague all knew what he was doing. Conversely, the Soviets had learned lessons from earlier failures and kept the Walker case extremely compartmentalized. Only a handful of senior KGB officers ever knew Walker's name.[49]

The FBI did not take Walker's wife's allegation seriously at first. They waited two weeks to interview her and dismissed her allegations because she drank heavily during the interview.[50] However, when the agent filed the report in February 1985, other agents took a harder look. The FBI notified NIS in March 1985. The ensuing investigation confirmed much of what Walker's wife had said, and in May 1985 the FBI arrested Walker as he loaded a dead drop with classified documents stolen by his son from the aircraft carrier USS *Nimitz* (CVN 68).[51]

In the end, the KBG paid Walker more than $1 million, and his espionage, along with cryptographic devices seized from the environ-

[47] Earley, *Family of Spies*, 268–69.
[48] Earley, *Family of Spies*, 275–79, 284–87; and "John Walker," Federal Bureau of Investigation, accessed 2 September 2023.
[49] Pete Earley, "Interview with the Spy Master," *Washington Post*, 23 April 1995.
[50] Earley, *Family of Spies*, 295–98, 302–5.
[51] Earley, *Family of Spies*, 322–27.

mental research ship USS *Pueblo* (AGER 2) when it was captured by North Korea in 1968, allowed the Soviets to compromise millions of classified messages sent over U.S. Navy radio circuits.[52] Walker's espionage today would be roughly equivalent to allowing an adversary to download 400 gigabytes of classified information over nearly 20 years. The Soviets boasted that Walker's espionage would have allowed them to win World War III.[53] Separately, U.S. secretary of the Navy John F. Lehman Jr. agreed. The year after Walker's arrest, he equated the Walker case to the Allied effort during World War II to break the German Enigma code, noting, "Luckily, it [the Walker case] did not happen in the middle of a war."[54] Walker was reportedly the highest rated Soviet agent in history.[55]

Walker pled guilty to violating the espionage statute in exchange for leniency for his son and was sentenced to two life terms. His brother Arthur was convicted of violating the espionage statute and was also sentenced to two life terms.[56] Likewise, Whitworth was sentenced to 365 years vice life and will be eligible for parole in 2045 when he is 106 years old.[57] Walker's son Michael also pled guilty to violating the espionage statute and was sentenced to 25 years, which was reduced to 15 years in exchange for his father's cooperation.[58]

---

[52] Pamela A. MacLean, "Defector: Walker Spy Ring a Gold Mine for KGB," United Press International, 29 August 1986; Heath, "An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System," 2–3, 14, 54–55; and Earley, "Interview with the Spy Master."
[53] Earley, *Family of Spies*, 180; George C. Wilson, "Soviet Submarines 'Have Closed the Gap,'" *Washington Post*, 3 April 1987; and Robert C. Toth, "Change in Soviets' Sub Tactics Tied to Spy Case: Material Reportedly Available to Walkers May Have Tipped Kremlin to Vessels' Vulnerability," *Los Angeles Times*, 17 June 1985.
[54] "Extensive Damage Done by Spy Ring," *Arizona Daily Sun*, 25 July 1986.
[55] Earley, *Family of Spies*, back cover flap.
[56] *Espionage*, 18.
[57] "Whitworth Gets 365 Years—Eligible for Parole in 60: 'I'm Sorry,' Navy Spy Tells Judge," *Los Angeles Times*, 28 August 1986.
[58] Earley, *Family of Spies*, 358.

The Walker brothers would have been eligible for parole in 2015 but both died in 2014.[59] Whitworth remains in prison in the U.S. Penitentiary in Atwater, California.[60] Michael Walker was released in 2000.[61]

Significance

Walker was a typical financial volunteer, a man in severe debt and in crisis who made a desperate choice. He slipped past all the DON's security measures and in 1967 slid through the FBI's counterintelligence net surrounding the Soviet embassy in Washington, DC. According to a history of the U.S. National Security Agency, "Cryptographic data supplied to the Soviets by the Walker espionage ring together with cryptographic equipment seized aboard the Pueblo would enable the Soviets to read US naval communications for years."[62] After an initial three-week damage assessment in 1985, the chief of naval operations, Admiral James D. Watkins, characterized the damage as serious but not catastrophic, noting that "the Soviets know of our ability to find and target their submarines" and that "we have witnessed [the Soviets] gaining on us in the technical differential, which was significant 10 years ago but has been shrinking. Perhaps Walker contributed to that shrinkage." Watkins claimed that the Soviets had not gained the ability to track and sink SSBNs, but intelligence officials suspected that Walker's revelations caused the Soviets to step up efforts to detect U.S. sub-

[59] Martin Weil, "John A. Walker Jr., Who Led Family Spy Ring, Dies at 77," *Washington Post*, 30 August 2014; and "Convicted U.S. Spy Arthur Walker Dies in Prison," Associated Press, 10 July 2014.
[60] "Find an Inmate: Jerry Alfred Whitworth," Bureau of Prisons, accessed 25 February 2021.
[61] "Find an Inmate: Michael Lance Walker," Bureau of Prisons, accessed 25 February 2021.
[62] Robert E. Newton, *The Capture of the USS* Pueblo *and Its Effect on SIGINT Operations* (Fort Meade, MD: Center for Cryptologic History, National Security Agency, 1992) 167. Declassified in 2023. This publication describes the effect of the Walker compromises on U.S. communications and signals intelligence operations.

marines.[63] Because Walker compromised command and control, the most significant form of espionage, his case became the most strategically significant in the history of the DON. It was also the most militarily ineffective investigation in the department's history. For perhaps a portion of Walker's espionage career, the Soviet Union had a *time, place, and manner advantage* over the DON, but the full extent of the advantage gained by the Soviet Union may never be fully understood.

Lessons Learned

The choice that Walker, and others like him, made brought into focus the DON's system-wide failure to address low pay, poor living conditions, and substance abuse. Failure to care for personnel resulted in higher rates of all crime, including espionage. This failure haunted the department for years. From an investigative perspective, this was only the second time in history that a significant other reported espionage that resulted in prosecution, the first being Thompson's roommate nearly 50 years earlier. More such cases would follow, and naval counterintelligence would demonstrate a mixed response to the DON's detriment. Once the FBI launched an investigation, surveillance was again a key element. The behavior of the Soviets suggested that they were aware of FBI surveillance in 1967, but catching Walker in the act in 1985 was crucial. Similar surveillance was part of most of the espionage investigations considered in this study, and only adequate numbers of trained, experienced surveillance personnel accomplished the task well.

[63] Robert Toth, "Worst Spy Loss Felt in Navy Sub Communication," *Los Angeles Times*, 12 June 1985, 1; and Toth, "Change in Soviet's Spy Tactics Tied to Spy Case."

The Crayon Box of Secrets

After Walker's 1967 walk-in to the Soviet embassy in Washington, DC, the Soviets literally had the "key" to the U.S. Navy's classified information vault. With the information they derived from decrypting the Navy's communications, the Soviets were able to achieve and maintain a *time, place, and manner advantage* over the Navy for nearly two decades and put at risk one leg of the U.S. nuclear triad. They had little need for other spies inside the DON, and for the next 13 years there were no other Navy spies found to have committed espionage on behalf of the Soviet Union. It would not be until 1980, when the cryptographic information from Walker dried up, that the Soviets began taking on new U.S. Navy volunteers.

During the early Cold War, the DON's counterintelligence efforts were based on an erroneous operational prioritization and, like all U.S. counterintelligence, hamstrung by insufficient legislation. As Navy officials became increasingly suspicious of the rapid advances in Soviet submarine and antisubmarine warfare, the absence of Soviet espionage in the Navy was a clue they overlooked.[64] However, detecting that clue and investigating the reasons behind it would have been extremely difficult because U.S. military counterintelligence at the time prioritized background investigations. For example, in 1966, 68 percent of all NIS cases, including criminal investigations, were background investigations, a mission which NIS was forced to retain until 1972.[65] Moreover, NIS had no dedicated counterintelligence investigators until after 1980.[66] John Walker's only brush with NIS before his arrest was a 1964 background investigation, which surfaced only his 1955 juvenile ar-

[64] Toth, "Change in Soviets' Sub Tactics Tied to Spy Case."
[65] *Naval Investigative Service Activities Report, 1966* (Washington, DC: Naval Investigative Service, 1967), C-3; and "History of the NCIS," in *Commanding Officer's Guide to NCIS* (Washington, DC: Naval Criminal Investigative Service, n.d.).
[66] Hearing before a Subcommittee of the House Committee on Government Operations, 99th Cong. (17 June 1985), 64.

rest for burglary—the original impetus for his Navy enlistment.[67] Additionally, a lack of legislation meant that classified information was extremely difficult to use in court.[68] All of these institutional shortfalls meant that few espionage cases were initiated within the DON throughout the early Cold War.

Only two espionage cases were prosecuted in the DON between 1967 and 1980, both of which were borne of desperation and ultimately unsuccessful. The following case brief was the first of them.

1968: Edward H. Wine

Background

In August 1968, Edward H. Wine, a former Marine, was a married 30-year-old sonar technician first class assigned to the shore patrol of the Naval Submarine Base in New London, Connecticut. Wine was disgruntled because Navy officials had denied his request for transfer from the attack submarine USS *Skate* (SSN 578) to USS *Fulton* (AS 11), a submarine tender in New London that rarely left port. Instead, the Navy issued Wine orders to Key West, Florida. Previously arrested along with his brother in 1964 for a drunken bar brawl while assigned to the submarine USS *Becuna* (SS 319), Wine was now experiencing marriage problems and drinking heavily.[69]

Initiation and Espionage

As a work aid aboard *Skate*, Wine had created classified "cheat sheets" of U.S. and foreign ships' acoustic signatures. Handwritten on index cards, he stored them in a crayon box at home. One drunken night,

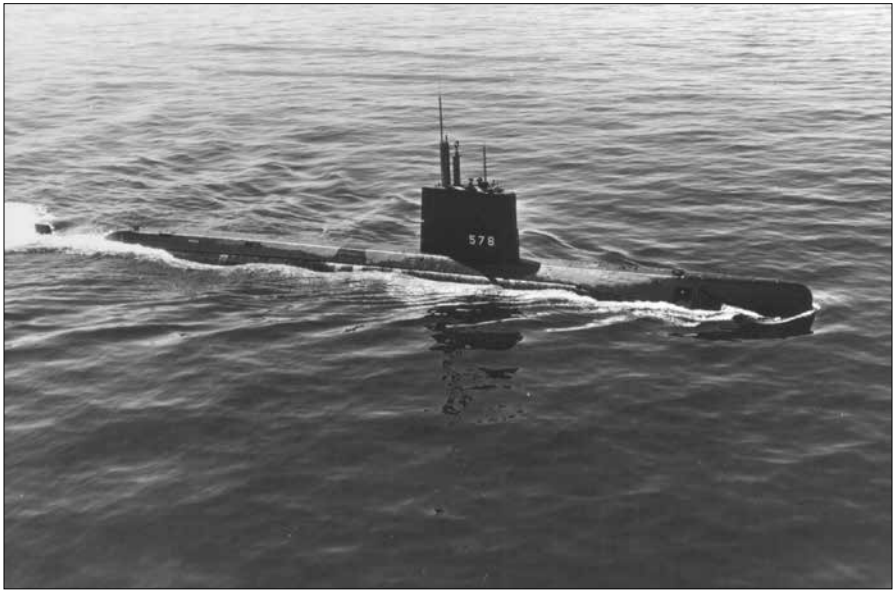
---

[67] Earley, *Family of Spies*, 31, 51.

[68] Melanie Reid, "Secrets behind Secrets: Disclosure of Classified Information before and during Trial and Why CIPA Should Be Revamped," *Seton Hall Legislative Journal* (5 May 2011), 272–73.

[69] "Brothers Held in Grill Fight," *Hartford* (*CT*) *Courant*, 22 December 1964, 3; and James Healion, "Navy Petty Officer Denies Any Intention of Selling Secrets," *Naugatuck* (*CT*) *Daily News*, 24 March 1969, 5.

Figure 38. USS *Skate* (SSN 578)



Source: NavSource Naval History Submarine Photo Archive, n.d.

U.S. Navy sonar technician first class Edward H. Wine's boat, USS *Skate* (SSN 578), conducting local operations near New London, CT, 1963.

Wine hit on a scheme to make some money by selling the index cards to the Soviets. He gave six of them to a drinking partner, Tom O'Neill, to take to New York City for him, to ensure his own security.

Investigation and Punishment

O'Neill had second thoughts and reported the plan to the FBI, who recruited him as a source and notified NIS.[70] O'Neill met with Wine for six weeks, and the pair made an abortive trip to New York City to visit the Soviet United Nations mission but turned back.[71]

[70] *Espionage*, 22.

[71] Thomas Failla, "Tipster Has Troubles," *Daily Times-Mail* (Bedford, IN), 13 November 1974, 21; and "State Sailor Is Serving Term for 'Mishandling' Secret Data," *Bridgeport* (*CT*) *Post*, 24 March 1969, B IX.

Wine pled guilty to mishandling classified information in a general court-martial and was sentenced to three years at Portsmouth Naval Prison in Kittery, Maine.[72] He was a model prisoner and only served one year before returning to active duty at his old rank. However, Wine left the Navy within a few years.[73]

Significance

Wine was another financial volunteer because he sought to sell classified information to the Soviets to solve his debt problems. In this case, the naval counterintelligence response was militarily effective because, thanks to O'Neill, the FBI and NIS intercepted Wine long before he contacted the Soviets. There was never any *unexpected advantage* gained. However, in 1968, the Soviets were just beginning learn how easily the United States could detect their "noisy" submarines. Wine's cheat sheets, had he sold them to the Soviets, may have accelerated that process. Wine's case demonstrates that every espionage attempt in the DON has the potential to be significant unless intercepted.

Lessons Learned

The Wine case marked the first time that a DON espionage subject attempted to involve a witting accomplice (a.k.a. a cut-out) in an espionage scheme. The FBI recruitment of that would-be coconspirator as an informant was a key element of the investigation. Additionally, the Wine case introduced the concept of the "classified hoarder," an individual who brings classified information home and later tries to sell that information. More hoarder espionage will be discussed later.

[72] "State Sailor Is Serving Term for 'Mishandling' Secret Data."
[73] George Gombossy and Paul Frisman, "Ex-Husband Cleared in Double Strangling," *Hartford* (*CT*) *Courant*, 19 October 1974, 10.

New Enemy, New Espionage

The next early Cold War case brief was more important for what did *not* happen than what did happen. After Ledbetter and Wine's abortive attempts at espionage, the DON's focus on background investigations meant that naval counterintelligence did not discover another espionage case for the next 12 years. While the Cold War and the Walker case continued, the DON remained busy with the Vietnam War through 1975. But there was another enemy on the horizon, particularly for the Navy—drug smugglers.

While variations on the term *War on Drugs* had been used since 1967, President Richard M. Nixon officially nationalized the idea in 1971 and announced legislation to "tighten the noose around necks of drug peddlers." Meeting with limited initial success, he expanded the effort by creating the Drug Enforcement Administration (DEA) in 1973.[74] Within a few years, the U.S. government enlisted the Navy's maritime domain awareness assets to assist the DEA and Coast Guard with tracking suspected drug-smuggling boats. The Navy's contribution was to augment the DEA and Coast Guard with its highly classified satellite-based maritime tracking capability and Grumman E-2 Hawkeye airborne early warning missions.[75]

[74] "Executive Order 11599: Establishing a Special Action Office for Drug Abuse Prevention," American Presidency Project, University of California Santa Barbara, accessed 25 November 2023; "President Nixon's Special Message to Congress on Drug Abuse Prevention and Control of June 17, 1971," Nixon Foundation, 4 May 2018; "Executive Order 11727: Drug Law Enforcement," American Presidency Project, University of California Santa Barbara, accessed 25 November 2023; "Sheriff D'Aloia Urges Passage of Narcotic Bill," *Belleville (NJ) Times*, 16 February 1967, 2; and "Nixon Declares War on Drug Abuse," *Charlotte (NC) News*, 17 June 1971, 1.

[75] Thomas O'Toole, "Satellites Used to Round up U.S.-Bound Marijuana Ships," *Washington Post*, 11 July 1978; Jan Brandon, "Drug Interdiction in the Pacific: West Coast Sailors Play Key Role," *All Hands* (June 1990): 36; Lee Bosco, "'80s Issues," *All Hands* (June 1990): 12; and Scott Allen, "Hot on Their Trail: Navy, Law Enforcement Agencies Team up to Stop Drug Smugglers," *All Hands* (June 1990): 18–19.

The War on Drugs created a new type of enemy for naval counterintelligence, a nonstate entity: the drug smuggler. As this study has demonstrated, throughout the first 70 years of naval espionage, whatever country was in the news as the "threat" to the United States attracted the financial volunteer. Once the Navy became involved in War on Drugs, that list now included drug smugglers.

In the meantime, Walker continued to compromise U.S. naval command and control. The United States had come to depend on its tremendous advantage in undersea surveillance and cueing, due primarily to the Sound Surveillance System (SOSUS), which provided deep-water long-range detection of the relatively noisy Soviet submarines. This system gave the general locations of Soviet submarines to tactical assets such as Lockheed P-3 Orion antisubmarine warfare patrol aircraft and attack submarines, making it much easier to find and track them.[76]

By 1973, the SOSUS began to "miss" Soviet attack submarines, which were able to position themselves off the coast of the United States. DON officials questioned how the Soviets knew about SOSUS and its effectiveness.[77]

The answer laid in the millions of messages decrypted by the Soviets with the cryptographic material sold to them by Walker. In those messages were communications of the naval facilities that processed the SOSUS information and transmitted submarine locations to the Naval Ocean Surveillance Information Center, which in turn relayed them to the fleet over the radio circuits Walker compromised.[78] Based on that information, the Soviets were able to piece together that the SOSUS system existed and relied on the noisiness of Soviet subma-

[76] Lt John Howard, USN, "Fixed Sonar Systems: The History and Future of the Underwater Silent Sentinel," *Submarine Review* (April 2011): 1.
[77] Toth, "Change in Soviets' Sub Tactics Tied to Spy Case."
[78] Christopher A. Ford and David A. Rosenberg. "The Naval Intelligence Underpinnings of Reagan's Maritime Strategy," *Journal of Strategic Studies* 28, no. 2 (April 2005): 379–409, https://doi.org/10.1080/01402390500088627.

rines.[79] So, in 1968, the Soviets initiated a crash program to quiet their submarines, aided by the feedback loop relayed to the Soviets through the decrypted U.S. Navy messages.[80]

That was where the next case brief started. While the Navy struggled to comprehend its setbacks, Walker continued to compromise U.S. naval command and control. Meanwhile, the Navy's most sensitive systems were partially refocused on a different enemy that presented yet another counterintelligence challenge.

1979: Lee E. Madsen

Background

In July 1979, Lee E. Madsen was a 24-year-old yeoman third class assigned to the Special Security Office at the Pentagon managing the security of a joint Defense Intelligence Agency/CIA analysis cell called the National Warning Staff, which provided warning primarily for an attack by the Soviet Union or the People's Republic of China.[81] As a result, the information available within the office was voluminous and extremely sensitive.[82]

Initiation and Espionage

Short of funds and unhappy in the Navy, Madsen schemed to sell classified information about narcotics trafficking to drug smugglers. He initiated the plan by asking an acquaintance, Richard Grant Noble, for

[79] Howard, "Fixed Sonar Systems."
[80] Richard Halloran, "A Silent Battle Surfaces," *New York Times Magazine*, 7 December 1986; and "The Cold War: History of the SOund SUrveillance System (SOSUS)," Discovery of Sound in the Sea, accessed 23 March 2021.
[81] "National Intelligence Warning," Director of Central Intelligence Directive no. 1/5 (Langley, VA: Central Intelligence Agency, 23 May 1979); and Roger George, Intelligence in the National Security Enterprise: An Introduction (Washington, DC: Georgetown University Press, 2020), 153.
[82] Stephanie Mansfield, "Sailor Accused of Espionage Wanted to 'Buy Things'," *Washington Post*, 16 August 1979; "Sold Secrets," *Daily News* (Lebanon, PA), 16 August 1979, 60; and "Pentagon Is Unnerved by Spying Indictment," *Daily Advertiser* (Lafayette, LA), 16 August 1979, 10.

Figure 39. The Pentagon

Source: Wikimedia Commons.

U.S. Navy yeoman third class Lee E. Madsen was stationed at the Pentagon in Washington, DC.

information about prospective buyers. Instead of helping Madsen, Noble contacted the FBI.[83]

Investigation and Punishment

Recruited as a source, Noble purchased several classified documents from Madsen and later introduced an FBI undercover agent. Madsen escorted the agent into his workspace, where he stole a highly classified document and smuggled it out of the Pentagon. Madsen also suggested a continuing cash-for-documents relationship.[84]

[83] Mansfield, "Sailor Accused of Espionage Wanted to 'Buy Things' "; and "Ex-Security Guard at Pentagon Gets Eight Years for Espionage," *Miami* (*FL*) *Herald*, 27 October 1979, 18-A.
[84] Mansfield, "Sailor Accused of Espionage Wanted to 'Buy Things' "; and "Pentagon Official Arrested in Spying—Drug Documents Involved," *News and Observer* (Raleigh, NC), 15 August 1979, 2.

A few days later, the FBI arrested Madsen. He pled guilty to violating the espionage statute, was sentenced to eight years, and served four. In court, Madsen claimed that he thought Noble was a criminal or enemy agent that he hoped to catch in the act.[85]

Significance

Madsen was another financial volunteer because he sought to sell classified material to an U.S. adversary. The case against him was militarily effective because, thanks to Noble, the FBI interdicted him before any compromise resulted in an *unexpected advantage* for drug smugglers. From a strategic perspective, the significance of the Madsen case was that it was the first DON espionage investigation that involved a nonstate entity. It demonstrated that naval counterintelligence needed to remain flexible and able to adapt to a changing threat environment.

Lessons Learned

As with the Wine case a decade earlier, the Madsen case was the second time that a suspect's casual acquaintance reported potential espionage. The case also marked the first use of an undercover agent in a naval espionage investigation since the 1916 unidentified chief petty officer case more than 60 years earlier. Critically, rather than using an ONI undercover agent to simply gather information as in 1916, in 1979 the FBI undercover's role was to establish beyond a reasonable doubt that Madsen voluntarily violated the Espionage Act. This technique would evolve into a foundational element of espionage investigations. NIS does not appear to have been involved in the case.

[85] "Ex-Security Guard at Pentagon Gets Eight Years for Espionage"; Robert Meyers, "Sailor Receives 8 Years in Jail for Espionage," *Washington Post*, 27 October 1979; "Man Gets 8 Years for Espionage," *Tampa Bay* (*FL*) *Times*, 27 October 1979, 3A; and "Find an Inmate: Lee Eugene Madsen," Bureau of Prisons, accessed 24 February 2021.

Naval Counterintelligence Stumbles, 1946–80

U.S. naval counterintelligence's failure to grasp the strategic shift in Soviet intelligence's focus on the SSBN community and to detect Walker's espionage punctuated the early Cold War. The development of the Polaris SLBM in 1960 plunged the U.S. Navy onto the front lines of the Cold War, but there is little evidence to suggest that naval counterintelligence recognized how dramatically the threat environment had shifted.

The first warning of the strategic shift should have come in September 1961, when a Canadian newspaper published a first-person memoir by Harry F. Houghton, a former British Royal Navy petty officer and convicted Soviet spy. According to Houghton, his Soviet intelligence handler told him "not to concern myself with the American nuclear Polaris submarines since agents in Scotland had been working the Holy Loch."[86] The first SSBNs had arrived in Holy Loch just a few months earlier.

Despite the apparently missed warning, six years later the Ledbetter case in Holy Loch should have spurred a reassessment of the operational priorities of naval counterintelligence. Instead, the DON again missed the strategic implications of an investigative success. Months later, U.S. counterintelligence left the path to espionage almost unimpeded for Walker, a path which would profoundly impact the department for decades.

Lessons Learned

While U.S. naval counterintelligence had several militarily effective tactical successes during the early Cold War, it failed to recognize the

[86] Houghton, "I Betrayed My Country—And the Woman I Love."

massive strategic shift in the threat from Soviet intelligence. As a result, the DON neglected to focus on protecting its arm of the nuclear triad from espionage, which resulted in what was likely the most damaging espionage case in U.S. naval history. This lack of focus on naval warfighting shifts that affected the counterintelligence threat was not a new phenomenon. In the 1930s, the introduction of the aircraft carrier was an earlier target, compromised by Farnsworth to the Japanese. Fortunately for the DON, Japanese naval intelligence handled Farnsworth poorly and his case was only partially militarily effective. In 1940, the movement of the U.S. Pacific Fleet from California to Hawaii should also have triggered a strategic shift in naval counterintelligence. The failure to do so allowed Yoshikawa to operate unhindered and contributed to the disaster at Pearl Harbor in December 1941. Through the early Cold War, the DON continued to miss the counterintelligence implications of major shifts in its naval strategy.

Chapter 4
Late Cold War Case Briefs, 1980–1992

The last 14 years of the Cold War were a time of great change in the world of U.S. counterintelligence. Congress passed the Foreign Intelligence Surveillance Act (FISA) of 1978 and the Classified Information Procedures Act (CIPA) in 1980.[1] The two laws represented watershed moments for counterintelligence, because counterintelligence agencies could now legally gather information about foreign intelligence activities within the United States and then present that information without risk of compromise in the courtroom. Finally, in 1981, President Ronald W. Reagan signed Executive Order 12333, which defined counterintelligence and provided a basis for expanding counterintelligence activities throughout the U.S. government.[2] Now, counterintelligence agencies had the backing they needed to pursue cases with the knowledge that prosecutors could safely use evidence gathered through intelligence activity in court. The result was an enormous increase in prosecuted espionage cases that otherwise would never have gone to trial.[3]

[1] Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978); and Classified Information Procedures Act, Pub. L. No. 96-456, 94 Stat. 2025 (1980).
[2] "Executive Order 12333: United States Intelligence Activities," Ronald Reagan Presidential Library and Museum, accessed 25 November 2023.
[3] Melanie Reid, "Secrets behind Secrets: Disclosure of Classified Information before and during Trial and Why CIPA Should Be Revamped," *Seton Hall Legislative Journal* 35, no. 2 (May 2011): 272–73.

Based on the cases identified in this study, between 1980 and 1992, the United States prosecuted 25 naval espionage cases, nearly one-half of all the U.S. Department of the Navy's (DON) espionage cases between 1898 and 2010.

As discussed in the previous chapter, John A. Walker had retired from the Navy in 1976 but had recruited his friend Jerry A. Whitworth to keep the flow of cryptographic material going to the Soviet Union. That continued until 1982, though the Soviet Committee for State Security (KGB) could probably sense that the operation was ending. By 1981, Whitworth was unhappy and stressed about the espionage and wanted out. His last delivery of usable cryptographic material was in 1982. After that delivery, the Soviet ability to read U.S. military message traffic soon ended. The Soviets were again in the dark and scrambling for a replacement.

That was where the next case brief began. The Soviets saw their window into U.S. naval command and control slowly closing and were already looking for the next opportunity. The DON still did not understand how the Soviets had gained such an *unexpected advantage* and, despite raging Cold War espionage around the globe, it had been 24 years since the last Navy prosecution for Soviet espionage (Nelson C. Drummond in 1962).

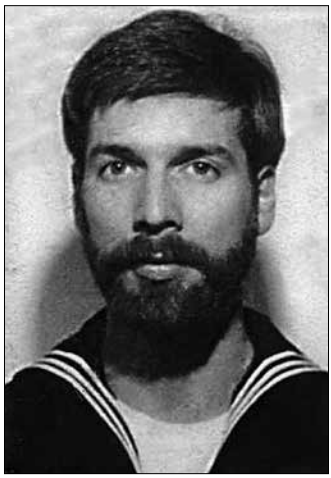
In 1980, the Soviets' sought-after opportunity appeared in Rome, Italy. Moreover, the unsatisfactory result of the eventual investigation meant that the Soviets again gained *unexpected time, place, and manner advantages* that could never be fully detailed.

1980: Glenn M. Souther

Background

In 1980, Glenn M. Souther was a married 23-year-old photographer's mate first class assigned to the U.S. Navy's Sixth Fleet Public Affairs Office aboard its flagship, the destroyer tender USS *Puget Sound* (AD 38), in Gaeta, Italy. He had access to classified information through duties

Figure 40. Glenn M. Souther



Source: Wikimedia Commons.

U.S. Navy photographer's mate first class Glenn M. Souther.

conducting handheld imagery intelligence collection. While in Gaeta, Souther began studying Communism and reading about early Soviet history and, to use current terminology, became a self-radicalized Marxist-Leninist.[4]

Initiation and Espionage

That year, Souther walked into the Soviet embassy in Rome and volunteered to commit espionage to help the Soviet Union. Ironically, he met with the same KGB agent that Walker had met with in Washington, DC, in 1967.[5] Within a year, Souther was a fully active Soviet in-

[4] "A Recruiting Virtuoso," *Nezavisimoye Voyennoye Obozreniye* [Independent Military Review], 2 June 2006. Note: this image is the same as Souther's FICEURLANT (Fleet Intelligence Center Europe and Atlantic) identification card depicted in Ronald Kessler, *The Spy in the Russian Club* (New York, Charles Scribner's Sons, 1990), 192.

[5] Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (Oxford, UK: Oxford University Press, 2015), 231; "A Recruiting Virtuoso"; and Pete Earley, "Interview with the Spy Master," *Washington Post*, 23 April 1995.

telligence asset, receiving coded messages over a short-wave radio and using a customized camera.[6]

In fall 1981, Souther made a drunken confession to his wife, an Italian civilian with no clearance whom Souther divorced and abandoned within a year. She had also seen his radio, code books, and camera and a few months later reported her suspicions to the U.S. Naval Investigative Service (NIS). The ensuing investigation did not uncover Souther's espionage, and NIS largely dismissed her allegations as an attempt at revenge.[7]

Souther returned to the United States and left active duty in 1982. He then attended Old Dominion University in Norfolk, Virginia, where he majored in Russian. He also drilled with the Navy Reserve at the Fleet Intelligence Center, Europe and Atlantic, also in Norfolk.[8] During drill periods, he stole and photographed unknown numbers of classified intelligence and operational documents, which he exchanged for cash at dead drops in the Washington, DC, area and in Rome.[9]

Investigation

In 1985, revelations about the Walker case made one witness in the original 1981 NIS investigation into Souther have second thoughts. Souther's ex-brother-in-law, a U.S. Navy officer, had dismissed Souther's ex-wife's allegations during the earlier NIS investigation. After the Federal Bureau of Investigation (FBI) arrested Walker based on a tip from his ex-wife, the brother-in-law recontacted NIS to retract his earlier dismal. With Souther no longer on active duty but in the reserves, NIS mistakenly passed the new allegation to the FBI. In May 1986, the

[6] Kessler, *The Spy in the Russian Club*, 19, 36.
[7] Kessler, *The Spy in the Russian Club*, 36–41, 49–51.
[8] Kessler, *The Spy in the Russian Club*, 113–19.
[9] Kessler, *The Spy in the Russian Club*, 62–66, 81–83, 88–89.

FBI conducted a routine interview of Souther with what appeared to be little preparation or follow-up.[10]

Nineteen days later, with the help of his Soviet handlers in Italy, Souther escaped to the Soviet Union.[11] He quickly discovered that the Communist paradise he had envisioned was instead a Stalinist nightmare, and in 1989 he committed suicide by running his car in the closed garage of the home provided to him by the KGB.[12]

Significance

Souther was only the second of what proved to be a rare type among the naval espionage cases considered in this study: the ideological volunteer. His initial motivation was his infatuation with Communism and a sincere desire to assist an adversary of the United States. However, as with other ideological volunteers in the study, he became dependent on the money given to him by his handlers. Despite the infrequent occurrence of ideological volunteers, the Souther case is significant primarily because it was militarily and legally a complete failure. He escaped to the Soviet Union, leaving the DON without any ability to account for the material he had sold to the Soviets. Critically, this left the department uncertain of what *unexpected advantages* his compromises had given the Soviets. Moreover, the Souther case demonstrates the DON's challenge with intercepting an espionage volunteer who contacts an adversary diplomatic establishment outside the United States. In this case, the department was wholly dependent on the local counterintelligence service.

---

[10] Kessler, *The Spy in the Russian Club*, 138–39, 151–52.
[11] Kessler, *The Spy in the Russian Club*, 157–59, 165–66.
[12] Kessler, *The Spy in the Russian Club*, 237–38; and Frank Rafalko, ed., *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century* (Washington, DC: National Counterintelligence Center, 1998), 281.

Lessons Learned

The Souther case was a failure primarily because NIS and the FBI failed to follow through aggressively on both the original allegation in 1981 and the second allegation four years later. Additionally, this was the third time in 45 years that a friend or family member reported naval espionage that proved accurate.

Off the Rails: A Counterintelligence Curveball

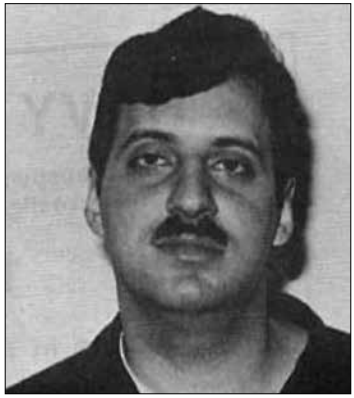
The next Cold War case brief is unusual because it involved a potentially brilliant young officer who essentially ran amok over romance and volunteered to commit espionage for South Africa. The case brief is important because it illustrates how the financial volunteers considered in this study chose their espionage partners based on whatever was in the news.

In late summer 1981, South Africa was big news in the United States. By the late 1970s, South Africa had become an international pariah due to its policy of strict racial segregation, known as Apartheid. South Africa had been banned from the Olympics in 1964 and was increasingly shunned by the international community over its treatment of its non-White population.[13]

In 1981, the South African national rugby team conducted its annual world tour, which included three games in the United States. The games became a lightning rod for controversy, attracting activists and extremists from both ends of the U.S. political spectrum. The South African team first toured in New Zealand, where the venues degener-

[13] D. N. Dhanagare, "Apartheid: Its Theory and Practice in South Africa," *India Quarterly* 23, no. 4 (October–December 1967): 338–61; Rob Nixon, "Apartheid on the Run: The South African Sports Boycott," *Transition* no. 58 (1992): 68–88, https://doi.org/10.2307/2934968; and Chuck Miller, "Rugby in the National Spotlight: The 1981 USA Tour of the Springboks," Chuck Miller Creative Writing Service, 10 April 1995.

Figure 41. Stephen A. Baba



Source: *Espionage* (Washington, DC: Naval Investigative Service, 1989), 6.

U.S. Navy Reserve ensign Stephen A. Baba, 1981.

ated into violent, bloody protests. The controversy over the rugby tour was headline news throughout the summer of 1981, and the South African team was due to play in the United States in late September.[14]

At the same time that Souther made his drunken confession to his wife and Walker continued selling cryptographic secrets, another espionage case began to unfold.

1981: Stephen A. Baba

Background

In September 1981, Stephen A. Baba was a 21-year-old ensign assigned to the frigate USS *Lang* (FF 1060) in San Diego, California. Baba was exceptionally intelligent, having graduated from high school at 16 and college at 18 before being commissioned in the Navy at age 20. While in the Philippines on liberty, he became infatuated with a 26-year-old

[14] Miller, "Rugby in the National Spotlight."

Filipino hostess at the Cubi Point Officer's Club who was now draining him of money.[15]

Initiation and Espionage

Once he had burned through his funds, Baba borrowed money to send to the woman. He then pursued criminal means to improve his accounts. He first attempted to extort money from the on-base Navy Federal Credit Union by faking a bomb threat and then stole classified microfiche from his ship and mailed it to the South African embassy in Washington, DC. While Baba's reason for choosing South Africa remains a mystery, it may have been because of the rugby tour press coverage that summer and because South Africa could have appeared less "treasonous" than the Soviet Union.

Baba, already in unauthorized absence status for missing his ship's departure, was desperate. With neither extortion nor espionage producing any funds, he attempted to rob a jewelry store in Coronado, California, and was finally detained.[16]

Investigation and Punishment

After Baba mailed the microfiche and an offer to commit espionage to the South African embassy, the embassy returned it to the Navy, which informed NIS. Based on the recontact instructions in the letter and other evidence, NIS quickly made the connection between Baba and the espionage offer.[17]

Baba was sentenced to eight years and received a bad-conduct discharge, but the sentence was suspended after two years per a plea

[15] " 'Brilliant' Naval Officer Faces Spying Charges," *Arizona Daily Star*, 22 December 1981, A7; "Ensign Receives 8-year Sentence," *St. Joseph* (*MO*) *Gazette*, 21 January 1982, 6A; and Nancy Ray, "Ensign Pleads Guilty to Disclosing Secrets; Navy Officer Asks Forgiveness in Case Tied to a Love Affair in the Philippines," *Los Angeles Times*, 20 January 1982, CC/Part II, 1.
[16] " 'Brilliant' Naval Officer Faces Spying Charges"; "Ensign Receives 8-year Sentence"; Ray, "Ensign Pleads Guilty"; and *Espionage* (Washington, DC: Naval Investigative Service, 1989), 6.
[17] *Espionage*.

agreement. Baba pled guilty to three espionage counts and numerous other charges, including attempted escape, uttering a bad check, offering violence against a superior officer, and unauthorized absence.[18]

Significance

Baba was yet another strategically insignificant, militarily effective financial volunteer. As with many other sailors before and after, problems in his personal life had left him indebted, desperate, and with nowhere to turn. However, the Baba case was a military success primarily because the South Africans saw more benefit to reporting his espionage attempt than accepting it. That was the significance of the Baba case, in that it was the first in the DON of a subcategory that can be termed *allied espionage*, or that the subject chose to commit espionage on behalf of a nation that was an ally or partner of the United States rather than an adversary. The gamble that every would-be spy took when they sought to volunteer to commit espionage for an ally or partner nation was whether their information would tip that partner nation's strategic risk versus gain equation. That equation was straightforward when volunteering to adversaries but very different when dealing with partners. Each of the espionage volunteers in this study placed their fate in the hands of the country they approached, but with an ally or partner country, the question of how that country would interpret the situation was much less certain. Some accepted the approach, but others reacted in the same way that the South Africans did and reported it to the authorities.

[18] According to Virginia code of law, Title 18.2. Crimes and Offenses Generally, Chapter 6. Crimes Involving Fraud, Article 4. Bad Check Law, § 18.2-181, *uttering a bad check* refers to knowingly passing or presenting a check that has insufficient funds (i.e., an attempt to defraud someone). It is a criminal offense in most jurisdictions and can be considered a form of theft or fraud depending on the circumstances and the amount of the check. "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996," Department of Justice, Office of the Pardon Attorney, Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

Lessons Learned

The Baba case demonstrated how the media can influence financial volunteers' decision-making processes. Those volunteers often resorted to whatever perceived adversary was a trending topic. Some were obvious; others were not. Additionally, unlike the fumbled reaction to the allegations made by Souther's wife, in the Baba case, a few months and a world apart, NIS's immediate aggressive investigation resulted in a positive outcome for the DON.

Fine-Tuning the Counterintelligence Interdiction Model

The next Cold War case brief occurred one year later at the Fleet Intelligence Center, Europe and Atlantic, at the same time that Souther began drilling there as a reservist.

This case brief marked the beginning of long, sad string of financial volunteers who, fortunately, were mostly unsuccessful. The reason for this sudden string of financial volunteers was somewhat unclear but may have its roots in the U.S. military buildup that began in 1979, increased anti-Soviet rhetoric, the change in military personnel demographics that followed the initiation of the all-volunteer force in 1973, increased drug use in the military, and a shift in counterintelligence focus from background investigations and physical security to a more active scrutiny of the threat. Those events combined to thrust the Soviet threat into the headlines, which in turn attracted financially strapped military personnel as volunteers while simultaneously ensuring that U.S. counterintelligence was much more likely to detect their attempts to contact Soviet officials.

However, there may have been another factor at play: the Navy family and the pressures on them. While Navy Family Service Centers were first instituted in 1966, they were not a success, and Admiral Elmo R. Zuwalt Jr., the chief of naval operations who initiated the

focus on the family in 1970, once remarked that in the Navy, "people were treated like a worthless piece of flotsam."[19] By 1978, Congress had lifted a previous cap on military pay, and the DON found that the main reasons for low reenlistment rates related to family issues.[20] In response, the first reenergized Navy Family Service Center opened in Norfolk in July 1979. This was a concept that evolved from the Family Awareness Conference held in November 1978 at Naval Station Norfolk. The Navy leadership in Norfolk were aware that the demographics of the all-volunteer Navy required a new approach. The result was a center staffed with active-duty personnel and volunteers who provided 24-hour information and referral services, follow-up, financial counseling, child welfare liaison, relocation information, special assistance, and family enrichment.[21]

While the DON aimed these services at retention, they also served to prevent many of the same family and financial crises that drove sailors such as Drummond and Walker to espionage.

That was the situation when the next case brief began. The United States was rallying behind its new president, Ronald W. Reagan, who seemed determined to destroy the Soviet Union, as the Navy scrambled to build up its forces while still coming to grips with a Soviet submarine threat that had caught up too quickly. Fresh off the Baba case, NIS seemed ready for a similar challenge.

---

[19] Ann O'Keefe, *Launching the Navy Family Support Program: A Heartfelt Blend of History and Memoir* (n.p.: Amazon Kindle Direct Publishing, 2019), 19, 64.

[20] "40 Years of Meeting Your Needs . . . at Home and at Sea," Fleet and Family Support Center, 31 May 2019; and Gerald M. Croan et al., *Roadmap for Navy Family Research* (Washington, DC: Office of Naval Research, Department of the Navy, 1980), 3, 14–15.

[21] "40 Years of Meeting Your Needs . . . at Home and at Sea"; and O'Keefe, *Launching the Navy Family Support Program*, 32.

Figure 42. Brian P. Horton

Source: *Espionage* (Washington, DC: Naval Investigative Service, 1989), 11.

U.S. Navy intelligence specialist second class Brian P. Horton, 1982.

1982: Brian P. Horton

Background

In April 1982, Brian P. Horton was a married 28-year-old intelligence specialist second class working in the Nuclear Strike Planning Branch of the Fleet Intelligence Center, Europe and Atlantic.[22]

Initiation and Espionage

In August 1982, Horton contacted the Soviet embassy in Washington, DC, to sell classified intelligence material to Soviet military intelligence.[23]

[22] *Espionage*, 11.

[23] *Department of Defense Appropriations for 1986: Hearing before a Subcommittee of the Committee on Appropriations, House of Representatives, Ninety-Ninth Congress, First Session*, pt. 4 (Washington, DC: Government Printing Office, 1985), 679; and *A Counterintelligence Reader*, 267.

Investigation and Punishment

What Horton did not realize was that the FBI was already aware of his approach.[24] Due to a critical mistake in the amateur espionage tradecraft that Horton employed, the FBI quickly identified him.[25]

Horton claimed that his contact with the Soviets was a misguided attempt to gather material for an espionage novel. However, the investigation indicated that his attempted espionage was genuine and motivated by a lack of funds. The evidence was mixed. Horton had spoken of bankruptcy in April 1982 when the contacts began but had also just received a large reenlistment bonus.[26] However, Horton admitted to efforts to commit espionage during interviews and a polygraph.[27]

In January 1983, he pled guilty to unauthorized contact with the Soviets and was found guilty of soliciting a Soviet to commit espionage. In exchange for a post-trial grant of immunity if he admitted any further espionage, Horton was sentenced to six years and received a bad-conduct discharge.[28]

Significance

If the prosecution's view of Horton's actions was accurate, he was another financial volunteer; otherwise, he was simply a naïve would-be author. However, his actions still amounted to espionage. Despite its quick resolution, Horton's case was extremely significant, a watershed in naval counterintelligence, because it was the first espionage case in which the subject was given post-trial immunity for full disclosure of

[24] David Wise, "The FBI's Fake Russian Agent Reveals His Secrets," *Smithsonian Magazine*, November 2016.
[25] *Counterintelligence and National Security Information: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-Ninth Congress, First Session, June 17, 1985* (Washington, DC: Government Printing Office, 1985), 80; and *Espionage*, 11.
[26] Philip Smith, "Sailor Sentenced after Bid to Sell Plans to Soviets," *Washington Post*, 14 January 1983.
[27] *Counterintelligence and National Security Information*, 80.
[28] *Counterintelligence and National Security Information*, 30, 80; and *Espionage*, 11.

the damage done. Moreover, Horton was the first truly militarily effective espionage prosecution in the DON's history because the case provided an accounting of the potential *time, place, and manner advantages* gained by an adversary that was verified by a polygraph examination.

The Horton case set a precedent that the DON would begin to practice routinely: to offer a reduced sentence and immunity from prosecution for further admissions of espionage while passing a polygraph and pleading guilty. At the time, NIS referred to this technique as the "Horton Clause."[29]

Lessons Learned

The Horton case was the first naval espionage case in the United States in which the subject's contact with a foreign embassy led to his capture. Critically, unlike the Lee E. Madsen investigation, the FBI and NIS did not incorporate an undercover approach for this particular investigation. Later, the undercover approach would become a standard response to volunteer cases, generating at least seven more investigative leads that led to espionage prosecutions between 1983 and 2010. Due to the amateur tradecraft employed by these volunteers, the initial communication with an adversary always posed the most risk for the espionage suspect and the most opportunity for counterintelligence investigators.

First Deserter-Spy

This next Cold War case brief occurred at the same time as the Horton case. The pace of attempted espionage within the DON in the early 1980s now exceeded the previous historical peak pace in the 1930s, just before World War II. Armed with FISA information, protected by

[29] *Counterintelligence and National Security Information*, 81; and *Espionage*, 11.

CIPA, and using the Horton Clause, the DON could finally militarily and effectively resolve espionage allegations. Relying on the Horton Clause, which calls for reducing someone's penalty for revealing more crimes, seems counterintuitive. However, the Horton plea bargain gave the DON leverage to extract a full confession and determine the full extent of the adversary's new *advantage*: Security: never permit the enemy to acquire an unexpected advantage.

Extending that principle of war to espionage suggests that the most elementary job of naval counterintelligence is to ensure that an adversary advantage obtained through espionage is *NOT unexpected*. The advantage must be known in advance so that the Navy can take steps to offset it. As demonstrated by the Walker case, and as the Germans found with Hans Schmidt, undetected naval espionage can give the adversary a tremendous *unexpected* advantage. Due to Schmidt, the Germans lost the Battle of the Atlantic, and due to Walker, the United States' ballistic missile submarine (SSBN) deterrent may have been at risk as the result of an espionage-related *unexpected* adversary advantage. Therefore, the purpose behind the immunity offers started during the Horton case were an attempt to ensure that the Navy was aware of all of the information compromised in an espionage case to ensure that adversaries did not have an *unexpected* advantage.

The challenge for naval counterintelligence was to remember that the law was a tool used to neutralize espionage for the benefit of Navy and Marine Corps leaders. The penalty may have a deterrent effect, but militarily its purpose was to gain leverage to extract the truth from espionage suspects. The threat of years in prison was what forced spies to fully disclose the extent of the compromise so that the Navy and Marine Corps could properly adjust. That was the end goal of all militarily effective espionage investigation: full disclosure of the compromise. The law and the penalty were just tools used to obtain it. Using the same investigative tools but employing the Horton Clause in prosecution, from 1982 to 2010, case after case within the DON mentioned

a reduced sentence and a plea agreement.[30] This was done to prevent the *unexpected advantage*.

That was where the next case brief began. The DON still did not know about Walker's espionage, but NIS realized that espionage cases were beginning to occur at a rate never previously seen within the department. The financial volunteer, seeking to relieve personal debt, had to glance at the headlines in the United States to believe that the Soviet Union would be their way out of whatever financial hole they had dug.

This next case details a young Marine attempting to desert from a distant post. The unique thing about this case was the surprising lack of Soviet interest. This was a petty espionage case that investigators needed to run down to expose any *unexpected advantage* that the Soviets might have gained, all while Walker's espionage was winding down and Souther's espionage was heating up.

1982: Brian E. Slavens

Background

In August 1982, Brian Slavens was an 18-year-old Marine private first class assigned to Marine Corps Security Force, Adak, Alaska, where he helped guard the weapons compound. He went on leave late in the month.[31]

Initiation and Espionage

While Slavens was on leave, he decided to desert his post.[32] Broke, he traveled to Washington, DC, and walked into the Soviet embassy to sell his knowledge of the facilities at Adak. Instead of paying him for information, the Soviets advised him to reconsider his actions. He

[30] *Counterintelligence and National Security Information*, 81.
[31] *A Counterintelligence Reader*, 281.
[32] "Price of Betrayal Small for Navy Spies, Say Data," *Record* (Hackensack, NJ), 3 December 1986, C-11.

Figure 43. Marine Barracks, Adak

Source: Courtesy of Barry Erdman.

U.S. Marine Corps private first class Brian E. Slavens deserted from Marine Barracks, Adak, AK, in 1982.

contacted his sister and told her about his plans to desert and his visit to the Soviet embassy. She told their father.[33]

Investigation and Punishment

Slavens's father, learning that his son intended to desert, contacted NIS. Slavens was arrested in September and in November pled guilty to several U.S. Uniform Code of Military Justice (UCMJ) violations. He was sentenced to two years but released after 18 months.[34]

Significance

Slavens was a deserter spy and financial volunteer whose case held no strategic value but was militarily effective. However, for the U.S. counterintelligence community, the Slavens case was a failure.

[33] *A Counterintelligence Reader*, 281.

[34] Ben Franklin, "Lonetree Will Fault Sentence by Citing Earlier Spy Cases," *Advocate-Messenger* (Danville, KY), 30 August 1987, 5; and *A Counterintelligence Reader*, 281.

Lessons Learned

Worryingly, there is no evidence that the FBI detected Slavens when he departed the Soviet embassy in Washington, DC. This may have been a strategically important gap in the counterintelligence net around the Soviet embassy. Surveillance of a fixed location is vital but in this case was the last layer of defense. Security awareness within units, such as the Navy officer who reported John S. Farnsworth in 1935, and friendly espionage operations that penetrate adversary intelligence, such as the FBI's recruitment of Soviet intelligence officer Dmitiri Polyakov in 1961, were both vital to detecting espionage because the last layer of defense around foreign establishments was not infallible. Like Walker before him, Slavens was also able to walk into the Soviet embassy and escape FBI detection, demonstrating the requirement for a multi-layered counterintelligence net.

A Second Deserter-Spy

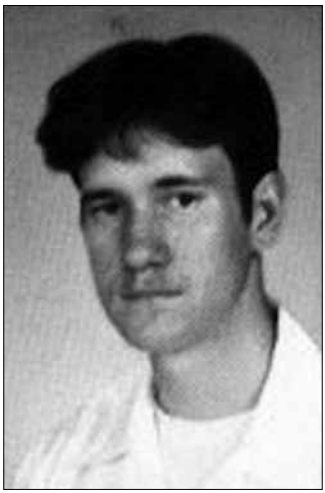
Like the Slavens case, this next case brief involved unauthorized absence, overseas travel, and a need for cash. However, in a new twist, this case involved hoarding classified information overseas. As this case unfolded, the number of petty espionage cases in the DON continued to accelerate as Walker's espionage wound down and Souther's espionage heated up.

1983: Hans P. Wold

Background

In summer 1983, Hans P. Wold was a 21-year-old intelligence specialist third class aboard the aircraft carrier USS *Ranger* (CV 61). Wold, a narcotics user, took local leave in San Diego, California, in June. Just as his leave was about to expire, he requested a leave extension from

Figure 44. Hans P. Wold



Source: *WESTPAC '82: 25 Years for Freedom* (USS *Ranger* (CV 61), 1982), 127.
U.S. Navy intelligence specialist third class Hans P. Wold, 1982.

Subic Bay in the Philippines, where he had traveled without authorization. The command granted the extension, but Wold failed to return.[35]

Since Wold had a top secret clearance, *Ranger* requested that NIS locate him in the Philippines.[36] NIS quickly found Wold at his Filipino fiancée's home in Olongapo City, just outside the Subic Bay Naval Base, where *Ranger* had been homeported the previous year.[37]

Investigation and Punishment

When NIS apprehended Wold, they found a roll of undeveloped film but thought nothing of it. When debriefed by the local Navy staff intelligence officer, Wold admitted that the roll of film contained

[35] *Espionage*, 23; *WESTPAC '82, USS Ranger (CV 61): 25 Years for Freedom* (Washington, DC: Department of the Navy, 1982), 127; and *Counterintelligence and National Security Information*, 82.
[36] *Counterintelligence and National Security Information*, 82.
[37] *WESTPAC '82*, 177.

photographs of pages of a highly classified document about satellite reconnaissance systems. NIS opened an investigation and Wold admitted that he had taken the photographs just before his leave with the intention of selling them to the Soviets to fund his trip to the Philippines. The roll of film contained images of the publication, but they were out of focus and useless.[38]

In October 1983, Wold pled guilty to violating 18 U.S. Code § 793 (gathering, transmitting, or losing defense information) as well as charges related to unauthorized absence, missing movement, drug use, and false swearing. Wold was sentenced to four years and received a bad-conduct discharge.[39] As with Horton 10 months earlier, Wold was granted immunity and offered less than two years if he passed a polygraph, which he did.[40]

Significance

Wold was another example of a financial volunteer case that was militarily effective because the DON was able to determine exactly what happened from his polygraph confession. Intercepted before he contacted any adversary, Wold's case was strategically insignificant but, importantly, his was the second case in which NIS used a polygraph examination to ensure that his confession was truthful.

Lessons Learned

The Wold case was another in a long line of cases in which a sailor turned to espionage to fund a romance. Starting with the disgraced former Commander Farnsworth, through Petty Officers Drummond and Garry L. Ledbetter, to Ensign Baba, poor romantic choices turned several servicemembers into would-be spies. Moreover, Wold was the

[38] *Espionage*, 23.
[39] Gathering, Transmitting or Losing Defense Information, 18 U.S. Code § 793; and *Espionage*, 23.
[40] *Counterintelligence and National Security Information*, 82.

DON's first example of hoarder espionage, in which a person steals classified information and stores it for later sale.

A Third Deserter-Spy

By summer 1983, NIS had simultaneously pursued three financial volunteer espionage investigations during the previous year. This theme repeats periodically in the history of U.S. naval counterintelligence. Unauthorized absence espionage cases resulted in less damage because the person's memory limits the quantity of information, as seen in the Slavens, Wold, Wine cases, or even further back in the classified memories of former servicemembers such as George A. Downing, Farnsworth and Frederick J. Rutland.

The second deserter-spy case in the summer of 1983, and the fourth financial volunteer espionage case in a year, coincided with the Wold case, both taking place in the Philippines.

1983: Alan D. Coberly

Background

In June 1983, Alan D. Coberly was a Marine private first class assigned to 3d Battalion, 1st Marine Regiment.[41] His battalion had deployed to Subic Bay in the Philippines in May 1983, while the battalion's India Company was further deployed to Diego Garcia. Circa 15 May, the battalion retrograded to Okinawa, and by June 1983 the entire battalion was in Okinawa—without Coberly, who had deserted and remained behind in the Philippines.[42]

[41] *Department of Defense Appropriations for 1986*, 681.

[42] *Marine Corps Command Center Operational Summary 18-83* (Washington, DC: Command Center and Operations Branch, Headquarters Marine Corps, 2 May 1983); and *Marine Corps Command Center Operational Summary 27-83* (Washington, DC: Command Center and Operations Branch, Headquarters Marine Corps, 6 July 1983).

Figure 45. Marines in the Philippines

Source: National Archives and Records Administration, College Park, MD.

U.S. Marine Corps private first class Alan D. Coberly was deployed to the Philippines with 3d Battalion, 1st Marine Regiment, in May 1983.

Initiation and Espionage

While Coberly pondered how he was going leave the Philippines to return to the United States, he visited the Soviet embassy. However, he did not have a security clearance and possessed no information of value.[43]

Investigation and Punishment

Coberly eventually found a way to travel from the Philippines to Seattle, Washington, where U.S. Customs arrested him. Customs searched Coberly's belongings and discovered the addresses of Soviet diplomatic establishments in Manila, Philippines. An extensive investigation confirmed much of what Coberly then admitted to NIS and Customs.[44]

[43] *Department of Defense Appropriations for 1986*, 681.
[44] *Department of Defense Appropriations for 1986*, 681.

In September 1983, Coberly pled guilty to several UCMJ violations including desertion and "other criminal acts," was sentenced to 18 months, and received a bad-conduct discharge.[45]

Significance

Coberly was another deserter spy, a financial volunteer, and a militarily effective case with no strategic value. With little information of value and little prospect of ever getting access to sensitive information, there was seemingly no interest in Coberly from the Soviets. However, this case points to the same problem observed with Drummond in London in 1957 and Souther in Rome in 1980: the ability or desire of the security services in countries hosting U.S. naval personnel to observe and report approaches by U.S. naval personnel to adversary diplomatic establishments. In Coberly's case, the Philippines either missed or failed to inform the United States of his approach to the Soviet embassy.

Lessons Learned

Coberly was the first deserter-spy intercepted by U.S. Customs at his return to the United States.

Mental Instability and Espionage

The next Cold War case brief begins to unfold at the same time as the Slavens, Wold, and Coberly cases in the summer of 1983. Beyond what appears to be the subject's mental instability, this case again illustrates that even without a clearance, some financial volunteers will take advantage of security lapses to steal classified to sell it.

This case brief mixes several elements, beginning with a simple thief who took advantage of a security lapse. It then evolved into a

[45] *Department of Defense Appropriations for 1986*, 681. Note: the exact nature of Coberly's "other criminal acts" were not released to the public.

classified information hoarder and eventually into an attempt at espionage. Note how naval counterintelligence caught the subject, as standard techniques utterly failed to identify him.

Strategically, in the summer of 1983, with Walker retired and his accomplice Whitworth refusing to cooperate, the Navy's command and control was finally secure after 15 years of compromise. However, both Walker and Souther were still providing a steady stream of highly classified documents to the Soviets.

Also of note, this case and the Baba case both involved microfiche. For readers unfamiliar with this system, in the 1970s and 1980s, before the digital files used today were practicable, the world had turned to microfiche to store information. This system used photographs of document pages that were reduced so that a dozen or more pages could fit on one index card-size sheet. Users could read and photocopy documents as needed using a special viewer/copier machine. The system reduced storage requirements and increased portability.

The U.S. Navy rapidly adopted microfiche to ease space issues aboard ships, but the increased portability of the media had the same counterintelligence implications as digital media when the DON introduced it into the workplace and aboard ships. It appears that officials did not consider the increased security vulnerability of microfiche prior to its introduction into the fleet. The lesson learned is that while every advance in moving information resulted in a new counterintelligence challenge, it seems that decision makers often overlooked those implications until after the first compromises occurred.

1983: Jeffery L. Pickering

Background

In 1982, Jeffery L. Pickering was a 33-year-old hospital corpsman aboard the frigate USS *Fanning* (FF 1076). A former Marine in the early 1970s, Pickering was described as a thief, a thrill seeker, and a perpetual liar. Pickering left the Marine Corps in 1973 and enlisted

Figure 46. USS *Fanning* (FF 1076)

Source: National Archives and Records Administration, College Park, MD.

U.S. Navy hospital corpsman Jeffery L. Pickering was serving aboard USS *Fanning* (FF 1076) when he stole 147 classified microfiche sheets.

in the Navy in 1979 under a false name to hide the facts of his prior service in the Corps.[46]

Initiation and Espionage

In summer 1982, Pickering stole several sheets of classified microfiche that had been left unsecured aboard *Fanning* and took them home. That winter, he transferred to the naval hospital in Seattle.[47] In May 1983, Pickering printed one of the microfiche documents and mailed

[46] *A Counterintelligence Reader*, 278.

[47] *A Counterintelligence Reader*, 278; and "A Navy Hospital Corpsman Who Said He Stole 'Out of Curiosity'. . . ," United Press International, 4 October 1983.

it, along with a letter with recontact instructions, to the Soviet embassy in Washington, DC. The Soviets never responded.

Investigation and Punishment

A few weeks after his attempted espionage, Pickering walked into work and spontaneously confessed to having stolen the classified microfiche. He later admitted to NIS and FBI agents to having tried to contact the Soviets. Pickering pled guilty to a variety of UCMJ violations, was sentenced to five years, and received a bad-conduct discharge. He served two years and was released in 1985.[48] A repeat offender, prior to enlisting in the Navy he had been convicted of larceny and theft, and after he was released from military confinement he pled guilty to sexually abusing a boy.[49]

After his release, Pickering returned to Oregon. In 1998, he was sentenced to 13 years in prison for threatening President William J. "Bill" Clinton after he placed two pipe bombs in a culvert near the airport where the president was due to arrive.[50] In 2001, he was again sentenced to an additional two years for fraud after he claimed veteran's disability benefits to which he was not entitled.[51] He was released in May 2012 after serving almost his entire sentence and was again arrested in 2013.[52]

Significance

Pickering was another financial volunteer whose case was militarily effective because the DON was able obtain a full accounting of his espionage during his plea agreement. Strategically, this case was insignificant but had huge significance for naval counterintelligence. At least

[48] *A Counterintelligence Reader*, 278.
[49] "Man Charged in Clinton Bomb Threat," *Albany* (*OR*) *Democrat-Herald*, 16 October 1998, A4.
[50] "Man Sentenced for Clinton Threat," Associated Press, 7 June 2000.
[51] "Phony Vet, Would-be Assassin Given Increased Prison Term," *Army Times*, 11 May 2001.
[52] "Jeffery Loring Pickering," ArrestFacts, 25 April 2013.

three layers of the DON's security bureaucracy failed to intervene with an individual who appears to have been profoundly unfit for service. First, he was able to enlist under a false name. Second, the theft of the microfiche sheets aboard *Fanning* did not implicate him. Finally, the presumed counterintelligence net around the Soviet embassy failed to detect his mail-in espionage offer.

If the Soviets had elected to respond, Pickering might have become another useful penetration of the DON. Fortunately for the department, his apparent mental instability intervened and he confessed.

Lessons Learned

The Pickering case, like the Farnsworth and Harry T. Thompson cases 50 years earlier, demonstrated that those without access to classified information can still commit espionage by taking advantage of security lapses. No clearance was not a reason to dismiss a potential subject. Like Wold at roughly the same time, Pickering was a second case of hoarder espionage, but unlike Wold, Pickering went through with the crime.

A Textbook Counterintelligence Interdiction

The next Cold War case brief introduces what became a tried-and-true response to attempts to evade the U.S. counterintelligence net around adversary diplomatic establishments. It also highlights the FBI's improvement of its coverage of the Soviet embassy and consulates.[53]

---

[53] Wise, "The FBI's Fake Russian Agent Reveals His Secrets"; William Overend, "FBI Also a Resident of S.F. Neighborhood: Soviet Consulate: Cow Hollow Intrigue," *Los Angeles Times*, 28 July 1985; *Department of Defense Appropriations for 1986*, 686; Jean McNair, "Revenge behind Try to Sell Secrets," *South Bend* (*IN*) *Tribune*, 11 January 1989, A6; David Montgomery, "Sucker or Spy: The Court Martial of Cpl. Charles Anzalone," *Buffalo* (*NY*) *News*, 18 January 1992; and "Navy Man Arrested on Spy Charge Offered Secrets to Russia," Associated Press, 24 April 1996.

The following case brief exemplified the concept that most financial volunteers use only the tradecraft they can conjure themselves. As with the Horton case, the most critical time in the financial volunteer espionage cases considered in this study were the brief interludes between the individuals' first overt act toward espionage and the moment that the adversary intelligence service began to apply professional tradecraft. That was when the DON's financial volunteers were most vulnerable and had caused the least amount of damage. Those were the "golden hours" when counterintelligence needed to react.[54]

As the next case brief demonstrates, the subject understood that the FBI might monitor his contact with the Soviets, and he attempted to conceal his identity. He gambled that the Soviets would react more quickly than the FBI to protect him. However, the FBI reacted at lightning speed.

1983: Robert W. Ellis

Background

In 1983, Robert W. Ellis was a married 23-year-old aviation antisubmarine warfare operator second class assigned to Patrol Squadron 46 at Naval Air Station (NAS) Moffett Field just outside San Francisco, California. Ellis was an aircrewman aboard a Lockheed P-3 Orion antisubmarine patrol aircraft with access to classified information. He was also deeply in debt.[55]

---

[54] E. Brooke Lerner and Ronald M. Moscati, "The Golden Hour: Scientific Fact or Medical 'Urban Legend'?," *Academic Emergency Medicine* 8, no. 7 (2001), 758–60, https://doi.org/10.1111/j.1553-2712.2001.tb00201.x. Note: the *Golden Hour* is a term widely used in emergency medicine to describe the concept that "trauma patients have better outcomes if they are provided definitive care within 60 minutes of the occurrence of their injuries." The term is adapted here to describe the quick reaction required of counterintelligence investigators to an attempt by a subject to contact a foreign intelligence officer.

[55] *Initial Assessment Study of Naval Air Station, Moffett Field, Sunnyvale, California* (Port Hueneme, CA: Naval Energy and Environmental Support Activity, 1984), 4-1; *Department of Defense Appropriations for 1986*, 686; and Edward Mickolus, *The Counterintelligence Chronology: Spying by and against the United States from the 1700s through 2014* (Jefferson, NC: McFarland, 2015), 91.

Figure 47. Lockheed P-3 Orion

Source: National Archives and Records Administration, College Park, MD.

U.S. Navy aviation antisubmarine warfare operator second class Robert W. Ellis served with Patrol Squadron 46, the "Grey Knights," which flew the Lockheed P-3 Orion maritime patrol aircraft.

Initiation and Espionage

That year, Ellis contacted the Soviet consulate in San Francisco to offer to sell classified information and provided recontact instructions. However, instead of being recontacted by a Soviet intelligence officer, an FBI undercover agent met Ellis.[56]

Investigation and Punishment

Ellis met the undercover agent as planned and exchanged photocopied classified documents and handwritten notes for $2,000. The FBI ar-

[56] Overend, "FBI Also a Resident of S.F. Neighborhood"; *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008* (Monterey, CA: Defense Personnel Security Research Center, 2009), 13; and *Department of Defense Appropriations for 1986*, 686.

rested him on the spot.[57] Ellis pled guilty to UCMJ violations. Sentenced to five years, his sentence was reduced in accordance with a pretrial agreement.[58]

Significance

Ellis was another financial volunteer who, thanks to a militarily effective investigation, was strategically insignificant. The FBI intercepted him before he could sell information that would have given the Soviet Navy an *unexpected advantage*.

Lessons Learned

The Ellis case showed that the DON was wholly reliant on the FBI for a quick reaction to volunteer espionage cases within the United States. Overseas, the DON was wholly reliant on host nations. This was why a naval counterintelligence imperative was to remain solidly connected with the FBI domestically and host nation security agencies in overseas base locations.

Another Successful Interdiction

At the investigative level, the next case brief demonstrates what could happen if, unlike the Horton and Ellis cases, there was a delay in the U.S. counterintelligence response to a financial volunteer.

In the Walker case, U.S. counterintelligence missed his walk-in at the Soviet embassy, and because the Soviets realized the gravity of the information he offered, they immediately applied tradecraft to protect him. The same chain of events occurred in the Souther case in Italy.

In the Ellis case, the Soviets never had a chance to apply tradecraft. In the words of retired FBI agent Dimitry Droujinsky about undercov-

[57] Mickolus, *The Counterintelligence Chronology*, 91.
[58] Mickolus, *The Counterintelligence Chronology*, 91.

er reactive operations, "The first thing I did was to try to keep [financial volunteers] away from the Soviets. I always said, 'Don't contact the Soviets again, the Soviet Embassy. I'm the guy who handles these cases for them'."[59]

Operationally, for naval counterintelligence, this was the seventh attempted petty espionage case in two years, a rate previously unseen in the DON's history. Unbeknownst to NIS, Walker's stooge, Whitworth, had retired from the Navy and was writing anonymous letters to the FBI, while Walker's brother and son supplied Walker with classified documents to sell to the Soviets. In a few months, Walker's wife would call the FBI. Souther continued to drill in the Navy Reserve, enjoying the run of classified spaces at the Fleet Intelligence Center in Norfolk one weekend per month to select documents to sell to Soviet intelligence.

So, while Soviet intelligence had lost access to U.S. Navy command and control, they accomplished their objective, as the Soviet Navy believed that it had sufficiently narrowed the subsurface warfare gap enough to protect the Soviet Union from U.S. SSBNs. The Soviets also continued to enjoy a steady flow of classified documents from within the U.S. Navy. They had little need to react to the six risky propositions posed by the Navy and Marine financial volunteers who had approached them during the past two years.

This was where the next case brief began, as a seventh risky proposition made by a Marine financial volunteer.

1984: Robert E. Cordrey

Background

In April 1984, Robert E. Cordrey was a 23-year-old Marine private with two years' service assigned as an instructor at the Fleet Marine Force, Atlantic's Nuclear, Biological and Chemical Defense School at Camp

[59] Wise, "The FBI's Fake Russian Agent Reveals His Secrets."

Figure 48. Camp Lejeune

Source: National Archives and Records Administration, College Park, MD.

U.S. Marine Corps private Robert E. Cordrey was stationed at Camp Lejeune, NC, when he attempted to commit espionage in 1985.

Lejeune, North Carolina.[60] Previously arrested for sexual offenses and going through a divorce, Cordrey made the desperate choice to commit espionage.[61]

Initiation and Espionage

Cordrey made numerous contacts with the Soviet, Czechoslovakian, Polish, East German, and West German embassies in Washington, DC, to sell documents and manuals relating to his job.[62] After many futile attempts, Cordrey contacted a Czechoslovakian intelligence officer and drove from Camp Lejeune to Washington for a clandestine

[60] "Marine Gets 12 Years at Spy Court-Martial," *New York Times*, 10 January 1985; and Jerry Hager, "State Marine Guilty of Trying to Sell Info," *Morning News* (Wilmington, DE), 9 January 1985, A1.
[61] *Counterintelligence and National Security Information*, 84; and "Family Court, Sussex County [Delaware]: Divorce Decrees," *Morning News* (Wilmington, DE), 19 April 1985, B8.
[62] *Department of Defense Appropriations for 1986*, 693; and *Counterintelligence and National Security Information*, 84.

meeting. Cordrey showed his contact a list of documents in his possession, all of which were unclassified. The intelligence officer told Cordrey that someone would contact him later.[63]

Investigation and Punishment

Instead of using the rapid Ellis case undercover technique, the FBI and NIS response in this case was apparently slow, allowing Cordrey enough time to meet with an intelligence officer.[64] However, the investigators made up for lost time and arrested Cordrey. In exchange for a sentence reduced from 12 years to 2 and a bad-conduct discharge, Cordrey pled guilty to failing to report contacts with a citizen of a Communist-controlled country. He successfully underwent post-trial interrogation and a polygraph, as outlined by the Horton clause.[65]

Significance

Cordrey was a strategically insignificant and militarily effective financial volunteer case.

Lessons Learned

The Cordrey case demonstrated the willingness of financial volunteers to advertise their espionage to multiple foreign countries, which often marked a measure of their desperation. The case also demonstrated the requirement for swift reaction to unfolding espionage allegations.

Prosecuting Leaks

As with the Madsen case and drug smugglers in 1979, the next case brings up a new nonstate espionage "adversary"—the press. The subject of the case claimed that he was a leaker devoted to exposing the

---

[63] *Espionage*, 7.
[64] Hager, "State Marine Guilty of Trying to Sell Info."
[65] *Espionage*, 7.

threat to the United States posed by the Soviet Navy. Prosecutors claimed that he was attempting to launch a career as a journalist.

This case was the first in which a government official was prosecuted for leaking classified information to the press. Since then, at least 16 such cases were prosecuted, raising questions about freedom of the press and the press's larger role as the "Fourth Estate" (the fourth branch of government) in a democratic society.[66] One of these later cases involved U.S. Navy nuclear electrician's mate second class Stephen Kellogg III, who in 2019 stole classified information about the Navy's nuclear-powered warships and planned to give it to a journalist and then defect to Russia. Kellogg said that he wanted to publish an exposé on waste within the military and admitted that he wanted to share the information with Russians.[67]

For investigators, the issue was simple: Did the leaker violate the nondisclosure agreement that they had signed? More important, however, was to determine the full extent of the disclosures to ensure that the Navy was aware of all the information compromised in an espionage case to ensure that an adversary did not have an *unexpected advantage*. In this next case, the precedent set with the Horton case two years before was not applied. There was no offer of a reduced sentence and immunity from prosecution for further admissions of espionage while passing a polygraph, so the full extent of his disclosures was never clear.

For prosecutors and juries, the situation becomes more complicated, as they need to determine the purpose of the leak. Were all other avenues to resolve a problem exhausted? Was the leak an altruistic effort to expose a problem hidden within the U.S. government, or was it

[66] Stephen J. Adler and Bruce D. Brown, "Let's Be Practical: A Narrow Post-Publication Leak Law Would Better Protect the Press," in *National Security, Leaks and Freedom of the Press: The Pentagon Papers Fifty Years On*, ed. Lee Bollinger and Geoffrey Stone (New York: Oxford University Press, 2021), 132–37.

[67] "Navy Sailor Sentenced for Attempted Communication of Classified National Defense Information," Federal Bureau of Investigation, 23 May 2019.

Figure 49. Samuel L. Morison

Source: *Espionage* (Washington, DC: Naval Investigative Service, 1989), 14.
Samuel L. Morison, 1985.

a cynical attempt to sell information or curry favor? In this case, that was the crux of years of appeals made all the way to the U.S. Supreme Court.

1984: Samuel L. Morison

Background

Samuel L. Morison was a 40-year-old civilian intelligence specialist at the Naval Intelligence Support Center who was also a published naval historian and a contributing editor with *Jane's Defence Weekly*.[68] The grandson of Rear Admiral Samuel E. Morison, who wrote the seminal history of the U.S. Navy in World War II, Morison was a former Navy officer who had served aboard the destroyer escort USS *Savage* (DE 386) in Vietnam and with the Navy History Division in Wash-

[68] "The Dark Side of Moonlighting," in *Security Awareness in the 1980s* (Richmond, VA: Department of Defense Security Institute, 1989), 81–92.

ington, DC, before leaving active duty and beginning work with naval intelligence.[69]

Initiation and Espionage

In 1984, after a British *Jane's* editor dangled full-time employment before him, Morison increasingly pushed the limits of classification in his articles to secure that employment. In July, he stole three classified satellite photographs from a colleague's desk and mailed them to *Jane's*. The colleague did not report the images missing, thinking another analyst had locked them up elsewhere in the secure office space.[70]

Investigation and Punishment

In August, the stolen photographs appeared in *The Washington Post* and *Jane's Defence Weekly*. Morison's colleagues immediately recognized the photographs and implicated Morison. Despite Morison's denial that he had seen or handled the images, NIS found one of Morison's fingerprints on the back of one of the original photographs returned by *Jane's*. In October, Morison admitted to stealing the photographs, cutting off the classification markings, and mailing them to *Jane's*.[71]

In December 1985, Morison was convicted of violating the espionage statute and sentenced to two years.[72] He remained free on appeal until entering prison in 1988, served eight months, and was later pardoned by President Clinton in 2001.[73] Inexplicably, the Navy rehired Morison in 2010 to write a history of the Navy during the Global War on Terrorism. Given access to the Navy historical archives, Morison was again arrested by the Naval Criminal Investigative Service (NCIS)

[69] Gave Rottman, "Government Leaks to the Press Are Crucial to Our Democracy. So Why Are We Suddenly Punishing Them So Harshly?," *Time*, 1 November 2018.
[70] "The Dark Side of Moonlighting," 81.
[71] "The Dark Side of Moonlighting," 81.
[72] "The Dark Side of Moonlighting," 81.
[73] "Pardon: Samuel Loring Morison—Collection Finding Aid," Clinton Digital Library, accessed 23 January 2024.

in 2014 for stealing a trove of his grandfather's archival material and attempting to sell some of it online. He pled guilty and served two years' probation.[74]

Significance

Morison was a strategically insignificant and militarily ineffective financial volunteer case. While the DON was able recover the classified photographs, the U.S. intelligence community probably lost some of its *unexpected advantage* after the Soviets were able to examine the detail that was available in U.S. satellite imagery. However, the reprinting of the photographs in *Jane's* rendered the images largely useless. Because Morison did not plead guilty and was not subjected to a polygraph, the DON was not able to determine what else, if anything, he had compromised to *Jane's* or other publishers. It was never clear what other *unexpected advantage* the Soviets might have gained through Morison's duplicity.

Lessons Learned

A basic investigative technique such as identifying fingerprints was key to convincing Morison to confess. Despite the sophisticated intelligence collection methods that were available to the DON at the time, the investigators remembered to use basic techniques because the espionage was, at its core, simple theft.

A Second Crypto Case

As with the many financial volunteers who came before, this next late Cold War case brief was a tragically stupid story of a thief trusted with classified information. Again, this financial volunteer used whatever

[74] Ian Duncan, "Navy Veteran Accused of Stealing from Files of Famed Historian Grandfather," *Baltimore* (*MD*) *Sun*, 10 June 2014; and Jessica Gresko, "Man Once Convicted of Spying Pleads Guilty to Naval Archive Document Theft," *Navy Times*, 12 March 2015.

concocted tradecraft he could to ensure his security. Fortunately, in this case, the subject was reckless and easily caught. What made this case unique was the number of coconspirators involved in the escapade.

Strategically, as the Walker and Souther cases continue to wind down, Cold War tensions remained high. To offset the as-yet inexplicable Soviet Navy gains in submarine warfare, the U.S. Navy began building the advanced *Los Angeles*-class attack submarines in the 1970s and replacing the compromised Sound Surveillance System (SOSUS) with T-AGOS ocean surveillance ships in the 1980s. Both systems remain in operation today.[75]

A few months earlier, during two speeches in March 1983, President Reagan publicly labeled the Soviet Union an "evil empire" and revealed the Strategic Defense Initiative (SDI), the development of a massive space-based antiballistic missile system.[76] SDI was a deception, as the technology was not feasible at the time. U.S. intelligence had determined that the Soviet economy was crumbling, and U.S. leaders believed that SDI and other increases in U.S. military spending would force the Soviets to keep pace and eventually bankrupt the Soviet Union.[77]

Against this dramatic clash of empires, a bumbling U.S. Navy radioman thought he could easily cash in.

---

[75] Edward C. Whitman, "SOSUS: The 'Secret Weapon' of Undersea Surveillance," *Undersea Warfare* 7, no. 2 (Winter 2005): 18.

[76] "Presidential Address: National Association of Evangelicals, Orlando, Florida, Tuesday, March 8, 1983," Ronald Reagan Presidential Library and Museum, accessed 25 November 2023; and "Address on Defense, March 23, 1983," Ronald Reagan Presidential Library and Museum, accessed 25 November 2023.

[77] *Report to Congress on the Strategic Defense System Architecture* (Washington, DC: Strategic Defense Initiative Organization, 1987); "Strategic Defense Initiative (SDI)," Atomic Heritage Foundation, 18 July 2018; and Tim Weiner, "Lies and Rigged 'Star Wars' Test Fooled the Kremlin, and Congress," *New York Times*, 18 August 1993, 1.

Figure 50. Michael T. Tobias

Source: Frank Rafalko, ed., *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century* (Washington, DC: National Counterintelligence Center, 1998), 282.

U.S. Navy radioman third class Michael T. Tobias, 1984.

1984: Michael T. Tobias

Background

In July 1984, Michael T. Tobias was a 20-year-old radioman third class aboard the tank landing ship USS *Peoria* (LST 1183) in San Diego. One Sunday afternoon, Tobias was part of a two-person detail assigned to document and destroy 12 crypto cards, the same type of cards that Walker and Whitworth had sold to the Soviets for 15 years. When the other radioman on duty falsified the destruction log with the approval of their supervisor to depart the ship before his watch was completed, Tobias stole the cards.[78]

Initiation and Espionage

Two weeks later, Tobias and his nephew, an 18-year-old Navy civilian employee named Francis X. Pizzo Jr., drove to the Soviet consulate in San Francisco to attempt to contact Soviet intelligence to sell the cryp-

[78] "United States, Plaintiff-Appellee v. Michael Tobias," U.S. Court of Appeals, Ninth Circuit, 6 January 1988; "Navy Man Guilty of Code Thefts," *San Bernardino County* (*CA*) *Sun*, 15 August 1985, A-9; and *A Counterintelligence Reader*, 282.

Figure 51. Francis X. Pizzo Jr.

Source: Frank Rafalko, ed., *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century* (Washington, DC: National Counterintelligence Center, 1998), 282.

Francis X. Pizzo Jr., 1984.

to cards for $100,000.[79] Being a Sunday, the consulate was closed, so they returned to San Diego. There, Tobias, Pizzo, and Tobias's brother, 19-year-old civilian Bruce Tobias, attempted to return the crypto cards to the U.S. government in exchange for a reward from the U.S. Secret Service of $1,000.

Investigation and Punishment

The FBI identified the callback number as a telephone booth, where they detained but inadvertently released Tobias and Pizzo, who then fled.[80] Realizing their involvement, the FBI eventually tracked down and arrested the pair in San Francisco. From jail, Tobias convinced a fourth conspirator, 24-year-old civilian Dale Irene, to help conceal the stolen cards.[81]

[79] Ronald J. Olive, *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice* (Annapolis, MD: Naval Institute Press, 2006), 122; "2 More Are Accused of Theft of Navy Codes," *New York Times*, 25 August 1984, 1; and "Espionage Raps Pend in Decoder Case," *Petaluma* (*CA*) *Argus-Courier*, 24 August 1984, 2A.

[80] "United States, Plaintiff-Appellee v. Michael Tobias"; and "Chula Vistans Arrested in Navy Code Card Stealing," *Imperial Beach* (*CA*) *Star-News*, 30 August 1984, B-3.

[81] "Suspect Pleads Guilty in Theft of Code Cards," *Sacramento* (*CA*) *Bee*, 8 August 1985, B10; and *Espionage*, 18.

Despite a plea bargain for a successful polygraph, none of the group could account for 2 of the 12 stolen crypto cards. The civilians pled guilty to a variety of charges regarding conspiracy and stolen property. Bruce Tobias received time served, Irene received two years, and Pizzo received 10 years. Tobias stood trial in federal court, was convicted of violating the espionage statute, and received 20 years.[82] He served 12 years and was released in 1996.[83] Pizzo served his full sentence and was released in 1995.[84]

Significance

Tobias was a potentially strategically significant but militarily effective financial volunteer case. While Tobias never sold the crypto cards, the case should have alarmed the DON because it had the potential to cause disaster. If Tobias had succeeded in contacting the Soviets, the case could have bloomed into a second Walker case, continuing the compromise of U.S. naval command and control and the longstanding *unexpected advantage* that the Soviet Navy had enjoyed for many years. The Tobias case should have triggered the DON to focus its counterintelligence efforts on the radiomen handling cryptographic material, but there was no record that the case garnered any more attention than the rest of the string of petty espionage cases that preceded it. The Walker case would not break for 10 more months, in May 1985.

Lessons Learned

Tobias was the first "partner espionage" within the DON. No previous sailor or Marine suspect had successfully colluded with another person to attempt to commit espionage. Both the Wine and Madsen cases featured a coconspirator, but they immediately approached the FBI. The Tobias multiple-suspect espionage case would not be the last of its

[82] "United States, Plaintiff-Appellee v. Michael Tobias."
[83] "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."
[84] "Find an Inmate: Francis X. Pizzo," Bureau of Prisons, accessed 14 April 2021.

kind. Additionally, the case pointed out that personnel can opportunistically neutralize security procedures such as two-person integrity through complacency and corner-cutting.

Espionage at the Circle K: Another Hoarder Case

The next late Cold War case brief featured a classified hoarder like Wold and Pickering. Those cases would not likely have resulted in enduring espionage because foreign intelligence services have little interest in someone who does not have ongoing access to classified information.

This case brief also typified the attitude of financial volunteers toward the classified information entrusted to them. They viewed it simply as a commodity, but in some cases the financial volunteer discriminated among potential customers and sought to sell the information to a lesser but still potentially lucrative threat, as in the case of Baba with South Africa and Madsen with drug smugglers.

Finally, this case brief demonstrated that the speed of reaction to a financial volunteer was critical to the success of the investigation. Like the Ellis case the year before in California, this case was quickly over.

By the time the subject of this case was sentenced, Walker's arrest was only four months away, and Souther's escape was a year away. Despite the dramatic uptick in cases, the DON still believed that it had the espionage situation under control. In two years, eight Navy and Marine financial volunteers had planned or attempted espionage. Only one, Pickering, had provided classified information to the Soviets. None had been recontacted.

In June 1985, a month after Walker's arrest, the NIS assistant director for counterintelligence testified before a congressional subcommittee stating, "Despite the recent events predicating this hearing [the Walker case], the improved posture of the Navy Foreign Counterintelligence Program, vis-à-vis 20 years ago, we are in a better posi-

tion today to identify and neutralize attempts to access our classified information." NIS written testimony before the same congressional subcommittee noted, "With the provision of resource allocations beginning in FY-82, NIS has been allowed to effect total dedication of NIS Special Agents [to counterintelligence] on a selective, progressive basis. The successes of the past few years in counterespionage investigations and operations are directly attributable to that dedication."[85]

The surge in cases had several causes, but the opinion of one Navy public affairs officer related to a 1986 case brief stands out: "I think every enlisted man in the service has financial difficulties of some kind. Maybe all the recent publicity about spies and the big money they sold information for caused a young man to see some easy money out there."[86]

That was where this next case brief began, as a former sailor facing financial difficulties looked for easy money.

1984: Jay C. Wolff

Background

In 1982, Jay C. Wolff was a storekeeper, helmsman, and planesman aboard the ballistic missile submarine USS *Sam Rayburn* (SSBN 635) who had been given a general discharge for drug violations.[87] While awaiting discharge, officials inexplicably assigned Wolff to a copy room aboard the submarine base in Kings Bay, Georgia, where he was responsible for making copies of classified publications about the nu-

[85] *Counterintelligence and National Security Information*, 63–106.
[86] "Navy Concerned about Theft Motivation," *Journal Herald* (Dayton, OH), 12 March 1986, 28NS.
[87] Bart Ripp, "Secrets on Sale in Albuquerque?," *Albuquerque* (*NM*) *Tribune*, 8 February 1985, 1.

Figure 52. USS *Sam Rayburn* (SSBN 635)

Source: Naval History and Heritage Command, Washington, DC.

Former U.S. Navy storekeeper, seaman, helmsman, and planesman Jay C. Wolff served aboard USS *Sam Rayburn* (SSBN 635) in 1981–82.

clear weapons carried aboard U.S. submarines. Wolff also made extra copies, which he stole and took with him after discharge.[88]

Initiation and Espionage

Wolff returned home to New Mexico, and by 1984 he was self-employed in a car detailing business. He struggled financially and was facing burglary charges. To solve these financial problems, Wolff turned to

[88] "N.M. Man Guilty of Selling Secrets," *Albuquerque* (*NM*) *Journal*, 18 May 1985, 14; Rosanne Pagano, "Man Sentenced for Selling Classified Papers," *Albuquerque* (*NM*) *Journal*, 29 June 1985, 21; and Theodore R. Sarbin, Ralph M. Carney, and Carson Eoyang, eds., *Citizen Espionage: Studies in Trust and Betrayal* (Westport, CT: Praeger, 1994), 54.

his cache of classified documents. He did not attempt to contact the Soviets, but nonetheless his attempts to find a buyer were swiftly reported to the FBI.[89]

Investigation and Punishment

The FBI office in Albuquerque, New Mexico, immediately launched an undercover operation and contacted a Navy officer at the Naval Weapons Evaluation Facility (NWEF) at nearby Kirtland Air Force Base to review the stolen documents' classification. The NWEF dealt with all aspects of the Navy's nuclear weapons arsenal. The FBI arranged an undercover meeting for the next day with Wolff in the parking lot of an Albuquerque Circle K convenience store. Wolff understood that he was selling the documents to a businessman from New York who enjoyed wargames.[90]

After Wolff handed over the documents, the Navy officer reviewed them and confirmed them as genuine and classified. The FBI then arrested Wolff.[91] Wolff pled guilty to violating the espionage statute and served three years of a five-year sentence.[92]

Significance

Wolff was another strategically insignificant and militarily effective financial volunteer case because he never succeeded in compromising information to an adversary and the DON received a full accounting of his activities. However, in 1982, Wolff's unsuitability for continued service should have also made him unsuitable for handling classified information. That was a major gap in the DON's security that facilitat-

[89] Rick Nathanson, "Gallup Man Charged with Selling Classified Papers," *Albuquerque* (*NM*) *Journal*, 18 December 1984, B2.
[90] Nathanson, "Gallup Man Charged with Selling Classified Papers"; "N.M. Man Guilty of Selling Secrets"; and Pagano, "Man Sentenced for Selling Classified Papers."
[91] Pagano, "Man Sentenced for Selling Classified Papers."
[92] "Find an Inmate: Jay Wolff," Bureau of Prisons, accessed 17 February 2021.

ed his attempted espionage and could have provided an adversary with an *unexpected advantage*.

Lessons Learned

As in the Ellis case, the FBI's immediate undercover response was effective. The speed of reaction in both undercover espionage response cases was critical. Additionally, Wolff's theft and hoarding of classified information, like that of Wold and Pickering before him, should have alerted someone to the potential for espionage.

First Allied Espionage

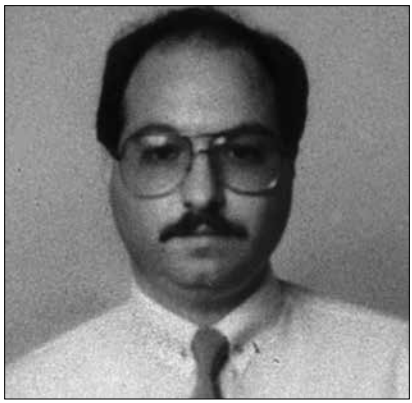
The next case brief described here involves an allied nation's espionage. It had only a tertiary involvement with the ongoing Cold War between the United States and the Soviet Union.

As explained previously, the key to allied espionage was the ally's risk versus gain calculations. In the Baba case, the South Africans did not accept his espionage offer and instead reported his approach to the U.S. Navy. In this next case, the foreign nation believed that the espionage was worth the risk of damaging relations with the United States and accepted the offer.

These types of cases were difficult to detect because usually the subject had a legitimate reason to be interacting with the allied foreign intelligence service. The problems arose when the subject began to overidentify with the foreign nation and the situation slid into an ideological volunteer or a recruitment-in-place scenario. In this case, the slide was particularly hard to detect because the subject's ethnicity and/or culture were already aligned with the entity with which they were legitimately interacting. This study identifies at least three of these cases, of which this particular case was the chronological first.

In this case, the U.S. intelligence relationship with the foreign nation was politically and culturally sensitive. Moreover, the subject was

Figure 53. Jonathan J. Pollard



Source: Federal Bureau of Investigation.

Jonathan J. Pollard, 1985.

wildly unsuited for a position of trust, but rather than confront the problem, DON leaders appear to have simply shifted him from one job to another.

1984: Jonathan J. Pollard

Background

In 1984, Jonathan J. Pollard was a married 31-year-old U.S. government general schedule (GS) 12 civilian intelligence analyst with NIS. The Office of Naval Intelligence (ONI) detailed Pollard to NIS, when the DON formed the Anti-Terrorist Alert Center (ATAC) in 1984.[93] Pollard had emotional and behavioral difficulties and fantasized about

[93] *The Naval Criminal Investigative Service: To Protect and Serve* (Washington, DC: Department of the Navy, 1994), 19; "Timeline," Naval Criminal Investigative Service Association, accessed 10 December 2024; and "DCI Terrorism Analyst Network," Central Intelligence Agency, accessed 10 December 2024.

being a spy and emigrating to Israel. He was also having financial difficulties and allegedly engaged in drug use.[94]

Pollard was involved in several U.S.-Israeli intelligence exchanges during his tenure with ONI and developed a strong perception of inadequate U.S. intelligence support for Israel, which he decided to correct himself. Rather than simply call, write, or walk into the Israeli embassy in Washington, DC, Pollard used a pro-Israel activist family friend as a go-between. The friend put him in touch with Israeli Air Force colonel Aviem Sella, who was attending New York University to complete a PhD.[95]

Initiation and Espionage

Sella and Pollard first met in the spring of 1984, just before Pollard began work at NIS. Sella's handler was Yosef Yagur, who worked for an Israeli military science and technology intelligence collection agency called the *Lishka le-Kishrei Mada* (LAKAM, or the Science Liaison Bureau), from within the Israeli embassy in Washington, DC.[96] LAKAM's interest in Pollard centered on Israel's need for information about the capabilities and amounts of military equipment that the Soviet Union had transferred to Israel's adversaries.[97]

Pollard quickly proved that he was genuine by providing dozens of classified documents to Sella. Within a few months, Pollard was re-

[94] *The Jonathan Jay Pollard Espionage Case: A Damage Assessment* (Langley, VA: Central Intelligence Agency, 1987); Olive, *Capturing Jonathan Pollard*, 2, 20–21, 45, 182–83; and " 'It's the Last Card We Have: Israel Renews Calls for U.S. to Free 'Gravely Ill' Jonathan Pollard, Jailed 27 Years Ago for Passing Secrets to Ally," *Daily Mail*, 12 April 2012.
[95] "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 47–48.
[96] Dan Raviv and Yossi Melman, *Every Spy a Prince: The Complete History of Israel's Intelligence Community* (Boston, MA: Houghton Mifflin, 1989), 70; and "Notes on April 1976 South African Visit to Israeli Scientific and Technical Intelligence Organization (LAKAM)," Wilson Center Digital Archive, June 1976.
[97] "Letter from Attorney General Janet Reno to President Clinton," Records of the Office of the Counsel to the President (Clinton Administration), Series: Mary Smith's Files, File Unit: Pollard, Jonathan, NAID: 40435991, William J. Clinton Library, Little Rock, AR; "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 65.

ceiving $1,500 per month ($3,600 today). He scoured the U.S. intelligence community for publications of interest to LAKAM, which he then acquired through an intelligence library system. His library requests, all hard copy at the time, poured into NIS, where Pollard took them home using his courier card up to three times per week. Every other Friday, Pollard took the accumulated material to an apartment in the Van Ness Condominiums in Northwest Washington.[98] Pollard was bringing so much material that the Israelis purchased a second apartment in the same building just to house the copiers. Pollard also asked for, and received, a raise to $2,500 per month ($6,000 today). Meeting his Israeli handlers in Paris and Tel Aviv as well as in Washington for the next 11 months, Pollard delivered hundreds of documents to the apartment.[99]

Investigation and Punishment

By October 1985, Pollard was working as head of the America's desk in the ATAC. On 25 October, an ATAC employee reported that Pollard left work with his wife carrying what appeared to be a package of highly classified material. A supervisor ran checks on Pollard's computer usage and could not discern unusual patterns but noticed that Pollard soon made two more end-of-day courier runs. The supervisor looked for the packages in his work space but found nothing. He then reported his suspicions and NIS opened a case. Cameras installed above his desk soon recorded him packaging more materials to remove from the ATAC at the end of the day.[100]

A few days later, as Pollard got into his car to leave with another package of classified documents, FBI and NIS agents confronted

[98] "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 68–69, 71–72.
[99] "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 63–65, 72, 84–85,
[100] "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 112–17.

him. After hours of questioning and a search of his apartment, Pollard admitted only to mishandling classified material and was released. That evening, Yagur instructed Pollard to delay while they arranged to smuggle him out of the United States. Sella left the United States the next day and Yagur the day after that.[101]

The next day, delaying as instructed, Pollard confessed but claimed that he was giving classified information to a private individual; he did not mention Israel. With Pollard's handlers gone, on 21 November 1985, Pollard and his wife (who knew everything) attempted to seek political asylum in the Israeli embassy. The embassy officials did not allow them inside, and the FBI arrested Pollard. He later made a complete confession in exchange for reduced sentencing.[102]

In 1986, Pollard pled guilty to violating the espionage statute and was sentenced to 30 years. He served his full sentence, was released in 2015, and now lives in Israel.[103]

Significance

Pollard was a strategically insignificant, partially militarily effective ideological volunteer case. While the United States lost control of vast amounts of intelligence information, none of it had a direct effect the nation's prosecution of the ongoing Cold War with the Soviet Union. The case was only partially militarily effective because it was unclear if the extensive interviews of Pollard revealed the full extent of his espionage.

At the DON level, Pollard's case was significant because it identified gaps in security. The fact that Pollard had any security clearance at all was a major flaw in the system, and his ability to use the intelligence

[101] "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 134–35.
[102] "The Jonathan Jay Pollard Espionage Case"; and Olive, *Capturing Jonathan Pollard*, 169–75, 177–81, 203–8.
[103] Elliot Gotkine, "Jonathan Pollard, Spy Who Passed U.S. Secrets to Israel, Arrives in Jewish State to Start New Life," CNN, 30 December 2020.

library system to gather so much information that was clearly outside his need-to-know was also a major gaff.

Lessons Learned

Pollard was difficult to detect because he had legitimate contact with a friendly foreign intelligence service and corrupted liaison was difficult to detect. Despite that, his statements about Israel were so outrageous, and his actions so brazen, that he should have been investigated much earlier. Fortunately, a coworker finally reported him. This was only the second espionage case reported by a coworker; Morison was first.

The Long Haul: The Navy's First People's Republic of China Case

The next late Cold War case brief introduced a new adversary, the People's Republic of China (PRC). Like the Soviet Union before 1960, when the United States introduced the SSBN, the PRC considered the United States in general to be an adversary but never appeared to have a specific interest in the U.S. Navy. That was not the whole story.

The first armed conflict between the United States and the PRC occurred in 1950, when the PRC intervened in the Korean War. During the Vietnam War, the U.S. Navy kept at least one aircraft carrier off the coast of North Vietnam in an area of the South China Sea known as "Yankee Station."[104] U.S. Navy aircraft flying from Yankee Station participated in bombing campaigns over North Vietnam, where, from 1965 to 1969, the PRC deployed dozens of construction and antiaircraft units to protect and rebuild bridges, railways, and roads as fast as the United States could destroy them. The result was that in both

[104] Norman Polmar and Edward J. Marolda, *Naval Air War: The Rolling Thunder Campaign* (Washington, DC: Naval Historical Center, 1994); and Edward J. Marolda, *By Sea, Air, and Land: An Illustrated History of the U.S. Navy and the War in Southeast Asia* (Washington, DC: Naval Historical Center, 1994), 86–118.

Korea and Vietnam, the U.S. Navy and Air Force were in direct combat with the PRC's People's Liberation Army (PLA).[105]

Another aspect considered in this case brief was the type and volume of information involved. This case spanned 40 years, 20 of which involved the compromise of at least 40,000 pages of sensitive yet unclassified technical information about U.S. Navy systems. As seen with the Ledbetter and Cordrey cases, protecting sensitive yet unclassified information was a challenge during the Cold War, and financial volunteers tried to sell information that would have given adversaries a *manner advantage*.

With the advent of widespread use of networked computers, that challenge grew exponentially. Readers should bear in mind that 40,000 scanned pages only equals about 3 gigabytes of data; this case took 20 years to compromise 3 gigabytes.[106] During January and February 2018 alone, the PRC hacked a Navy contractor and stole 614 gigabytes of sensitive but unclassified technical information about Navy systems.[107] This was more than 200 times more information lost in less than 1 percent of the time with no risk to a human asset, which presented an exponentially increased challenge.

This case brief was just one more that highlighted the challenge of sensitive but unclassified technical information, a challenge that had plagued the U.S. Navy since the USS *Pennsylvania* (BB 38) plans were stolen in 1913. Left to fester for more than a century, as the speed of

[105] VAdm Robert F. Dunn, USN (Ret), "Navy Air Strike North Vietnam," *Naval History* 29, no. 6 (December 2015); Chen Jian, "China's Involvement in the Vietnam War, 1964–69," *China Quarterly* no. 142 (June 1995): 356–87; and *Intelligence Memorandum: Chinese Communist Forces in North Vietnam* (Langley, VA: Central Intelligence Agency, Directorate of Intelligence, 29 September 1966).

[106] Edward M. Roche, *Snake Fish: The Chi Mak Spy Ring* (New York: Barraclough, 2008), 75; and "Electronic Case Filing Document Size Limitations," U.S. District Court, District of South Carolina, accessed 13 April 2021.

[107] Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, 8 June 2018.

Figure 54. *Zumwalt*-class guided-missile destroyer

Source: Wikimedia Commons.

The People's Republic of China tasked Chi Mak with providing information about advanced warship designs such as those eventually incorporated into the U.S. Navy's *Zumwalt*-class guided-missile destroyers.

movement of information increased, this problem increased along with it.

1985: Chi Mak

Background

In 1985, Chi Mak was a married 43-year-old engineer working for a defense contractor on multiple U.S. Navy contracts. He was also an asset of the PRC's military intelligence service. While this case brief began in 1985, prosecutors alleged that Mak's espionage story may have begun much earlier, when he moved from the PRC to the British colony of Hong Kong in 1965.[108]

[108] Roche, *Snake Fish*, 92.

In 1965, Hong Kong was a routine liberty port for U.S. Seventh Fleet units in the western Pacific despite its proximity to the PRC. In August 1964, the Central Military Commission of the Chinese Communist Party (CCP) and the PLA General Staff in Beijing set the stage for espionage when they ordered the military regions headquartered in Kunming and Guangzhou (the two military regions adjacent to Vietnam) and PLA Air Force and Navy units stationed in southern and southwestern China to "pay close attention to the movement of American forces, and be ready to cope with any possible sudden attack."[109] Guangzhou was also the closest major PRC city to Hong Kong.

In 1965, the PRC secretly went to war with the United States. PLA construction units with organic air defense entered North Vietnam and deployed mostly north of Hanoi during October–November 1965, returning to the PRC by October 1968. The PLA claimed that these troops fought against U.S. strike operations over North Vietnam, participating in more than 2,000 battles and shooting down more than 1,700 U.S. aircraft.[110]

Within a few months of the start of the U.S. strike campaign in 1965, codenamed "Rolling Thunder," U.S. aircraft carriers began a pattern of making one port visit to Hong Kong midway through, or at the end, of each deployment. During 1965–68, the U.S. Navy conducted more than 300 port visits per year to Hong Kong, and a U.S. aircraft carrier was in port in Hong Kong during 31 of 48 months. Most of these aircraft carriers, if not all, were involved in Rolling Thunder air operations.[111]

---

[109] Chen, "China's Involvement in the Vietnam War."
[110] Chen, "China's Involvement in the Vietnam War."
[111] "Carrier Deployments during the Vietnam Conflict," Naval Aviation History Office, Naval Warfare Division, Naval Historical Center, August 2003; and "Deck Log Book, USS *Ranger* (CVA 61), January 1965," Record Group 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Ranger* (CVA 61)–January 1965, NAID: 102267592, National Archives and Records Administration, College Park, MD, 5.

The net effect was that throughout the entirety of the Rolling Thunder campaign, U.S. naval aviation was engaged in combat with PLA air defense units in North Vietnam, operating from aircraft carriers in the South China Sea that then made port visits to a British colony within a few miles of the PRC border. In response, the PRC combated the United States diplomatically and lodged four formal protests with the British government about U.S. Navy port visits to Hong Kong. The British government acquiesced to PRC concerns and limited U.S. aircraft carriers to one per month. The formal protests ended with the PRC's withdrawal of PLA troops from Vietnam, suggesting that the U.S. Seventh Fleet was a major PRC concern. As the PRC's leader Mao Zedong told a visiting Syrian delegation in early 1965, "The U.S. has four fleets altogether: The Seventh Fleet is the biggest and surrounds us."[112]

In Hong Kong, one place that U.S. Navy officials advised sailors to visit was the Royal Navy's China Fleet Club, where the third floor housed the U.S. Navy Purchasing Branch (NPB). This was a shopping area where authorized Hong Kong businesses offered sailors goods without the fraud that many sailors experienced with unvetted businesses in the city.[113]

Initiation and Espionage

One of the vetted businesses at the NPB was Johnson Tailors. In 1965, Mak began working for Johnson as their representative inside the NPB. Here, Mak interacted with thousands of U.S. Navy personnel who crewed the ships and aircraft that were engaged in combat with the PLA in North Vietnam. While prosecutors suggested that Mak

[112] Chi-kwan Mark, "Vietnam War Tourists: U.S. Naval Visits to Hong Kong and British-American-Chinese Relations, 1965–1968," *Cold War History* 10, no. 1 (2010): 1–28, https://doi.org/10.1080/14682740902837001.
[113] Mark, "Vietnam War Tourists"; "Touring Exotic Hong Kong: Liberty Roundup," *All Hands* (January 1971): 18–23; and "Hong Kong," *USS Bennington: Her History and Her Crew*, accessed 21 February 2021.

committed espionage during the Vietnam War in the 1960s while at Johnson Tailors, they did not charge him in connection with that allegation.[114]

Mak left Johnson and the NPB in 1973. He then worked for a British company in Hong Kong before immigrating to the United States in 1978.[115] In the United States, he worked for the engineering firm Teledyne Inet, a maker of aircraft equipment, from 1981 to 1990, and then for the U.S. Navy contractor Power Paragon. Mak and his wife became U.S. citizens in 1985, and he received a secret clearance in 1996. Mak was reportedly sending information back to PLA intelligence the entire time. By 2004, his contact was a PRC military intelligence officer working undercover in an academic political-military research center.[116]

Investigation and Punishment

In fall 2004, the Central Intelligence Agency (CIA) recruited a source with access to the PRC's military and security establishment who identified a spy ring in Los Angeles, California, that the FBI found was led by Mak.[117] The FBI and NCIS began physical and technical surveillance, watching Mak for about 18 months. In February 2005, a routine examination of Mak's garbage, an investigative technique known as a "trash cover," paid off as agents found two torn-up notes that appeared to be intelligence tasking lists.[118]

For eight more months, investigators continued to watch Mak and his family, who served as his couriers. In October 2005, when it became clear that another installment of information was about to be

[114] Roche, *Snake Fish*, 92.
[115] Dunn, "Navy Air Strike North Vietnam"; and Roche, *Snake Fish*, 207.
[116] Yudhijit Bhattacharjee, "How the F.B.I. Cracked a Chinese Spy Ring," *New Yorker*, 12 May 2014; and "United States, Plaintiff, v. Chi Mak et al.," U.S. District Court for the Central District of California, October 2005.
[117] Bill Gertz, "Enemies," *Washington Times*, 18 September 2006.
[118] Bhattacharjee, "How the F.B.I. Cracked a Chinese Spy Ring."

couriered to the PRC, the FBI and NCIS arrested Mak and his family.[119] After his arrest, Mak partially confessed but later recanted.[120]

In 2008, Mak was found guilty of conspiracy, attempting to violate export control laws, failing to register as a foreign agent, and lying to federal investigators. He was sentenced to 24 and a half years.[121] As of 2020, he was in Lompoc Federal Prison and was due for release in 2026.[122]

Significance

Mak was a strategically significant, militarily ineffective patriotic penetration of the DON. While eclipsed by later computer hacking, for 20 years Mak provided a steady supply of sensitive but unclassified technical information that may have given the PLA Navy an *unexpected manner advantage* over the U.S. Navy. Just how much Mak's espionage assisted the PLA Navy will probably never be known, but the PRC's naval modernization effort, which began around the same time that Mak joined Power Paragon, transformed the PLA Navy into a much more modern and capable force.[123] Control of sensitive but unclassified technical information was a century-old issue that started with the *Pennsylvania* case in 1913 and still haunted the DON through at least 2018.[124]

Lessons Learned

Patriotic penetrations such as Mak generally required a long lead time for an adversary intelligence service to identify, train, and dispatch to

[119] "United States, Plaintiff, v. Chi Mak et al."
[120] Bhattacharjee, "How the F.B.I. Cracked a Chinese Spy Ring"; and "On Stand, Mak Denies Spying," *Press Telegram*, 1 May 2007.
[121] Bhattacharjee, "How the F.B.I. Cracked a Chinese Spy Ring."
[122] "Find an Inmate: Chi Mak," Bureau of Prisons, accessed 30 April 2020.
[123] Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2021).
[124] Nakashima and Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare."

the United States. In Mak's case, he spent 13 years in Hong Kong before emigrating to the United States. Regarding Mak's potential but unproven espionage while in Hong Kong, like Kuehn, Othmer and Yoshikawa during World War II, the Mak allegation suggests that passive observation of a port combined with poor operations security can have strategic impact. Placing a PLA intelligence asset among U.S. naval personnel who were on liberty in Hong Kong would have been a logical step that would have provided accurate order of battle information as well as potential warnings of intensified U.S. strike operations. Beyond an old list of ships, the prosecution appears to have shown no evidence that Mak was such an asset. Despite the lack of evidence against Mak, espionage that took advantage of operational patterns such as port visits was a threat to maritime operations throughout the span of this study. To crack the Mak case, physical and technical surveillance, as well as basic steps such as a trash cover, were key to gathering enough evidence to neutralize him. While time-consuming and labor-intensive, these basic investigative elements were often crucial to proving espionage.

Moscow Honeypot

In May 1985, the FBI finally arrested Walker. The extent of his espionage was a serious blow to the entire U.S. Navy. NIS, which had thought it was doing well in coping with the unprecedented number of petty espionage cases, had to reevaluate its entire counterintelligence program. In 1981, NIS did not have any counterintelligence dedicated special agents, but by 1985 it had dedicated nearly 200 of its 1,000 agents to investigating counterintelligence issues.[125]

Unbeknownst to NIS, another case was just beginning that would consume the NIS counterintelligence program for most of 1987,

[125] *Counterintelligence and National Security Information*, 63–106.

even though the case did not directly relate to the DON. This was an embassy-based case that targeted the U.S. Department of State and the CIA and had little to do with the core warfighting missions of the U.S. Navy and Marine Corps. The burden of counterintelligence coverage of Marines and sailors assigned to U.S. diplomatic missions had fallen between the bureaucratic cracks and essentially no agency was covering it at the time. Despite that, when this case broke, the bulk of the investigative burden fell on NIS rather than the State Department or the CIA.

Based on a false confession by one individual tangentially related to this case, NIS formed the Bobsled Task Force, which conducted hundreds of interviews and polygraphs to attempt to corroborate the confession.[126] Only the original subject was tried. In hindsight, it was a waste of resources. Later revelations suggested that the entire espionage operation was a KGB distraction to explain the sudden loss of numerous U.S. intelligence assets in the Soviet Union and shift attention away from Aldrich H. Ames, the actual deep penetration of U.S. intelligence.[127]

Between May 1985 and December 1986, the revelations of Walker's lengthy espionage, the escape of Souther, Pollard's treachery from within, and now what at first appeared to a fourth massive security breach rocked NIS. The agency applied a huge effort to ensure this case did not turn into another fiasco.

1985: Clayton J. Lonetree

Background

In 1985, Clayton J. Lonetree was a 24-year-old Marine sergeant serving in the embassy guard detachment in Moscow. Lonetree had arrived at

[126] Don Oberdorfer, "Spy Scandal Snowballed, Melted Away," *Washington Post*, 17 January 1988.
[127] "Marine to Leave Prison, but He Won't Shed Legacy," *Deseret News* (Salt Lake City, UT), 25 February 1996.

Figure 55. Clayton Lonetree

Source: *Espionage* (Washington, DC: Naval Investigative Service, 1989), 12.
U.S. Marine Corps sergeant Clayton Lonetree, ca. 1984.

the embassy in 1984 and in 1985 met Violetta Seina, a telephone operator and translator at the embassy. Seina was a "Swallow," assigned by KGB counterintelligence to target vulnerable Americans in Moscow through sexual blackmail, called honeytrap operations.[128]

Initiation and Espionage

Seina and Lonetree met several times in the fall of 1985, and by January 1986 they had become intimate. In late January, Seina took Lonetree to meet her "Uncle Sasha," a KGB counterintelligence officer. The KGB officer successfully recruited Lonetree, who began providing information about U.S. intelligence spaces and personnel in the embassy and classified documents stolen from burn bags. Lonetree accepted several thousand dollars in payment.[129]

[128] Rodney Barker, *Dancing with the Devil: Sex, Espionage, and the U.S. Marines: The Clayton Lonetree Story* (New York: Simon & Schuster, 1996), 36.
[129] William C. Rempel, " 'He Was Walter Mitty,' Lawyer Says: Accused Marine Spy Lived out Fantasy," *Los Angeles Times*, 16 April 1987.

Investigation and Punishment

In March 1986, Lonetree transferred to the U.S. embassy in Vienna, Austria, where in early December he was handed off to the KGB's foreign intelligence arm. Lonetree only met with the KGB once after that. Drinking heavily, he attempted to surrender in October and in December turned himself in to the CIA station chief.[130]

An NIS investigation confirmed much of his confession, and in August 1986 a court martial found Lonetree guilty of UCMJ espionage violations, sentencing him to 30 years and a bad-conduct discharge.[131] Lonetree was released from prison in 1996 after serving 9 years of his 30-year sentence.[132]

Significance

Lonetree was a strategically insignificant but militarily effective recruitment-in-place that had little bearing on the U.S. military because it occurred within the support element of a U.S. embassy. Moreover, it may have only been a deception operation aimed at the CIA. Finally, the Lonetree case was not relevant to most potential DON espionage cases because it occurred inside an adversary country with the highest of foreign intelligence threat environments. None of the other cases considered in this study occurred in such a location.

Lessons Learned

This type of counterintelligence investigation required close relationships with the State Department and the CIA, which were apparently largely absent at the time. Naval counterintelligence should have been nurturing those relationships in such a high-threat locale.

---

[130] Oberdorfer, "Spy Scandal Snowballed, Melted Away."
[131] Oberdorfer, "Spy Scandal Snowballed, Melted Away"; and Claire Robertson, "Lonetree Sentenced to 30 Years," *Washington Post*, 24 August 1987.
[132] "Marine to Leave Prison, but He Won't Shed Legacy."

An Espionage Business Model

This next case brief began in late 1985, following Walker's arrest and conviction. Unfortunately, the publicity of the Walker case generated a tranche of copycats who NIS spent the next five years pursuing.

One of the most aggressive NIS responses to the Walker case was the Proactive Counterespionage Program (PACE). This program targeted specific U.S. Navy commands to identify potential espionage suspects. NIS special agents in the program interacted directly with command members through counterintelligence briefings and interviews of command personnel. Behind the scenes, NIS personnel conducted criminal record inquiries, service record reviews, reviews of command disciplinary and indebtedness records, identification of potential areas of compromise, and facility security profiles.[133]

While none of the following case briefs resulted from the PACE program, it did target the most at-risk commands, raised the profile of NIS across the Navy, and systematized the NIS approach to counterintelligence.

Most significantly, the wakeup call that resulted from the Walker, Souther, and Pollard cases was effective. Based on the cases considered in this study, between 1986 and 2010, the Navy did not experience another case in which an active-duty or civilian member of the DON repeatedly compromised classified information to an adversary intelligence service.

Strategically, the Soviet intelligence services had a new challenge: a new Soviet leader dedicated to massive changes that would eventually result in the collapse of the nation.[134] The U.S. Navy was already working to recover from Walker's compromise of SOSUS with a new un-

[133] "Counterintelligence/Counterespionage in the U.S. Navy" (Newport, RI: Naval War College, 14 May 1990), 17.
[134] Ron Hill, "The Collapse of the Soviet Union," *History Ireland* 13, no. 2 (March–April 2005): 38–39.

Figure 56. Wilfredo M. Garcia

Source: Jeff Norwitz, "Operation Touchdown: The Story of the Wilfredo Garcia Espionage Case," *NCIS Gold Shield*, May 2013.

U.S. Navy master-at-arms first class Wilfredo M. Garcia, 1987.

derwater detection capability, the T-AGOS ocean surveillance ships, which, as previously described, remain in the fleet today.[135]

This case was the first in a series of bumbling Walker copycats.

1985: Wilfredo M. Garcia

Background

In 1985, Wilfredo M. Garcia was a master-at-arms first class at the Mare Island Naval Shipyard in Vallejo, California, with 15 years of service.[136]

Initiation and Espionage

In fall 1985, one of Garcia's jobs was to investigate and safeguard unsecured classified information aboard the shipyard. Instead, he began making copies or outright stealing the unsecured documents to sell. To ensure his security, Garcia planned to use a middleman to move the

[135] Whitman, "SOSUS."

[136] Jeff Norwitz, "Operation Touchdown: The Story of the Wilfredo Garcia Espionage Case," *NCIS Gold Shield*, May 2013.

documents to relatives in the Philippines to sell to the Soviets there. Garcia succeeded in stealing several classified documents relating to submarines, which he sold to the middleman, a local businessman, for $800.[137]

Investigation and Punishment

The local businessman agreed to move the documents to Garcia's relatives in Manila, in the hopes that he would recoup his investment and more. Fortunately, a few months later, the local businessman was indicted on federal bribery charges. In return for immunity, the businessman revealed Garcia's espionage scheme. During the next few months, NIS and the FBI corroborated the allegations with surveillance, fingerprints, and wiretaps. Meanwhile, the documents languished in Manila for nearly 18 months until March 1987, when NIS and the Philippine police recovered them.[138]

Garcia was arrested and eventually confessed to the scheme. In January 1988, he was convicted at a court-martial of espionage, conspiracy to commit espionage, larceny, conspiracy to commit larceny, and sale of government property. He was sentenced to 12 years and received a dishonorable discharge. There was no mention of a Horton Clause plea agreement in the public record. Garcia was paroled in February 1995 after serving seven years of his sentence.[139]

Significance

Garcia was a strategically insignificant, militarily effective financial volunteer case. The documents he stole were unsecured but never provided the Soviets with an *unexpected advantage*. Due to a close working relationship with the local FBI office, NIS was able to swiftly

[137] Norwitz, "Operation Touchdown"; and *Espionage*, 9.
[138] Norwitz, "Operation Touchdown."
[139] Norwitz, "Operation Touchdown"; *Espionage*, 9; and "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."

take advantage of the espionage lead, identify the suspect, and gather enough evidence to neutralize him.

Lessons Learned

Garcia had hoped to insulate himself from the espionage by having a witting intermediary known as a "cutout," the local businessman, move the documents. He also hoped to use his relatives in the Philippines as cutouts to make the approach to the Soviets. However, widening the conspiracy was ultimately his downfall.

Another Espionage Entrepreneur

The next case shows a new trend in the post-Walker Navy. Like Wolff and Madsen before him, this subject did not attempt to approach a foreign power, seeking instead to sell classified information to any buyer.

Wolff was simply out of ideas, but sailors such as Garcia and this next subject were exposed to news reports and counterintelligence briefings that spoke of the vast sums of money paid to Walker for classified information. These individuals did not view the Walker revelations as a warning but instead saw an opportunity.

So, in early 1986, just as the Garcia case opened in northern California, this case began in southern California, another in a series of inept Walker copycats.

1986: Robert D. Haguewood

Background

In March 1986, Robert D. Haguewood was a 24-year-old aviation ordnanceman third class at the Pacific Missile Test Center in Point Mugu, California. Haguewood, in serious financial trouble, approached Shannon Hughes, a woman he was seeing in the city of Oxnard, which

Figure 57. Naval Air Station Point Mugu

Source: National Archives and Records Administration, College Park, MD.
Like these sailors loading a target drone, U.S. Navy aviation ordnanceman third class Robert D. Haguewood was assigned to Naval Air Station Point Mugu, CA.

surrounds the base, and asked her if she could find a buyer for classified information.[140]

Investigation and Punishment

Unbeknownst to Haguewood, Hughes was an Oxnard City Police informant, and she quickly reported Haguewood's proposition. The Oxnard Police immediately contacted NIS, and together the two agencies initiated an undercover purchase using an Oxnard Police detective. The detective did not portray himself as representing any foreign country. For $360, Haguewood sold the detective half of a classified training manual and some other papers that he had stolen from his workspace.

[140] "Debt-driven Sailor Admits Selling Government Papers," *Santa Cruz* (*CA*) *Sentinel*, 20 June 1986, A-14.

He was unaware that the training manual had been declassified several years earlier.[141] NIS arrested Haguewood, who pled guilty to UCMJ violations regarding handling of documents. He was sentenced to two years and received a bad-conduct discharge.[142]

Significance

Haguewood was another strategically insignificant, militarily effective financial volunteer case.

Lessons Learned

Haguewood was the third "sale-to-a-criminal" espionage case covered here. The Haguewood case represents the ultimate example of treating classified as a commodity. This sale-to-a-criminal case was thankfully a short-lived trend in the post-Walker Navy that created a subset of the financial volunteer.

A Second Case of Allied Espionage

This next case involved a NIS intelligence source gone rogue in the Philippines. To understand this case, one needs to understand that by the late 1980s, Olongapo, the city just outside the Subic Bay Naval Base, had become notorious as the world's biggest brothel, home to thousands of prostitutes that attracted sex tourists from around the world and the naval base.[143]

---

[141] "Debt-driven Sailor Admits Selling Government Papers"; "Espionage Case Charge Reduced," *Albuquerque* (*NM*) *Journal*, 19 June 1986, C10; and Miles Corwin, "Petty Officer Arrested in Sale of Secret Documents," *Los Angeles Times*, 11 March 1986.

[142] "Navy Man Gets 2-year Sentence for Selling 'Secret' Documents," (Spokane, WA) *Spokesman-Review*, 20 June 1986; and "The Region: UCLA Bone Marrow Surgeon Honored," *Los Angeles Times*, 20 June 1986, 2.

[143] Uli Schmetzer, "U.S. Naval Base in Philippines Means Ships, Sex," *Chicago Tribune*, 7 September 1989; and Randolph Harrison, "Sex Drives the Philippine Economy outside Base," *Orlando (FL) Sentinel*, 25 July 1988.

With Subic Bay serving as the home of U.S. Seventh Fleet, Olongapo had been a rest and recreation center for servicemembers during the Vietnam War, and almost 20 years later, business was still booming. At the time, Ferdinand Marcos, a dictator backed by the United States, ruled the Philippines. A popular uprising ousted Marcos in 1986, and more a democratic government eventually forced the closure of U.S. bases in 1991.[144] U.S. Navy activities then shifted to Japan, Guam, and Singapore.[145]

Before that move, the Marcos regime had long battled a Communist insurgency, and periodically the insurgents turned their attention toward U.S. bases. In 1974, 1987, 1989, and 1990, the Communists attacked U.S. military personnel, killing seven Americans. The 1974 and 1990 attacks occurred in the Subic Bay–Olongapo area and killed three Navy officers and a Marine Corps gunnery sergeant.[146]

With a crime-ridden city just outside the gates and an active insurgency threatening to attack U.S. sailors and Marines at any time, NIS was extremely busy and needed sources that could provide warnings. At the same time, the Philippine authorities were seeking similar warning. While cooperating to a degree, both sides probed for information about the insurgents that went beyond routine liaison exchanges.

One answer for both sides lay with the many retired Navy personnel who owned businesses in Olongapo. These retired sailors, with

[144] "Philippines Announces Subic Closure," Associated Press, 27 December 1991; and David Briscoe, "Remembering Revolt that Ousted Filipino Dictator," *San Diego (CA) Union-Tribune*, 25 February 2011.

[145] Gregory P. Corning, "The Philippine Bases and U.S. Pacific Strategy," *Pacific Affairs* 63, no. 1 (Spring 1990): 6–23, https://doi.org/10.2307/2759811; "Speech by Deputy Prime Minister and Minister for Defence Teo Chee Hean at the Inauguration of PC V Detachment," Singapore Ministry of Defence, 20 November 2009; and *Navy Maintenance: Overseas Ship Repairs and Associated Costs* (Washington, DC: General Accounting Office, 1992), 17–18.

[146] *History of the Seabees* (Washington, DC: Naval Facilities Engineering Command, 1996), 42; *Significant Incidents of Political Violence against Americans: 1987* (Washington, DC: Department of State, Bureau of Diplomatic Security, 1988), 33; *Significant Incidents of Political Violence against Americans: 1989* (Washington, DC: Department of State, Bureau of Diplomatic Security, 1990), 21; and *Significant Incidents of Political Violence against Americans: 1990* (Washington, DC: Department of State, Bureau of Diplomatic Security, 1991), 19.

Figure 58. Navy Telecommunications Center, Naval Air Station Cubi Point

Source: National Archives and Records Administration, College Park, MD.

Retired U.S. Navy senior chief radioman Michael H. Allen worked as a copy clerk at the Navy Telecommunications Center at Naval Air Station Cubi Point, Philippines.

access to both the naval base and the local community, were ideal sources for both NIS and the Philippine authorities.

That was where this case brief began, with NIS facing a deadly insurgency in a town filled with crime and sailors and a source with divided loyalties who began to blur reality and his fantasy world.

1985: Michael H. Allen

Background

In 1985, Michael H. Allen was a 53-year-old retired senior chief radioman who was employed as a civilian photocopy clerk in the Navy Telecommunications Center at NAS Cubi Point in the Philippines. He had retired from the Navy in 1972 and ran a bar in Olongapo, but in

1982 he sought the civilian position. Allen continued to run the bar as well as a used car dealership and a cock-fighting ring in Olongapo.[147]

Initiation and Espionage

At some point, Philippines Constabulary officers recruited Allen, seeking U.S. information about rebel movements in the country. The Philippines Constabulary, disbanded and absorbed into a civilian police force in 1991, was the oldest of the Philippines' four armed forces.[148] In the communications center, Allen began making copies of messages and writing up intelligence reports, which he provided to his Philippine contacts. Allen even carried Philippines Constabulary credentials. The Philippine authorities did not pay Allen, but he found that with them on his side, his business operations ran more smoothly.[149]

Beyond his financial interests, Allen also sought a way to boost his self-esteem. He fantasized that he was working as a U.S. Navy counterintelligence agent and carried fake NIS credentials, which were widely available in Olongapo.[150]

Investigation and Punishment

Finally, in July 1986, one of Allen's coworkers at the communications center reported him. NIS launched an investigation, and extensive video surveillance confirmed that Allen was removing classified information, including summaries of rebel force movements and planned Philippine government actions, from the communications center.

[147] Jim Schachter, "Linked to Filipinos: Ex-Navy Man Found Guilty on 10 Spy Charges," *Los Angeles Times*, 15 August 1987; and "Caught by Candid Camera: The Case of Michael Allen," in *Security Awareness in the 1980s*, 95–97.
[148] "Philippines Constabulary," CountryData, June 1991.
[149] Mark Evje, "Trial Begins for Navy Man Charged with Espionage," United Press International, 5 August 1987; and "Caught by Candid Camera," 95–97.
[150] "Caught by Candid Camera," 95–97.

Allen even tried to recruit an NIS agent during the investigation.[151] When he was arrested in December, he confessed.[152]

Because Allen was living overseas, the U.S. Department of Justice (DOJ) would not prosecute him. Instead, the U.S. Secretary of the Navy authorized Allen's prosecution under the UCMJ as a retired Navy servicemember. In August 1987, Allen was found guilty of espionage violations and sentenced to eight years. He lost all of his retirement benefits and was paroled in 1991 after serving four years.[153]

Significance

Allen was a strategically insignificant and relatively militarily effective recruitment-in-place. While his duplicity may have compromised some force protection intelligence sources, it had no bearing on the DON's ongoing Cold War confrontation with the Soviet Navy.

Lessons Learned

Allen was the DON's second allied espionage case that resulted in compromised classified information. While the Soviet Union remained the primary adversary of the United States, naval counterintelligence was ready to take a close look at the Navy's intelligence partners. Like Israel, certain individuals within the Philippines military believed that it was worth the risk to recruit a U.S. Navy civilian employee. Additionally, this case was the third time in the DON's history that espionage reported by a coworker led to a successful interdiction. (Farnsworth was the first in 1935 and Pollard was the second in 1985.) Reports of suspicious activities proved fruitful on occasion.

---

[151] Hector Gutierrez, "Bid to Move Military Spy Case to Civilian Court Fails," *Los Angeles Times*, 7 April 1987, pt. 2, 2.
[152] Schachter, "Linked to Filipinos"; Sharon Jones, "Investigator: Suspect Saw Tape, Confessed," *Times-Advocate* (Escondido, CA), 7 August 1987, B2; and "Caught by Candid Camera," 95–97.
[153] "Caught by Candid Camera," 95–97; and "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."

Overseas Partner Espionage Case

This case brief is a good example of how close cooperation with a host nation's counterintelligence service can pay off. Of the six previous case briefs in which the initial approach occurred overseas, U.S. naval counterintelligence only interdicted one, Ledbetter. Two, Drummond and Souther, went on to become serious espionage cases. The other three were unusual, in that Coberly had no access, Lonetree was based in an embassy, and the host nation itself recruited Allen.

There were three truly serious Soviet espionage cases in the DON during the Cold War: Walker, Drummond, and Souther. While Walker was by far the worst, the other two started overseas, and there was a reason for that. As with all elements of force protection even today, the DON was heavily reliant on the host nation for counterintelligence coverage of adversary intelligence services. Understanding the capabilities and limitations of the host nation to put a counterintelligence screen around adversary intelligence services was important. Equally important was establishing a conduit to move counterintelligence investigative leads that might help identify a sailor or Marine in contact with an adversary intelligence service.

That was where the next case brief began, with a sailor encountering an adversary intelligence officer overseas who sought to offset the *manner advantage* achieved by the U.S. Navy with its newest aircraft.

1988: James R. Wilmoth and Russell P. Brown

Background

In September 1988, James R. Wilmoth was a 22-year-old Navy Reserve airman recruit and Russell P. Brown was a 21-year-old electronic war-

Figure 59. James R. Wilmoth

Source: Frank Rafalko, ed., *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century* (Washington, DC: National Counterintelligence Center, 1998), 283.

U.S. Navy Reserve airman recruit James R. Wilmoth, 1989.

Figure 60. Russell P. Brown

Source: *Magic Moments* (USS *Midway* (CV 41), 1989), 209.

U.S. Navy electronic warfare technician seaman Russell P. Brown, 1988.

fare technician seaman. Both were stationed aboard the aircraft carrier USS *Midway* (CVN 41) in Yokosuka, Japan.[154]

Initiation and Espionage

Wilmoth, a narcotics user, arrived aboard *Midway* in May and began working in the mess. Soon after, Wilmoth met "Alex" from the Soviet Trade Representative Office while on liberty in Tokyo. Japanese authorities had already identified another Soviet intelligence officer using the Trade Representative Office to target U.S. military aircraft technology.[155] By December, Alex offered Wilmoth cash for classified

[154] *Magic Moments*, 209; and "Espionage," Naval Criminal Investigative Service, 1995, video, hereafter "Espionage" video.

[155] "Soviets Expel Japanese Aide, Businessman: 2 Accused of Spying; Tokyo Orders Moscow Trade Official out," *Los Angeles Times*, 21 August 1987.

information about McDonnell Douglas F/A-18 Hornet fighter aircraft.[156]

Because Wilmoth did not have access to classified information, he approached Brown, who needed money to pay a civilian fine. Brown agreed to find classified information to sell and began rummaging through burn bags to find it.

Investigation and Punishment

With Japanese authorities closely watching the activities of the Soviet Trade Representative Office, NIS soon became aware of Wilmoth and Brown's activities. After NIS counterintelligence briefs, both Wilmoth and Brown lied and reported only innocuous contacts with Alex. Meanwhile, months of missed meetings went by. Finally, in May 1989, NIS recruited an informant who gave Wilmoth classified to sell, but Wilmoth could not locate Alex.[157]

NIS then arrested both men, who were convicted of attempted espionage and conspiracy to transfer classified information, failure to report contact with a Soviet, and distribution and possession of hashish. Wilmoth was sentenced 35 years, which was reduced to 15 years after a pretrial agreement, and received a dishonorable discharge. Brown was sentenced to 10 years.[158] Wilmoth served an undetermined sentence but was eligible for parole in 1994. Brown served five years.[159]

---

[156] "Court Convicts Nebraskan for Selling Military Secrets: Navy Airman Gets 35 Years in Prison," *Lincoln* (*NE*) *Journal Star*, 5 October 1989, 15; and "United States v. James R. Wilmoth, Airman Recruit (E-1), U.S. Naval Reserve," U.S. Navy–Marine Corps Court of Military Review, 23 December 1991.

[157] "United States v. James R. Wilmoth, Airman Recruit (E-1), U.S. Naval Reserve."

[158] Susanne Schafer, "Second Nebraska Sailor Convicted of Espionage," Associated Press, 26 October 1989.

[159] "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996"; "Find an Inmate: James Rodney Wilmoth," Bureau of Prisons, accessed 17 May 2020; and "Find an Inmate: Russell P. Brown," Bureau of Prisons, accessed 17 May 2020.

Significance

The Wilmoth and Brown case was a potentially strategically significant but very militarily effective recruitment-in-place. The neutralization of the pair occurred so early in the recruitment cycle that NIS struggled to gather enough evidence to prosecute. The apparent close cooperation with Japanese authorities was critical to ensuring that the United States maintained its *manner advantage* by ensuring that the Soviets did not learn classified details about the F/A-18.[160]

Lessons Learned

Wilmoth and Brown were the DON's second "partner espionage" case after the Tobias and Pizzo case four years earlier. This case only occurred because of good overseas liaison with the host nation, the same good liaison that occurred during Ledbetter case in Great Britain in 1967. These cases emphasized that close relationships with host nation security services in naval concentration areas were vital to sharing leads. Also, while unusual in the espionage cases considered in this study, coconspirators were involved in some cases.

Another Espionage Entrepreneur

This next case brief involves what appears to be another financial volunteer's attempt to commit espionage on behalf of narcotics smugglers.

In the decade since the 1979 Madsen case, the U.S. Navy's involvement in the War on Drugs had increased. Navy surveillance aircraft

[160] Deborah Kidwell, "OSI Cracks Espionage Ring in Japan," Office of Special Investigations, 28 May 2020; "4 Japanese Charged in Sale of U.S. Secrets to Soviets," *Toronto Star*, 20 May 1987, 3; *Japan: Controlling Technology Leakage to the USSR: An Intelligence Assessment* (Langley, VA: Central Intelligence Agency, 1983); and William Sexton, "U.S. Reportedly Anxious to Plug Technology Leaks in Japan," *Tampa Bay (FL) Times*, 29 May 1987, 15A. Note: in 1987, the U.S. Air Force Office of Special Investigations pursued a similar case in cooperation with the Tokyo Metropolitan Police Department. Both cases were part of a larger Japanese effort begun in 1983 to stem the flow of advanced technology to the Soviet Union.

were routinely employed to detect narcotics smuggling boats in the Caribbean and Pacific, and Navy surface units joined the mix of law enforcement ships and boats conducting the interdictions. Joint Task Forces Four and Five in Florida and California, respectively, coordinated the activity, particularly the collection and dissemination of narcotics trafficking related intelligence information.[161]

With millions of dollars at stake with each load of narcotics and information about Navy and law enforcement efforts to stop them flowing through U.S. Department of Defense communications centers, it was only a matter of time before another Madsen case cropped up.

This case brief describes that event, but more importantly, it describes a competent and professional NIS reaction. Several more such successes would follow.

1988: Randall S. Bush

Background

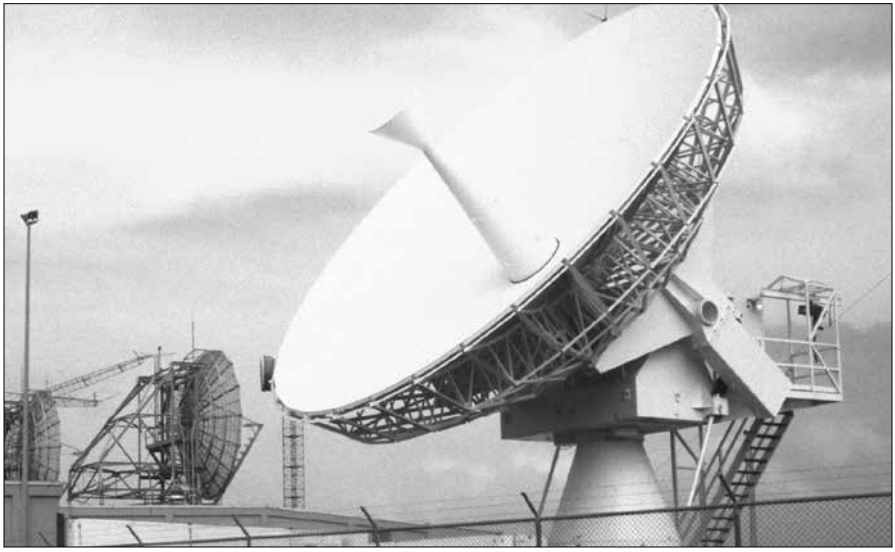
In December 1988, NIS caught Randall Bush, a 23-year-old radioman, in an undercover counterespionage operation.[162] During a meeting in a hotel room, the NIS undercover agent made a controlled purchase of classified information and made no pretense of being a foreigner.[163]

[161] "Narcotics and National Security," National Security Decision Directive no. 221 (Washington, DC: White House, 8 April 1986); Statement of Frank Conahan, Department of Defense Counter-Drug Activities, *[General Accounting Office] Review of [Department of Defense] Compliance with FY 1989 [Department of Defense] Authorization Act* (Washington, DC: General Accounting Office, 17 October 1989); Memorandum for the Deputy Attorney General from Stephen Colgate, "Overview of Federal Counternarcotics Intelligence Centers," 7 March 1996, Record Group 60: General Records of the Department of Justice, Series: Files of Associate Deputy Attorney General Merrick B. Garland, File Unit: DEA/Drug Intelligence Centers, NAID: 44134503, NARA, 5; and Scott Allen, "Hot on Their Trail: Navy, Law Enforcement Agencies Team up to Stop Drug Smugglers," *All Hands* (June 1990): 18–19.

[162] Public information was sparse as there was no press coverage of this case.

[163] "Espionage" video.

Figure 61. Satellite communications dish



Source: National Archives and Records Administration, College Park, MD.

U.S. Navy radioman Randall S. Bush worked with equipment like this satellite communications dish.

Investigation and Punishment

During the meeting, Bush offered to continue to provide classified information throughout his Navy tour and then, after attending college, to resume selling classified from a position within the FBI, CIA, or Drug Enforcement Administration.

Bush was arrested and charged with UCMJ espionage violations.[164] Sentenced to 18 years, he served 13 and was released in 2002.[165]

Significance

Bush was another strategically insignificant but militarily effective financial volunteer. As a radioman, like Walker, Bush could have caused

[164] *Espionage*, 34; and *A Counterintelligence Reader*, 296.
[165] "Find an Inmate: Randall Bush," Bureau of Prisons, accessed 14 May 2020.

serious damage, but the quick undercover response led by NIS neutralized him.

Lessons Learned

This was the first of several undercover espionage responses led by NIS, demonstrating that on some occasions, the DON conducted these investigations without FBI assistance.

"Smarter than Walker": A Classified Memories Case

The next case spans the winter of 1988–89. The Soviet Union's domestic and international situation was grim. The arms race begun by the United States in 1979 was having the desired effect, driving the Soviet economy into ruin. As Soviet internal political controls relaxed to stimulate the economy, supporters of democracy in Communist-controlled eastern Europe rose in bloodless revolutions called "Velvet Revolutions." Unlike in the past, the Soviet Union did not respond with force, and one by one the countries of eastern Europe separated from the Soviet Union and became democracies. In hindsight, this was clearly the first stage of failure for the Soviet Union.[166]

Meanwhile, during the previous decade, the FBI had perfected its ability to respond to financial volunteers who contacted Soviet diplomatic establishments. That was where this next case began, with the FBI and NIS lying in wait as a sad character tried to capitalize on his memories of classified information to feed his drug habit.

---

[166] Coit D. Blacker, "The Collapse of Soviet Power in Europe," *Foreign Affairs* 70, no. 1 (1990/1991): 88–102, https://doi.org/10.2307/20044696; Mark Kramer, "The Demise of the Soviet Bloc," *Journal of Modern History* 83, no. 4 (2011): 788–854, https://doi.org/10.1086/662547; and Hill, "The Collapse of the Soviet Union," 37–42.

Figure 62. Lockheed P-3 Orion sensor operators

Source: National Archives and Records Administration, College Park, MD.

Like these sailors, former U.S. Navy antisubmarine warfare operator chief Craig D. Kunkle served as a sensor operator aboard a Lockheed P-3 Orion patrol aircraft.

1988: Craig D. Kunkle

Background

In 1988, Craig D. Kunkle was a narcotics-abusing 39-year-old security guard at the Portsmouth General Hospital in Virginia. A formerly stellar aviation antisubmarine warfare operator chief, he was discharged under less than honorable conditions three years earlier after he was

convicted of indecent exposure and serious problems with alcohol. Kunkle was the son of a decorated Navy pilot, his older brother was a Navy commander, and his younger brother was a former Navy lieutenant.[167]

Initiation and Espionage

In December 1988, Kunkle contacted the Soviet embassy in Washington, DC, to offer to sell military secrets. Undercover FBI special agent Dimitry Droujinsky responded. Kunkle claimed to be angry at the Navy for his discharge and wanted money. Droujinsky asked Kunkle to mail information to a cover address to prove his access. Kunkle mailed the FBI classified notes he made from memory.[168]

Investigation and Punishment

The FBI, along with NIS, arranged a meeting with Kunkle in January 1989 at a motel in Williamsburg, Virginia. At the meeting, Kunkle bragged that he was smarter than Walker and brought a copy of his service record. He also proposed that he rent a condominium overlooking the submarine base in Norfolk to report U.S. Navy submarine movements to the Soviets. After accepting $5,000, Kunkle was arrested.[169] In May 1989, he pled guilty to violating the espionage statute. He was sentenced to 12 years and served 10.[170]

---

[167] Douglas Ashley, "Spy Suspect Asks Judge to Move Trial from Area," *Daily Press* (Newport News, VA), 27 January 1989, B4; and Robert Becker, "Information Could Have Helped Soviet Subs," *Daily Press* (Newport News, VA), 11 January 1989, A6.

[168] Wise, "The FBI's Fake Russian Agent Reveals His Secrets"; and McNair, "Revenge behind Try to Sell Secrets."

[169] Wise, "The FBI's Fake Russian Agent Reveals His Secrets"; "Ex-sailor Arrested in Bid to Sell Secrets: Calls to Soviet Embassy Monitored," *Pittsburg* (*PA*) *Post-Gazette*, 11 January 1989, 1; and Nancy Cook, "Beach Man Charged with Espionage: Sting Yields Documents on Sub Tracking," *Daily Press* (Newport News, VA), 11 January 1989.

[170] Michell Miller, "Former Seaman Pleads Guilty to Espionage Charge," United Press International, 4 May 1989; and "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."

Significance

Kunkle was a strategically insignificant but militarily effective financial volunteer case. Because he lacked ongoing access, the Soviets were unlikely to respond to his offer, and the damage he could have done would have been limited. In any case, the FBI and NIS quickly neutralized Kunkle through an efficient undercover operation and the Soviets did not acquire an *unexpected advantage*.

Lessons Learned

Kunkle was the second case in which a member or former member of the DON attempted to contact an adversary embassy to commit espionage and instead the FBI snared them in an undercover operation. Ellis was the first such case, and more would follow. This case also marked the first time that a member or former member of the DON attempted to sell classified information from memory. Again, more would follow.

Another Partner Espionage Case

This next case brief offers a good example of how NIS could easily cross over from a criminal investigation to a counterintelligence investigation. An existing criminal case of simple theft of aircraft spare parts became much more serious when investigators realized that the subjects had access to classified information. By introducing an Iranian "foreign buyer," the investigators were able to test the willingness of the subjects to not only steal from the Navy but to commit espionage as well.

Despite the U.S. Navy's conflict with Iran in the Tanker War of the 1980s, strategically this case was meaningless.[171] Walker and Souther

[171] Samuel J. Cox, "No Higher Honor: The Road to Operation Praying Mantis," Naval History and Heritage Command, 18 April 1988.

were both gone, and the Navy's information was largely secure. The Soviet economy was beginning to collapse and its leadership was beginning to loosen controls to reform from within—an experiment that would end in disaster for the Communist regime.[172]

Despite these facts, the Navy clearly had a problem, and this case highlighted it: narcotics use. In 1981, an aircraft accident aboard the USS *Nimitz* (CVN 68) killed 14 sailors, injured another 48, and caused damage that cost an estimated $150 million to repair. Six of the dead sailors tested positive for marijuana, and the pilot was using over-the-counter cold medicine, but none of that was found to be a contributing factor in the accident. However, the resulting publicity was very negative, and in response the Navy intensified its existing drug testing program and throughout the 1980s steadily expanded the urinalysis program and lowered the limits for those tests. In spite of all this, in 1988, nearly 5 percent of all military personnel still admitted to using drugs during the past 30 days.[173]

As most law enforcement authorities know, drug abuse is a major driver for crimes of all kinds, as users attempt to scrape together enough funds for the next purchase. According to the DOJ, "The evidence indicates that drug users are more likely than nonusers to commit crimes. . . . over the life-course, opiate users have elevated rates of

[172] Hill, "The Collapse of the Soviet Union," 37–42.

[173] Commander Carrier Group Four, "Investigation to Inquire into the Facts and Circumstances Concern[ing] an Accident and Subsequent Events Occurring on Board USS *Nimitz* (CVN 68) on 26 and 27 May 1981, Involving EA-6B Aircraft BUNO 159910 from Marine Tactical Electronics Warfare Squadron Two," Department of the Navy, 30 June 1981, 45; Leo A Cangianelli, "The Effects of a Drug Testing Program in the Navy," in *Problems of Drug Dependence 1989: Proceedings of the 51st Annual Scientific Meeting of the Committee on Problems of Drug Dependence, Inc.*, National Institute on Drug Abuse Research Monograph 95, ed. Louis S. Harris (Rockville, MD: National Institute on Drug Abuse, 1989), 212–13; and "Military Drug Program Historical Timeline," Department of Defense, Office of the Under Secretary for Personnel and Readiness, accessed 17 April 2021.

acquisitive offending."[174] Like the Tobias case in 1984, this case brief was just another example of that trend.

1989: Donald W. King and Ronald D. Graf

Background

In January 1989, Donald W. King and Ronald D. Graf were both 23-year-old aviation storekeeper airmen with Naval Air Reserve Patrol Squadron 94 at NAS Belle Chase, New Orleans. Cocaine users, the pair was in financial trouble and discussed a plan to steal and sell parts for P-3 Orion aircraft. They shared their idea with an individual who later approached NIS and provided their identities.[175]

In the 1980s, several allied countries and one adversary, Iran, employed the P-3. In 1975–76, the Imperial Iranian Air Force bought six P-3s, several of which remain in service today with the Islamic Republic of Iran Air Force. Due to U.S. sanctions, Iran can only repair its P-3s using spare parts smuggled into the country.[176] The King and Graf case was not the first case of its kind in the Navy, as in 1985 an active-duty aviation storekeeper and a Navy civilian were convicted in an Iranian P-3 parts smuggling case that did not involve espionage.[177]

Investigation and Punishment

With that previous case in mind, NIS responded to King and Graf's approach with an undercover operation in which an NIS agent posed

[174] Tina L. Dorsey, ed., *Drugs and Crime Facts* (Washington, DC: Department of Justice, 2004), 5; "Fact Sheet: Drug-Related Crime," Department of Justice, Bureau of Justice Statistics, 1994; and Matthias Pierce et al., "Insights into the Link between Drug Use and Criminality: Lifetime Offending of Criminally-Active Opiate Users," *Drug and Alcohol Dependence* 179 (2017): 309–16, https://doi.org/10.1016/j.drugalcdep.2017.07.024.
[175] "Navy Accuses 2 of Espionage, Theft," *Sacramento* (*CA*) *Bee*, 5 March 1989, A5; and "Grand Island Man Accused of Trying to Sell Data on Bombers," *Lincoln* (*NE*) *Star*, 11 March 1989, 17.
[176] Dylan Malyasov, "Iranian P-3 Aircraft Flew Dangerously Close to U.S. Navy Warships," *Defence Blog*, 29 November 2019.
[177] Merrill Hartson, "FBI Arrests Five in Alleged Plot to Smuggle Arms to Iran," Associated Press, 16 July 1985.

Figure 63. Lockheed P-3 Orion

Source: San Diego Air and Space Museum Archive.

U.S. Navy aviation storekeepers Donald W. King and Ronald D. Graf were assigned to Naval Air Reserve Patrol Squadron 94, the "Crawfishers," which flew the Lockheed P-3 Orion maritime patrol aircraft.

as a foreign buyer. NIS never identified Iran but strongly hinted that the ruse suggested an Iranian buyer. The pair sold approximately 30 items to the undercover agent, including classified aircraft parts and manuals. With King and Graf willing to sell classified information to a foreign power, the investigation shifted from a theft and export control case to an espionage case. NIS arrested King and Graf in March 1989.[178]

King and Graf pled guilty to UCMJ espionage violations. King was sentenced to 10 years and received a bad-conduct discharge, while Graf was sentenced to 5 years and also received a bad-conduct discharge.[179]

[178] "2 at New Orleans Base Accused of Espionage," *New York Times*, 6 March 1989.
[179] "Navy Airmen Sentenced in Spy Case," United Press International, 7 July 1989; and "Abilenian Arrested, Accused of Espionage," *Abilene* (*TX*) *Reporter-News*, 11 March 1989, 12.

Significance

The King and Graf case was a strategically insignificant but militarily effective financial volunteer case. Given its struggle to control the shipping lanes in the Persian Gulf for the past several decades, Iran would have benefitted from acquiring the classified parts to maintain the maritime surveillance capabilities of their aging P-3 aircraft. However, there was never any actual Iranian involvement in the case and no chance for Iran to achieve an *unexpected advantage*. The NIS undercover reaction to the informant's information was swift and the pair was effectively neutralized.

Lessons Learned

King and Graf were the DON's third partner espionage case and the second NIS-led undercover espionage reaction. Moreover, what began as a theft case turned into espionage. Criminal leads rarely became important leads for counterintelligence purposes, but in this case NIS was prepared. Thanks to earlier cases such as Tobias and Wilmot, NIS was also prepared for the possibility that additional coconspirators were involved.

Mentally Disturbed Classified Memories

The next case brief was somewhat like the Pickering case in 1983. Essentially, both cases involved people with access to classified information who had an untreated mental illness. The entire case unfolded without NIS participation, mostly due to the length of time that the subject had been out of the Marine Corps and the type of classified information he compromised.

Strategically, the Velvet Revolutions continued to collapse Communism in eastern Europe.[180] However, perhaps more importantly, during the same summer that the next case brief unfolded, protests in the PRC set the stage for the U.S.-PRC confrontation of today.[181]

In 1972, President Richard M. Nixon worked to open "Red China" as an ally that would help contain North Vietnam and pressure the Soviet Union. The anti-Soviet partnership grew to such a point that in the 1980s the United States began military sales to the PRC. In the same way that eastern European countries began to shed Communism, a student-led democracy movement in the PRC began its own protest against the single-party rule of the CCP. However, in June 1989, the CCP sent the PLA to attack the protesters, killing at least hundreds and possibly thousands of unarmed civilians.[182]

To survive the protests, the CCP regime veered away from Communism, established its own brand of market-economy socialism, and forced the Chinese people to accept economic benefits in exchange for their political freedom. That tradeoff set the stage for the PRC's enormous economic growth, which fueled the CCP's military expansion.[183]

That was where this case brief began. With Communism on the rocks around the world, a mentally ill former Marine was out of money and ideas.

---

[180] John Lamberton Harper, *The Cold War* (Oxford, UK: Oxford University Press, 2011), 232–42.
[181] "Lessons of the 40 Years since Nixon Went to China," CNN, 21 February 2012.
[182] Evelyn Goh, "Nixon, Kissinger, and the 'Soviet Card' in the U.S. Opening to China, 1971–1974," *Diplomatic History* 29, no. 3 (June 2005): 475–502; William Tow and Douglas Stuart, "China's Military Turns to the West," *International Affairs* 57, no. 2 (Spring 1981): 295–97, https://doi.org/10.2307/2619165; and Cindy Cox, "Chronology of Events Related to the 1989 Tiananmen Square Incident," *World Affairs* 152, no. 3 (Winter 1989–1990): 129–34.
[183] "Lessons of the 40 years since Nixon went to China."

Figure 64. PRD-1 radio direction finder

Source: National Security Agency, X (formerly Twitter) post, 13 September 2018.

The PRD-1 radio direction finder was used extensively by U.S. Marine Corps tactical signals intelligence operators such as Frank A. Nesbitt in Vietnam.

1989: Frank A. Nesbitt

Background

In 1989, Frank A. Nesbitt was a 44-year-old former Marine Corps chief warrant officer and enlisted U.S. Air Force and Marine Corps signals intelligence operator who had served in Vietnam with the Marine Corps' 1st Radio Battalion.[184] For reasons not publicly available, he was forced to resign from the Corps in 1979 and was working in information technology for a law firm in Tennessee. He had held no security clearance for a decade.[185]

[184] "K-Bay Salutes," *Windward Marine*, 11 June 1971, 6; "Recruiters Say: Strike Boosts Enlistments," *Eugene* (*OR*) *Guard*, 9 August 1963, 6B; "Germany is First Residence," *Fresno* (*CA*) *Bee Republican*, 12 October 1965, 15-A; "15 SNCO's Selected for DCP," *Marine Corps Gazette* 59, no. 8 (August 1975): 2; and *Congressional Record–Senate, August 25–September 12, 1978*, vol. 124, pt. 21 (Washington, DC: Government Printing Office, 1978), 28080.

[185] "Arrested Would-be Spy Says He Wanted to Cross Soviets," *Palm Beach* (*CA*) *Post*, 16 October 1989, 5A; and "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."

Initiation and Espionage

That summer, Nesbitt was experiencing mental health problems when he abruptly left his wife and began traveling in Central and South America. According to Nesbitt, while he was drifting through Bolivia, he met members of a touring Soviet ballet company who introduced him to Soviet diplomats. Nesbitt then agreed to a KGB debrief in exchange for money. The Soviets flew him from Peru to Moscow, where the KGB interviewed him for 11 days in exchange for $2,000. Nesbitt provided the Soviets more than 60 pages of top-secret information, including maps and diagrams, pertaining to U.S. signals intelligence activities. Although the information was dated, Nesbitt disclosed targets and procedures still in operation and caused significant damage to intelligence efforts.[186] The KGB then allegedly asked Nesbitt to return to the United States to act as a courier for a KGB asset working at the Los Alamos National Lab, New Mexico, where Nesbitt had worked briefly after resigning his commission.[187]

Investigation and Punishment

However, during his return travel, Nesbitt instead contacted U.S. authorities and confessed, hoping to offer his services as a double agent. The FBI ignored his offer and arrested him, but not before Nesbitt gave a full interview to the press.[188]

Nesbitt pled guilty to violating the espionage statute. In April 1990, he was sentenced to 10 years in a psychiatric treatment facility and

[186] Memorandum for the Honorable Charles F.C. Ruff, Counsel to the President, "Recommended Denials of Executive Clemency—16 Petitions for Commutation Sentence," Washington, DC: Office of the Deputy Attorney General, 19 March 1997.
[187] "Frank Arnold Nesbitt, Petitioner, v. United States of America, Respondent," U.S. District Court for the Eastern District of Virginia, 6 September 1991; and Michael York, "Odyssey of a Suspected Spy," *Washington Post*, 15 October 1989.
[188] "Frank Arnold Nesbitt, Petitioner, v. United States of America, Respondent; and York, "Odyssey of a Suspected Spy."

was released in 1998.[189] He was arrested again in 2004 at the age of 60 for attempting to rob a bank in Orlando, Florida, in a bid to go back to prison for medical care.[190]

Significance

Nesbitt was a strategically insignificant but militarily effective financial volunteer case for the DON but appears to have had some impact on U.S. intelligence activities. There was essentially no means by which naval counterintelligence could have interdicted him, but he was thoroughly debriefed after his return. Since his information was related to intelligence vice operations, it likely had only a tangential influence on the United States' confrontation with the Soviet Union and probably provided the adversary with no *unexpected advantage*.

Lessons Learned

Nesbitt was the DON's third "classified from memory" case and the second department-related subject taken to the adversary country for debriefing, with Pollard being the first. Nesbitt was the first adversary attempt to reuse a naval asset in another intelligence capacity after exhausting their memory of classified information.

Another Failed Walker Copycat

The next case brief was another sad example of a sailor who was out of money and ideas. Contrary to the routine, in this case, one of the NIS counterintelligence briefs blanketing the Navy had the opposite of their intended effect. The brief helped the subject plan his espionage, but to no avail because one of his shipmates took the message to heart.

---

[189] "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996"; and "Find an Inmate: Frank Arnold Nesbitt," Bureau of Prisons, accessed 18 May 2020.
[190] "Man Robs Bank Hoping to Go to Federal Prison, but Gets State," WFTV Orlando, 8 July 2005; and "Hold ups: The High Price of Health Care," *Washington Post Express*, 12 July 2005, 2.

While the premise of this case appears ridiculous and was another in a long series of petty espionage attempts, readers should remember that Walker should have been a ridiculous petty espionage attempt, but mistakes allowed his case to balloon into the most serious espionage the DON ever experienced.

This case should also drive home a key theme of this study: that occasionally desperate sailors and Marines turned to espionage.

1989: Charles E. Schoof and John J. Haeger

Background

In 1989, Charles E. Schoof and John J. Haeger were, respectively, 20- and 19-year-old operations specialists third class assigned to the tank landing ship USS *Fairfax County* (LST 1193) in Norfolk, Virginia. Haeger, due to receive a large trust fund when he turned 21, was doing well in the Navy. Schoof, broke because of drinking and drugs, was recently demoted from duty in the ship's combat information center (CIC) to the deck division due to an unauthorized absence.[191]

Initiation and Espionage

In October 1989, Schoof, now without access to the classified information in the CIC, suggested to Haeger, who had access to the CIC safe, that they sell classified information to the Soviets. Inexplicably, Haeger agreed, and they stole 12 classified microfiche, which Schoof hid in his shipboard locker. Later that month, a NIS counterintelligence brief inspired Schoof to emulate Walker, and he contacted the Soviet embassy twice, unsuccessfully asking them to come to Norfolk.[192]

[191] "Espionage" video.
[192] "United States v. Charles E. Schoof, Operations Specialist Third Class (E-4), U.S. Navy," U.S. Navy–Marine Corps Court of Military Review, 30 January 1992.

Figure 65. Charles E. Schoof and John J. Haeger

Source: "Espionage," Naval Criminal Investigative Service, 1995, video.

U.S. Navy operations specialists third class Charles E. Schoof (left) and John J. Haeger, 1989.

Investigation and Punishment

In November, Schoof began to drive to Washington, DC, to sell the microfiche to the Soviets but changed his mind. Back in Norfolk, while drinking heavily at a bar, he met Peter Atkins, a former *Fairfax County* shipmate on terminal leave. Schoof offered Atkins $1,000 to drive him to Washington, but Atkins instead reported the incident. A search of the CIC confirmed the microfiche were missing, and NIS quickly arrested Schoof and Haeger.[193]

[193] "United States v. Charles E. Schoof, Operations Specialist Third Class (E-4), U.S. Navy"; and "Ex-sailor Who Helped Navy Crack Latest Spy Case Miffed," *Daily News Leader* (Staunton, VA), 5 February 1990, A3.

Both men were convicted of UCMJ espionage violations. Schoof was sentenced to 25 years, while Haeger was sentenced to 19 years.[194] Both men were eligible for parole in 1996.[195]

Significance

The Schoof and Haeger case was a strategically insignificant but militarily effective financial volunteer case. The pair never actually contacted the Soviets and were interdicted thanks to the prompt action of a well-intentioned shipmate and the immediate response of NIS. There was never an opportunity for the Soviets to achieve an *unexpected advantage*.

Lessons Learned

Schoof and Haeger were the fourth and last known case of partner espionage. Partner espionage often presented with one subject having a security clearance while the other did not. This case was also the fourth time in which a coworker reported espionage, highlighting both the importance of the NIS counterintelligence briefings that generated espionage leads and the rapid investigations of those reports.

A "Big Dumb" Final Soviet Espionage Attempt

This next case brief was last of the Cold War. One year later, the Soviet Union collapsed and its republics began to separate into independent countries.

The collapse of the Warsaw Pact in 1990 foretold the fate of the Soviet Union. As background, in 1949, the United States led the effort to

[194] "John J. Haeger, Petitioner-Appellant v. Michael A. Lansing, Commandant, [United States Disciplinary Barracks]–Ft. Leavenworth, Kansas, Respondent-Appellee," U.S. Court of Appeals Tenth Circuit, 9 February 2001.
[195] "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."

create the North Atlantic Treaty Organization (NATO) to contain the Soviet Union. The Soviets reacted with a massive anti-NATO disinformation operation that amplified the rhetoric of "peace campaigners," in much the same way that the Russians are doing today. In 1955, West Germany became a NATO member, which the Soviets, looking back to World War II, believed was an offensive threat. They reacted by forming the Warsaw Pact, which included all the Communist-led eastern European countries. These were the countries that Cordrey contacted during his espionage attempt in 1984. With democracies emerging quickly in eastern Europe, the Warsaw Pact dissolved in 1990, leaving NATO "victorious."[196]

While this case brief was a sad final chapter of inane Cold War espionage attempts, the 1990 demise of the Warsaw Pact is key to understanding the modern-day Russian obsession with breaking up NATO. In the Russian view, the loss of the protective buffer zone between Russia and Western Europe was devastating and hastened the demise of the Soviet Union. Today, new NATO members in Eastern Europe have edged right up to the Russian border, which increases the anxieties of the Russian authorities about an effort to remove them from their posts by force. No matter how illogical that may seem to NATO, those are the Russian fears, and they explain why Russia spends so much time and effort combating NATO, just as the Soviet Union did in the early 1950s.[197]

[196] "The Warsaw Treaty Organization, 1955," U.S. Department of State, Office of the Historian, accessed 27 January 2024; Lawrence S. Kaplan, "NATO and the Warsaw Pact: The Past," in *The Warsaw Pact: Political Purpose and Military Means*, ed. Robert W. Clawson and Lawrence S. Kaplan (Wilmington, DE: Scholarly Resources, 1982), 67–91; and Mark Kramer, "The Collapse of East European Communism and the Repercussions within the Soviet Union (Part 1)," *Journal of Cold War Studies* 5, no. 4 (2003): 202–3.

[197] Benn Steil, "Russia's Clash with the West Is about Geography, Not Ideology," *Foreign Policy*, 12 February 2018.

Against that strategic background, a "big, dumb" Marine, as his staff noncommissioned officer called him, was looking for some extra money and stumbled into the FBI's counterintelligence net.[198]

1990: Charles F. L. Anzalone

Background

In 1990, Charles F. L. Anzalone was a 23-year-old Marine corporal telephone lineman assigned to Marine Corps Air Station Yuma, Arizona. In November, he contacted the Soviet embassy in Washington, DC, regarding college scholarships and asked to be recontacted at his residence.[199]

Investigation and Punishment

While the Soviets never recontacted him, an FBI undercover agent did. Anzalone asked that the Soviet government pay for his college education in return for U.S. government information that he would supply.[200]

In the now-perfected technique, an FBI undercover agent met Anzalone in a hotel in Yuma in February 1991. At the meeting and through the mail, Anzalone sold the undercover agent several restricted technical manuals for cryptographic equipment, an expired flight line security badge, and guard schedules for the weapons storage area.[201]

Anzalone was arrested and convicted of espionage, as well as adultery and marijuana use. He was sentenced to 15 years, which was reduced to 8 by military clemency granted by the outgoing Secretary of

[198] Montgomery, "Sucker or Spy."
[199] Montgomery, "Sucker or Spy"; and "Charles Anzalone," Facebook, accessed 12 May 2020, hereafter Charles Anzalone Facebook page.
[200] Ray Tessler, "Video of Hotel Meeting Shown at Spy Trial," *Los Angeles Times*, 2 May 1991.
[201] Tessler, "Video of Hotel Meeting Shown at Spy Trial."

Figure 66. Charles F. L. Anzalone

Source: "Charles Anzalone," Facebook, n.d.

U.S. Marine Corps corporal Charles F. L. Anzalone, 1989.

the Navy in 1992. Anzalone was paroled in 1994.[202] He continues to maintain that the FBI entrapped him.[203]

Significance

Anzalone was a strategically insignificant, militarily effective financial volunteer case. Whether he intended to do so or not, Anzalone never had the opportunity to compromise any sensitive information due to the rapid response by the FBI. There was never an opportunity for the Soviets to achieve an *unexpected advantage*.

Lessons Learned

The Anzalone case marked the third time that a sailor or Marine attempted to contact an adversary diplomatic establishment to volunteer to commit espionage that resulted in an undercover response. That

[202] David Montgomery, "Jamestown Marine Is Granted Clemency: Accused Spy Anzalone Now Eligible for Parole This Year," *Buffalo* (*NY*) *News*, 15 January 1993; and "Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996."
[203] Charles Anzalone Facebook page.

type of response was extremely effective when rapidly conducted, before the adversary could apply tradecraft to the relationship.

Naval Counterintelligence Keeps Pace, 1980–92

For U.S. naval counterintelligence, the late Cold War period was an awakening. Finally receiving dedicated, trained personnel with the authority to bring espionage cases to prosecution, the DON was involved in nearly as many espionage prosecutions during those 12 years as it was during the entire time between 1898 and 2010.

This period also saw the introduction of the seminal Horton Clause, which leveraged the long sentences of the Espionage Act to extract full confessions, backed by a polygraph, to ensure that the DON was not subject to an adversary's *unexpected advantage*. This merger of intelligence and law enforcement was the critical step in ensuring that naval counterintelligence cases were militarily effective. Based on the cases considered in this study, once prosecutors introduced the Horton Clause and U.S. counterintelligence neutralized lingering cases such as Walker and Souther, the DON did not suffer any further cases of an insider repeatedly compromising classified information to the United States' most likely adversary, the Soviet Union.

While the DON obviously botched the Souther case, overreacted to the Lonetree case, and had to remedy the aftermath of the Walker case, NIS and the FBI quickly and efficiently handled more than two dozen other naval espionage cases. Moreover, the DON and the FBI honed the undercover espionage response model during this period. The FBI ran the 1983 Ellis and 1984 Wolff cases alone and detained both men within a day. Beginning in 1986, naval counterintelligence conducted a half-dozen undercover espionage response themselves or

jointly with the FBI. These swift responses helped ensure the Soviet Union did not benefit from any further *unexpected advantages*.

During this period, NIS cooperation with the FBI and several other U.S. agencies also grew, strengthening the DON's counterintelligence response. Finally, allied counterespionage cooperation grew with Japan, likely referring one case lead that led to prosecutions.

This period also saw the introduction of several novel espionage twists: partner espionage, allied espionage, hoarder espionage, and deserter espionage. Partner espionage, in which two coconspirators operated together, occurred four times in just five years and never again since. However, later years would see the unique circumstances of allied and deserter espionage repeated.

Lessons Learned

Overall, during the 12 years of the late Cold War period, naval counterintelligence recognized the Soviet Union as the United States' strategic adversary and was able to take advantage of the legal tools provided by FISA, CIPA, and the Horton Clause to largely neutralize espionage within the DON. Moreover, the department's efforts to increase retention likely assisted naval counterintelligence by reducing the financial and family pressures on its personnel. After struggling for 75 years, naval counterintelligence had finally found its stride.

Chapter 5
Post-Cold War Case Briefs, 1993–2010

By 1991, attempts to restructure the Soviet economy by dismantling the repressive Communist regime put in place by Joseph Stalin were failing. The bloated Soviet bureaucracy resisted change and attempted a coup. The ensuing struggle and chaos destroyed the Soviet Union and ended the Cold War. The end of the decades-long conflict left the United States as the world's sole super power.[1]

Since World War II, throughout the Cold War and beyond, the United States had major interest in the oilfields of the Middle East, and since 1944 the U.S. military had maintained a training unit in Saudi Arabia. In the early 1990s, this unit, called the U.S. Military Training Mission in Saudi Arabia, had several hundred personnel assigned and acquired increased importance after the skirmishes with Iran during the Tanker War in 1987–88 and the 1990–91 Gulf War with Iraq.[2]

[1] Coit D. Blacker, "The Collapse of Soviet Power in Europe," *Foreign Affairs* 70, no. 1 (1990): 88–102, https://doi.org/10.2307/20044696; Mark Kramer, "The Demise of the Soviet Bloc," *Journal of Modern History* 83, no. 4 (December 2011): 788–854, https://doi.org/10.1086/662547; and Ron Hill, "The Collapse of the Soviet Union," *History Ireland* 13, no. 2 (March/April 2005): 37–42.

[2] MajGen Silas R. Johnson Jr., USAF, "United States Military Training Mission: A Paradigm for Regional Security," *DISAM Journal of International Security Assistance Management* 23, no. 3 (Spring 2001): 97–102; Samuel J. Cox, "No Higher Honor: The Road to Operation Praying Mantis," Naval History and Heritage Command, 18 April 1988; *Gulf War Air Power Survey*, vol. 3, *Logistics and Support* (Washington, DC: U.S. Government Printing Office, 1993), 37; and Anthony Cordesman, *Saudi Military Forces Enter the 21st Century* (Washington, DC: Center for Strategic and International Studies, 2001), 117, 238–39.

As with Pollard's espionage for Israel and Allen's espionage for the Philippines, there were Department of the Navy (DON) personnel who thought that U.S. allies were not getting enough information from the United States. Additionally, as with Dickinson, Souther, and, again, Pollard, there were people who became ideologically attached to foreign entities and were willing to spy for them. In the special case of Pollard, the combination of allies and ideologic motivation proved to be a particularly potent mixture.

At the investigative level, a notable fact in this case was the use of electronic media. Through the early Cold War period, all espionage within the DON involved passage of hard-copy documents. That limited the movement of information due to bulk; the Pollard case was a prime example of how the bulk of the paperwork burdened an espionage operation. Later, espionage began to include microfiche, which allowed for faster movement of information with less bulk. Now, with the introduction of computers into the working levels of the U.S. Navy and Marine Corps in the early 1990s, the first espionage involving electronic media occurred.

Also around this time, in the face of questions about several high-profile investigations, the DON renamed the Naval Investigative Service (NIS) the Naval Criminal Investigative Service (NCIS) and placed the agency under civilian leadership in 1992.[3]

The first espionage case brief to take place in the post-Cold War era began with a U.S. Navy officer doing a joint tour overseas. This officer had been a hostage of the Iraqi government in 1990, early in the Gulf War. Now, embedded with the Royal Saudi Navy, the lines seemingly began to blur for him.

[3] "History of the NCIS," *Commanding Officer's Guide to NCIS* (Quantico, VA: Naval Criminal Investigative Service, n.d.), 9; and Art Pine, "Naval Investigative Service to Be Revamped," *Los Angeles Times*, 26 September 1992.

Figure 67. U.S. Military Training Mission, Saudi Arabia

Sources: Wikimedia Commons, courtesy of Ameen Mohammad.

U.S. Navy lieutenant commander Michael S. Schwartz was assigned to the U.S. Military Training Mission in Saudi Arabia in support of the Royal Saudi Navy.

1992: Michael S. Schwartz

Background

In 1992, Michael S. Schwartz was a 41-year-old lieutenant commander assigned to the U.S. Military Training Mission (USMTM) in Riyadh, Saudi Arabia. He had started his career as a radarman aboard the aircraft carrier USS *Coral Sea* (CV 43) in the early 1970s and returned to Texas in 1973 to attend college, graduating with a bachelor's degree in criminal justice in 1977.[4] Commissioned as a Navy officer in 1980, Schwartz was on temporary duty at the U.S. embassy in Kuwait when Iraq invaded in 1990. He was one of several hundred foreign hostages held by the Iraqi government as human shields against Coalition air attacks.[5]

[4] "Our Men in Service," *El Paso* (*TX*) *Times*, 26 December 1971, 8B.

[5] Paul W. Westermeyer, *U.S. Marines in the Gulf War, 1990–1991: Liberating Kuwait* (Quantico, VA: Marine Corps History Division, 2014), 25–31, 55, 101; "El Pasoan Saw Executions in Kuwait," *El Paso* (*TX*) *Times*, 13 December 1990, 2B; and Janet Perez, "With Son in Kuwait, El Paso Family Keeps an Optimistic Outlook," *El Paso* (*TX*) *Times*, 18 August 1990, 2B.

Initiation and Espionage

In 1992 at the USMTM, Schwartz began unilaterally passing secret documents on computer diskettes to Royal Saudi Navy personnel. In 1994, another U.S. officer learned that the Saudis possessed unapproved classified material.

Investigation and Punishment

The ensuing NCIS investigation identified Schwartz and confirmed the original allegation. Reportedly, the Saudis neither solicited nor paid Schwartz, who appeared to have simply overstepped the bounds of cooperation in the immediate wake of the Gulf War. Schwartz did not receive any money, and officials suggested Schwartz was just trying to be friendly and cooperative.[6]

Prosecutors initially charged Schwartz with Uniform Code of Military Justice (UCMJ) espionage violations. However, he agreed to a plea bargain, in which he would receive no prosecution in return for an other-than-honorable discharge and no retirement benefits.[7] This suggests that prosecutors lacked enough evidence to convict Schwartz. However, some observers speculated that the United States minimized Schwartz's case to prevent public criticism of the politically sensitive U.S.-Saudi alliance.[8]

Significance

Schwartz was a strategically insignificant, partially militarily successful potential ideological volunteer case. While he overstepped the bounds of the intelligence sharing agreement between the United

[6] "American Naval Officer Is Accused of Passing Secrets to Saudi Arabia," *Los Angeles Times*, 25 May 1995; and "Norfolk Naval Officer Faces Court-Martial in Espionage Case," *Washington Post*, 13 September 1995.
[7] *Espionage Cases, 1975–2004: Summaries and Sources* (Monterey, CA: Defense Personnel Security Research Center, 2004), 41.
[8] Joshua Teitelbaum, "Saudi Arabia," in *Middle East Contemporary Survey*, ed. Bruce Maddy-Weitzman (Boulder, CO: Westview Press, 1995), 546.

States and Saudi Arabia, his motivation was never publicly revealed. Often in these cases, such as the Dickinson and Pollard cases, the subject overidentifies with a foreign culture. That could be what happened to Schwartz and could explain why he may have been an ideological volunteer. Despite his motivation, the compromises appear to have done little damage to the U.S.-Saudi relationship, and the Saudis did not achieve an *unexpected advantage*.

Lessons Learned

The Schwartz case was a watershed event, in that it was the first digital compromise to a foreign power in the DON's history. It would be nine years before the next digital case occurred. The Schwartz case should have prompted some controls over removable computer media.

Espionage in Margaritaville

While the Communist regimes in the Soviet Union and eastern Europe had collapsed in the late 1980s and early 1990s, just 145 kilometers south of Key West, Florida, another Communist regime clung to power. The United States and Cuba had clashed seriously twice already during the Cold War: a failed U.S. invasion of the island country in 1961 and a near-nuclear confrontation over the presence of Soviet nuclear missiles in Cuba in 1962.[9] For the rest of the Cold War, the United States and Cuba fought each other in proxy wars and minor combat in Africa, the Caribbean and Latin America, to include Angola in 1971–91, Grenada in 1983, Nicaragua in 1979–87, and Panama in 1988–89.[10]

---

[9] "U.S.-Cuba Relations, 1959–2021," Council on Foreign Relations, accessed 27 April 2021.
[10] "Proxy Wars during the Cold War: Africa," Atomic Heritage Foundation, 24 August 2018; "United States Invades Grenada," History Channel, accessed 27 April 2021; "More Cubans May Be in Nicaragua," *Los Angeles Times*, 15 February 1987, 1; and LtCol Nicholas Reynolds, USMCR, *Just Cause: Marine Operations in Panama, 1988–1990* (Washington, DC: History and Museums Division, Headquarters Marine Corps, 1996), 10.

Against this background of animosity, Cuba's leaders were wary of a U.S. attack. The closest U.S. air base to the Cuban capital of Havana was Naval Air Station (NAS) Boca Chica in Key West. A U.S. Navy McDonnell Douglas F/A-18 Hornet fighter flying at top speed from Boca Chica could be over Havana in less than 10 minutes. As a result, the Cubans reasoned that a visual observer in Key West could identify the telltale signs of a surprise attack from the United States.[11] While there were several technologically advanced ways to watch an airfield and provide warning, the basic method was the same as it had been during the Kuehn, Othmer, and Yoshikawa cases just before World War II and possibly the Mak case during the Vietnam War—to place an observer in or near a strategic base or port.

That was where the next case began, with a nervous Communist regime just a short hop from Florida looking for a *time and place advantage* in the event of a U.S. surprise attack.

1993: Antonio Guerrero

Background

In 1993, Antonio Guerrero was a 35-year-old Cuban civil engineer recruited by Cuban intelligence to gain access to NAS Boca Chica as part of an agent network that came to be known as the Red Wasp Network. Born in the United States to Cuban parents, Guerrero and his parents returned to Cuba when he was a boy, but he retained his U.S. citizenship.[12]

Initiation and Espionage

With a plausible false personal history and documents produced by Cuban intelligence, a *legend* in intelligence jargon, to explain his background, U.S. Navy Public Works hired Guerrero in 1994. He imme-

[11] David Adams, "Spy Suspect Reported on MacDill," *Tampa Bay (FL) Times*, 17 January 2005, 4A.
[12] Wayne Carter, "A Look at the 'Cuban Five' Agents Jailed in the U.S.," *Dallas* (*TX*) *Morning News*, 17 December 2014.

Figure 68. The Cuban Five

Source: Wikimedia Commons.

Antonio Guerrero (center) and his coconspirators were celebrated as heroes in Cuba.

diately began sending information to Cuba on encrypted computer diskettes via his handlers, who were under nonofficial cover in Miami. Guerrero met them once or twice per month and used pager codes to signal for immediate contact. For four years, Guerrero sent nearly 400 reports including information about aircraft movements (especially surveillance aircraft), communications systems, security arrangements, and potential future espionage recruits.[13]

Investigation and Punishment

The investigation against Guerrero began when, sometime prior to 1995, a Cuban intelligence cryptographer volunteered to commit espionage for the Central Intelligence Agency (CIA). His information led

[13] Curt Anderson, "Cuban Spy Gets Reduced Sentence of about 22 Years," *San Diego* (*CA*) *Union-Tribune*, 13 October 2009.

to the breaking of Cuba's coded messages, which its intelligence service broadcast to agents around the world.[14] Just as the Federal Bureau of Investigation (FBI) operation that netted more than 30 German spies of the Duquesne Spy Ring in 1941 started with the ring's radio operator 55 years earlier, the Cuban cryptographer provided leads for numerous Cuban espionage cases, including Guerrero.[15] As in 1940, years of surveillance provided reams of evidence that allowed the FBI to net as many agents as possible.[16] In September 1998, another member of the network was preparing to flee the United States after his laptop and encrypted diskettes were stolen.[17] Within days, the FBI hastily arrested the entire network.

In 2001, Guerrero was sentenced to life for violating the espionage statute. In 2009, his sentence was reduced to 22 years, and in 2014 Guerrero and the entire Red Wasp Network were exchanged for U.S. assets in Cuban prisons, including the cryptographer that helped unmask them.[18]

Significance

Guerrero was a potentially strategically significant and partially militarily successful patriotic penetration case. While he had no access to classified information, Guerrero's persistent and lengthy access to NAS Boca Chica made him an ideal indication and warning collection asset. Should the United States have considered some type of military action against Cuba between 1994 and 1998, Guerrero might have been

[14] Elias Groll, "Agent at Center of Spy Swap Was Cuban Crypto Expert," *Foreign Policy*, 19 December 2014.
[15] "Subject: Frederick Duquesne: Interesting Case Write-Up," Federal Bureau of Investigation, 12 March 1985; and Carol J. Williams, "Cuban-Born Spy Credited with Exposing Fidel Castro's U.S. Operatives," *Los Angeles Times*, 18 December 2014.
[16] Tim Collie, "A Glimpse Inside the Lives of Suspected Cuban Spies," *Chicago Tribune*, 16 September 1998.
[17] Kirk Nielsen, "Inside the Wasp's Nest," *Miami* (*FL*) *New Times*, 22 February 2001.
[18] Anderson, "Cuban Spy Gets Reduced Sentence of about 22 Years"; and "U.S. Wins Big with Release of Blue Chip Spy Held in Cuba," *CBS Miami*, 17 December 2014.

able to warn the Cubans well in advance. Because Guerrero was able to gain employment aboard the naval base and report for a period before the FBI detected him, this case was only partially militarily successful. The Cubans, for a period, did achieve an *unexpected advantage* over the DON. However, Guerrero was likely under close surveillance for much of his time in Key West, Florida, which would have limited the military utility of his intelligence collection.

Lessons Learned

Guerrero was the fourth and last patriotic penetration case to affect the DON. A somewhat dated concept, open-source information and commercially available satellite imagery largely replaced this type of collection. Mak and Guerrero were patriotic penetrations, and both were detected based on information derived from a CIA recruitment of an asset within the foreign intelligence service. The other two patriotic penetrations, Jahnke (perhaps) and Yoshikawa, occurred prior to World War II, and naval counterintelligence never fully identified them as such. The CIA's work against foreign intelligence services proved vital to uncovering Mak and Guerrero, and close cooperation between them and naval counterintelligence was a bedrock requirement.

Espionage Nest Egg

This next case brief was yet another example of allied espionage. In this case, like that of Allen, the allied intelligence service recruited the subject in place in exchange for potential business-related favors.

Strategically, during this time, Russia continued to struggle through post-Soviet chaos and the former Yugoslavia broke up amid ethnic violence and civil war.[19] Just as this case began, the international

[19] Mark Galeotti, *We Need to Talk about Putin: How the West Gets Him Wrong* (London: Ebury Press, 2019), 24, 37–41, 79.

community brokered a peace agreement in Yugoslavia, and the United States and the North Atlantic Treaty Organization (NATO) deployed a peacekeeping force into Bosnia.[20] Two years earlier, a little-known terrorist group called al-Qaeda used a truck bomb to attack the World Trade Center in New York City.[21]

While the former Yugoslavia, Iran, Iraq, and al-Qaeda distracted the United States, the People's Republic of China (PRC) quietly initiated its naval modernization program. Like the United States in the 1880s and Japan in the early 1900s, the PRC began seeking naval technologies from around the world in the 1990s. By 2008, the People's Liberation Army (PLA) Navy had improved enough to deploy away from the coastline of China for the first time, and in 2012 the PRC commissioned its first aircraft carrier.[22]

At the investigative level, this case was critical to the future of NCIS. It broke just as NCIS emerged from a three-year pause in new special agent hires.[23] Soon after, NCIS expanded on the early 1980s NIS initiative to train several hundred individual counterintelligence agents by forming a specialized counterespionage unit.[24]

Additionally, because of the agent-analyst teaming that had occurred in the Philippines in the late 1980s, investigators in this case

[20] R. Cody Phillips, *Bosnia-Herzegovina: The U.S. Army's Role in Peace Enforcement Operations, 1995–2004* (Washington, DC: U.S. Army Center of Military History, 2005), 5.
[21] "World Trade Center Bombing 1993," Federal Bureau of Investigation, accessed 13 December 2023.
[22] Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2021); and Alison A. Kaufman, *China's Participation in Anti-Piracy Operations off the Horn of Africa: Drivers and Implications* (Arlington, VA: Center for Naval Analysis, 2009).
[23] Dana Rosenberg, *The Story behind the Naval Criminal Investigative Service* (Quantico, VA: Naval Criminal Investigative Service, 2004), 9–10.
[24] "What Do You Know about Espionage in the U.S. Navy?," NCIS Association History Project, 1 December 2019; *NCIS-1* (Quantico, VA: Naval Criminal Investigative Service, 2013), 88; *U.S. Department of Defense Inspector General Semiannual Report to the Congress, April 1, 2012–September 30, 2012* (Alexandria, VA: Department of Defense Office Inspector General, 2012), 91; and "John Shea v. United States, Defendant," U.S. Court of Federal Claims, 31 January 2018, 3.

brought in a former active-duty U.S. Navy intelligence officer who had teamed with NIS, John Beattie. Now a civilian employee, Beattie's tactical analysis was critical to proving this case, and he received a Defense Counterintelligence Award for his efforts.[25]

Meanwhile, an aging civil servant looking for a soft retirement opportunity found himself at a crossroads. He chose the wrong direction.

1995: Robert C. Kim

Background

In 1995, Robert C. Kim was a 56-year-old civilian computer specialist in the Maritime Systems Directorate at the Office of Naval Intelligence (ONI) in Suitland, Maryland. Kim, a naturalized U.S. citizen, was a technical support engineer for an ONI maritime domain awareness system. Born in South Korea, he had moved to the United States in 1966 as an adult.[26]

Initiation and Espionage

In November 1995, ONI assigned Kim to act as a translator during an information exchange meeting. There, he met Republic of Korea (ROK) Navy captain Baek Dong-Il, a South Korean naval attaché. Baek, frustrated by the pace of U.S. information sharing, recruited Kim as a source. In January 1996, Kim began removing classified documents from ONI and giving them to Baek to curry favor for a retirement job as an ROK Navy computer consultant.[27]

---

[25] "Two from NCIS Receive DOD FCI Awards," *U.S. Naval Criminal Investigative Service Bulletin* 2, no. 6 (October 1998): 15.

[26] "Robert Kim's American Passion," Korean Broadcasting System, 29 August 2018.

[27] "Two from NCIS Receive DOD FCI Awards"; Dongryong Oh, "'Former Naval Officer to the U.S., Baek Dong-il, Took off His Military Uniform in the 'Robert Kim Incident'," *Chosun Pub*, 1 November 2016; and Charles W. Hall, "Kim Allegedly Sought Job with S. Korea," *Washington Post*, 2 October 1996.

Figure 69. Office of Naval Intelligence

Source: National Archives and Records Administration, College Park, MD.
Robert Chaegon Kim worked for the Office of Naval Intelligence.

Investigation and Punishment

Eventually, the FBI and NCIS learned of Kim's contacts with Baek. The resulting investigation included computer searches, physical and technical surveillance, and a mail cover, all of which confirmed that Kim was compromising classified information. Employing little tradecraft, Kim and Baek frequently spoke on the telephone and even went golfing together. The investigation did not uncover any wider conspiracy.[28]

By September 1996, NCIS and the FBI were ready to arrest Kim. However, a warning of his impending arrest was prematurely released to senior U.S. Navy leaders, and the investigators scrambled to arrest Kim before he could become aware of the investigation and escape. The FBI and NCIS arrested Kim at Fort Myer in Arlington, Virginia, while he was attending a South Korean Armed Forces Day reception.[29]

[28] Richard Keil, "U.S. Military Worker Arrested after Passing Documents to S. Korea," Associated Press, 26 September 1996.
[29] Charles W. Hall and Dana Priest, "Navy Worker Is Accused of Passing Secrets," *Washington Post*, 26 September 1996.

Kim pled guilty to violating the espionage statute and was sentenced to nine years.[30] He served seven years and was released in 2004.[31]

Significance

Kim was a strategically insignificant, militarily effective recruitment-in-place case. The information he compromised had little effect on any potential naval campaign, and he was apparently carefully monitored almost from the start of his relationship with Baek. It was unclear if the DON would have eventually provided the information to South Korea anyway. No U.S. adversary achieved an *unexpected advantage*.

Lessons Learned

Kim was the fourth allied espionage case to affect the DON. The investigators used every tool available to prove the case against Kim, which allowed the U.S. government to arrange a plea deal. The Horton Clause of 1982 remained a critical tool for the DON.

Cold War Hangover

As the Kim investigation proceeded, another case opened and closed. The strategic situation remained the same, with the former Soviet Union in chaos. However, as this case brief will show, the counterintelligence situation remained largely unchanged.

In 1993, 10 days of street fighting in Moscow over control of the Russian government killed several hundred before forces loyal to Russian president Boris Yeltsin prevailed. Soon after, a corrupt election voted in right-wing nationalists and kept the president in power. Cru-

[30] Brooke A. Masters, "Va. Man Sentenced to 9 Years in Spy Case," *Washington Post*, 12 July 1997.
[31] "Find an Inmate: Robert Kim," Bureau of Prisons, accessed 11 February 2021; and Barbara Demick, "Bitter South Koreans Rally behind Spy Convicted in U.S.," *Los Angeles Times*, 8 June 2004.

cially, in 1996, a former Soviet Committee for State Security (KGB) officer turned politician named Vladimir Putin was named to a critical position overseeing the transfer of Soviet state property to private businesses. To ensure the support of Russia's emerging business elite, the oligarchs, Yeltsin had Putin illegally sell off the remaining old Soviet infrastructure at bargain prices.[32] This set the stage for today's modern Russian state.

Meanwhile, a desperate U.S. Navy sailor turned to espionage and, like most financial volunteers, turned to the "enemy in the news."

1996: Kurt G. Lessenthien

Background

In 1996, Kurt G. Lessenthien was a 29-year-old machinists' mate first class serving as an instructor at the Naval Nuclear Power School in Orlando, Florida. Lessenthien had previously served on two ballistic missile submarines, an attack submarine, and a submarine tender, USS *Simon Lake* (AS 33), coincidently the same tender on which Ledbetter served in 1967.[33]

Investigation and Punishment

Having squandered thousands of dollars in pursuit of romance, by 1996 Lessenthien was seriously in debt. In a throwback to the Cold War, in March, he reportedly contacted the Russian embassy in Washington, DC, offering to sell classified information that he had been hoarding among his personal belongings. An undercover FBI agent responded,

[32] Hill, "The Collapse of the Soviet Union," 37–42; and Galeotti, *We Need to Talk about Putin*.
[33] Jim Leusner and Tom Leithauser, "Orlando Sailor in Spy Arrest," *Orlando* (*FL*) *Sentinel*, 24 April 1996; and "Navy Prosecutor Seeks Life in Prison for Spy," *Daily Press* (Newport News, VA), 25 October 1996, A5.

Figure 70. USS *Tennessee* (SSBN 734)

Source: Defense Visual Information Distribution Service.

U.S. Navy machinist's mate first class Kurt G. Lessenthien served aboard USS *Tennessee* (SSBN 734).

and Lessenthien mailed an initial package of classified information to an FBI accommodation address.[34]

In April 1996, Lessenthien met with the undercover agent at a hotel in Orlando and was arrested. He pled guilty to UCMJ espionage violations and was sentenced to 27 years, of which he served 15.[35]

Significance

Lessenthien was a strategically insignificant, militarily effective financial volunteer case. He never provided any information to the Russians and consequently they did not achieve an *unexpected advantage*.

[34] Robert Burns, "Navy Man Arrested on Spy Charge Offered Secrets to Russia," Associated Press, 24 April 1996; and William McMichael, "Would-be Spy Did All for Love," *Daily Press* (Newport News, VA), 25 October 1996.

[35] "Would-be Spy Gets 27 Years behind Bars," *Deseret News* (Salt Lake City, UT), 29 October 1996; and "Kurt Lessenthien," LinkedIn, accessed 11 February 2021.

Lessons Learned

Lessenthien was the fourth Navy or Marine Corps attempted espionage/undercover response case. While less frequent than a decade earlier, the FBI–NCIS response was a carbon copy of the Kunkle case—rapid and effective. Like Kunkle, Lessenthien pled guilty, suggesting that prosecutors were still using the Horton Clause more than a decade later. Finally, like Wolff in 1982 and Wold in 1983, Lessenthien was another case of hoarder espionage. He had amassed classified information at home, which he turned to when he became desperate for funds.

New Adversary, New Espionage

The next case brief did not begin for another six years, marking the longest period without a naval espionage case since the decade-long interval between the Wine case in 1968 and the Madsen case in 1979.

As the Soviet Navy rusted pier-side and the PRC had yet to build its modern navy, this break in espionage reflects the absence of a U.S. maritime adversary for much of the late 1990s. That changed in 2000 with the al-Qaeda attack on the guided missile destroyer USS *Cole* (DDG 67). In the wake of the *Cole* attack, the Navy substantially increased its defenses against asymmetric maritime attacks, and after the 11 September 2001 terrorist attacks in the United States, the Navy went on the offensive based on the now-discredited theory that al-Qaeda would move or attack using commercial shipping owned or controlled by the bin Laden family.[36]

[36] "Command Investigation into the Actions of USS *Cole* (DDG 67) in Preparing for and Undertaking a Brief Stop for Fuel at Bandar at Tawahi (Aden Harbor) Aden, Yemen on or about 12 October 2000," U.S. Navy, 27 November 2000; "United States v. Jamal Ahmed Mohammed, Ali Al-Badawi, and Fahd Al-Quso," U.S. District Court, Southern District of New York, 2003; John C. K. Daly, "Al Qaeda and Maritime Terrorism, Part 1," *Terrorism Monitor* 1, no. 4 (2003); Gregory Bereiter, *The U.S. Navy in Operation Enduring Freedom, 2001–2002* (Washington, DC: Naval History and Heritage Command, 2016); John Mintz, "15 Freighters Believed to

The sole success of the U.S. Navy's attempt to interdict al-Qaeda at sea was the widely publicized 2002 detention of 15 Pakistani nationals aboard a ship in the Mediterranean Sea who U.S. authorities alleged were tied to al-Qaeda. After 10 months' investigation, Italian authorities quietly released all 15.[37]

As happened in the 1970s with narcotics traffickers, with militant extremists in the news as a U.S. Navy adversary, it was only a matter of time before espionage emerged. Based on the nature of extremism, a financial volunteer was doubtful, but the other three types of espionage subjects were potentially damaging possibilities. During the United States' two decades of conflict against militant extremists since 2000, the U.S. military saw all three: ideological volunteers, recruitments-in-place, and patriotic penetrations.[38] This case saw the first active-duty U.S. military member commit espionage on behalf of the militant extremists.

That was where this next case brief began, with a sailor who was drifting toward extremism and preparing to deploy to the Persian Gulf deciding to give al-Qaeda a *time and place advantage* over his own ship.

2001: Hassan Abu-Jihaad

Background

In 2001, Hassan Abu-Jihaad was a 21-year-old signalman third class aboard the destroyer USS *Benfold* (DDG 65). He joined the Navy in 1998 but by 2000 was drifting toward militant extremism. Abu-Jihaad

---

Be Linked to Al Qaeda," *Washington Post*, 31 December 2002; Robert Ackerman, "Intelligence Empowers New Fleet Operations," *Signal Magazine* (December 2006); and William K. Rashbaum and Benjamin Weiser, "A Nation Challenged: Al Qaeda's Fleet; A Tramp Freighter's Money Trail to bin Laden," *New York Times*, 27 December 2001.

[37] Daniel Williams, "Detainees in Italy Seen as Al Qaeda," *Boston (MA) Globe*, 13 September 2002, A20; and "The 15 Pakistanis Arrested in Gela 10 Months Ago Have Been Freed: They Are Not Terrorists!," *Il Pane e le Rose*, 26 June 2003.

[38] "2004: Ryan Gibson Anderson," Defense Human Resources Activity, accessed 18 May 2021; Madeleine Gruen, "Backgrounder: Sgt. Hasan Akbar," National Education Association Foundation, January 2010; and "Nidal Hasan," Counter Extremism Project, accessed 18 May 2021.

had a security clearance and access to his ship's transit plan for its early 2001 deployment to the Persian Gulf.[39] The classified transit plan specified the battle group's itinerary, listing dates for anticipated port calls in Hawaii and Australia as well as its transit through the Strait of Hormuz.[40]

Initiation and Espionage

Using his official U.S. Navy email address, Abu-Jihaad had been communicating with British extremists running a United Kingdom-based online retailer called Azzam Publications that specialized in extremist literature and videos that encouraged his extremist views. In late February 2001, while in port in San Diego, California, Abu-Jihaad typed the classified transit plan into an email and sent it to Azzam, along with details of the vulnerabilities of U.S. Navy ships' defenses. Investigators later speculated that Abu-Jihaad's intent was to provide targeting data for militant extremists. However, nothing happened. In 2002, Abu-Jihaad was honorably discharged and returned home to Arizona, where he later became involved in a conspiracy to conduct a domestic terrorist attack.[41]

Investigation and Punishment

In December 2003, British investigators found a digital copy of the text of Abu-Jihaad's email on a diskette hidden in the bedroom of one of Azzam founders. A U.S. Department of Homeland Security investigator working with the British made the connection between

[39] "United States v. Hassan Abu-Jihaad," United States District Court, District of Connecticut, 4 March 2009; and "USS *Benfold* (DDG 65) Command History for CY 2001," Department of the Navy, 5 March 2002.
[40] "United States v. Hassan Abu-Jihaad"; Mark Kravitz, "Court Analyses Material Support to Terrorists—United States v. Abu-Jihaad No. 3:07CR57 (D. Conn. 03/04/2009)," U.S. District Court, District of Connecticut, 4 March 2009; and "Passing Secrets at Sea—To Terrorists, No Less," Federal Bureau of Investigation, 10 March 2008.
[41] Kravitz, "Court Analyses Material Support to Terrorists."

Figure 71. Hassan Abu-Jihaad

Source: "66th Military Intelligence Brigade Baseline Briefing" (Fort Belvoir, VA: Army Intelligence and Security Command, n.d.).

U.S. Navy signalman third class Hassan Abu-Jihaad, ca. 1998.

Abu-Jihaad's official U.S. Navy emails to Azzam and the email text because both referenced *Benfold*.[42]

In 2008, on the strength of the digital trail uncovered by investigators, Abu-Jihaad was convicted of violating the espionage statute and material support to terrorism and was sentenced to 10 years. He was released in 2016.[43]

Significance

Abu-Jihaad was a potentially strategically significant, militarily ineffective ideological volunteer. His compromise, if acted on, could have resulted in severe damage to or even the loss of one of the ships in his battle group, perhaps even his own. A second successful terrorist attack on a U.S. Navy ship would have had strategic impact on the

[42] "The 'Unremarkable' Life of a Sailor Turned Terror Suspect," *Hartford* (*CT*) *Courant*, 24 February 2008.

[43] "United States v. Hassan Abu-Jihaad. 3:07CR57 (MRK) (District of Connecticut)," U.S. Attorney's Office, District of Connecticut, 18 March 2015; and "Passing Secrets at Sea."

Global War on Terrorism. Despite Abu-Jihaad's extremist leanings and open use of U.S. Navy email to contact extremist-promoting propagandists, he was neither reported nor investigated. Naval counterintelligence only discovered his duplicity long after the fact, making this case militarily ineffective. Like Yoshikawa 60 years before, Abu-Jihaad provided a *time and place advantage* to an adversary. Fortunately for the DON, as happened with Yoshikawa in 1941, the adversary did not use the intelligence to their best advantage.

Lessons Learned

Abu-Jihaad was the DON's fifth ideological volunteer and the second who received no money for their trouble. Nine years after Schwartz became the first all-digital compromise, Abu-Jihaad was the first use of email for espionage in the DON's history.

The Papier-Mâché Pig

The next case brief segues from Cold War hangover espionage into the future, the current reality today. Like the narcotics smugglers of the 1970s, the press in the 1980s, and militant extremists in the 2000s, there was always a new adversary over the horizon.

Using unthinkably poor intelligence tradecraft, this was the tale of a bumbling PLA military intelligence operation that was nonetheless successful in pilfering some classified information. Because the operation could not withstand even the slightest counterintelligence scrutiny, it never had a chance of becoming a long-term penetration. This case, and others like it, are best described as "smash-and-grab" espionage. In this case, the PLA spent a decade putting an intelligence asset in place in the United States and then left him exposed through sloppy tradecraft.

The likely reason behind this failure was reminiscent of a story about a papier-mâché pig during the Chinese Communist Party's

(CCP) "Great Leap Forward." The Great Leap Forward (1958–63) was a catastrophically ill-advised CCP plan of forced agricultural collectivization and rural industrialization that resulted in financial ruin and tens of millions dead from starvation.[44] Part of this tragedy was an epidemic of self-deception as local CCP leaders faked results to match the unrealistic expectations of the central government. In one instance, commune leaders claimed to have bred a pig the size of a truck. Everyone in the commune cheered at the amazing feat of animal husbandry. It was no matter that the pig was fake and just made of papier-mâché.[45]

Like the CCP's papier-mâché pig, in this case, PLA military intelligence deceived itself into believing that their espionage operation against the United States was both secure and worth the human cost. Neither was true. This case indicated that local CCP leaders were still more than willing to fake results, even to the point of self-destruction.

That was where this story began, as PLA military intelligence tried to determine what *manner advantage* Taiwan had achieved and deceived a longtime asset, who in turn deceived his subsource, a former U.S. Navy sailor turned bureaucrat with information about foreign military sales to Taiwan. Was the information critical enough for the PRC to risk their longtime asset? Probably not, but the CCP demanded results. What they got was another papier-mâché pig.

2004: Gregg W. Bergersen

Background

In 2004, Gregg W. Bergersen was a 47-year-old Navy veteran employed by the Navy International Programs Office (NIPO), where he directed foreign military sales of command, control, communications, comput-

[44] Wei Li, and Dennis Tao Yang, "The Great Leap forward: Anatomy of a Central Planning Disaster," *Journal of Political Economy* 113, no. 4 (August 2005): 840–77, https://doi.org/10.1086/430804; and Felix Wemheuer, "Dealing with Responsibility for the Great Leap Famine in the People's Republic of China," *China Quarterly* 201, no. 10 (March 2010): 176–94.
[45] Jung Chang, *Wild Swans: Three Daughters of China* (London: Harper Collins, 1991), 297–98.

ers, intelligence, surveillance, and reconnaissance (C4ISR) systems. In 2005, Bergersen, who had a gambling and alcohol problem, moved to the Defense Security Cooperation Agency. His wife, who was not implicated, worked for NCIS.[46]

Initiation and Espionage

In 2004, while working on a program to sell Taiwan a version of the U.S. Joint Tactical Data Information System (JTIDS, or Link 16), a secure airborne situational awareness communications system, Bergersen met a U.S. businessman originally from Taiwan named Tai Shen Kuo.[47] Kuo was pursuing contracts related to the sale. Like Kim eight years before, Bergersen was thinking about a retirement job, and by 2006 he had begun feeding Kuo insider information, including classified information, about the system.[48]

Unbeknownst to Bergersen, Kuo had been an asset of PLA military intelligence since 1997. His handler was Lin Hong, who operated undercover from a government-backed overseas outreach group in the PRC and had participated in the Mak case. In return for the promise of future business opportunities in the PRC, Hong demanded U.S. military information from Kuo. Kuo responded by arranging for James W. Fondren Jr., a former U.S. Air Force officer and civilian U.S. Pacific Command official, to write opinion papers that incorporated classified information. When pressed for more sensitive information, Kuo began to cultivate Bergersen. As with Fondren, Kuo misled Bergersen to believe that he was providing the information to Taiwan, not the PRC.

[46] Stephanie Gaskell and Corky Siemaszko, "Spy Suspect Just an 'American Dad'," *New York Daily News*, 13 February 2008; "Espionage: Stealing America's Secrets," *CBS News*, YouTube video, 13:23, 29 August 2010; and "Gregg Bergersen," LinkedIn, accessed 16 February 2016. Note: Bergersen's LinkedIn profile has been removed as of 2021.
[47] "Link 16 Products," BAE Systems, accessed 16 December 2023.
[48] "How a Networking Immigrant Became a Chinese Spy," *CBS News*, 9 May 2011; and "Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation," U.S. Department of Justice, 11 July 2008.

Figure 72. Defense Security Cooperation Agency

Source: Defense Visual Information Distribution Service.

Gregg W. Bergersen worked for the Defense Security Cooperation Agency.

Investigation and Punishment

The major mistake by PLA military intelligence was their failure to properly compartmentalize their agent operations. Hong provided identical contact information to both Kuo and Mak. In the same way that the Colombia-based German *Abwehr* agent's confession led to both Othmer and Koedel in 1944, Hong's lack of compartmentalization led directly from Mak to Kuo in 2004.[49]

In 2008, Bergersen pled guilty to violating the espionage statute and was sentenced to five years, of which he served three.[50]

[49] "Testimony before the U.S.-China Economic and Security Review Commission" (testimony, David Major, founder and president, CI Centre, 9 June 2016), 6–7; Bill Gertz, "Chinese Spy Buy Caught on Surveillance Video," *Washington Times*, 1 March 2010; Peter Grier, "Four Arrested on Charges of Spying for China," *Christian Science Monitor*, 13 February 2008; "United States v. Tai Shen Kuo, Gregg William Bergersen, and Yu Xin Kang," U.S. District Court for the Eastern District of Virginia, Alexandria Division; and David Wise, *Tiger Trap: America's Secret Spy War with China* (Boston, MA: Houghton Mifflin Harcourt, 2011), 223–24.

[50] "Find an Inmate: Gregg Bergersen," Bureau of Prisons, accessed 31 May 2020.

Significance

Bergersen was a strategically insignificant, militarily effective financial volunteer case. While he compromised aspects of a military command and control system, his guilty plea suggests that prosecutors used the Horton Clause and compelled him to divulge everything he compromised to reduce his sentence. The PRC gained some information but failed to achieve an *unexpected advantage* because the FBI quickly neutralized the PLA military intelligence operation.

Lessons Learned

The Bergersen case was complex. The PLA mixed incentives in the case, using connections and favors, called *guanxi*, to reward Kuo while Kuo used money to reward Bergersen. Because Kuo used Taiwan as a false flag (a false nationality), the case took on aspects of allied espionage like the Kim case. Allied espionage was particularly difficult to detect because there was legitimate contact, so it became difficult to parse out espionage. As a Taiwan false flag, Bergersen's meetings with Kuo did not arouse suspicion. Finally, as with the Guerrero case, the CIA's work against an adversary intelligence agency in the Mak case also provided a priceless lead in the Bergersen case. Moreover, as with the Germans in World War I, the Alvarez and Faucher cases, and the Othmer and Koedel cases, poor PLA compartmentalization of the Mak, Fondren, and Bergersen cases proved to be a major gaffe.

A Partially Successful Deserter-Spy

This next case brief was another Cold War throwback that occurred in 2005. At the strategic level, the U.S. Navy still reigned supreme, but both Russia and the PRC were beginning to stir.

The Russian Navy spent the decade of 1995–2005 trying keep its most capable platforms afloat while also attempting to invest in the future. Russia reduced the massive Soviet Navy by 75 percent and shifted

funds toward developing a smaller navy with more modern designs and systems.[51]

Meanwhile, the PRC's quiet naval modernization efforts sputtered along, mostly by purchasing bargains discarded by the Russian Navy.[52] Simultaneously, the PRC ramped up its efforts to steal naval technology, but old-school methods were giving way to modern technology theft. NCIS and the FBI finally arrested Mak, the old-school technology theft exemplar, in 2005, and one year earlier, in 2004, the first publicly acknowledged PLA cyber theft of sensitive but unclassified U.S. Navy technical information occurred.[53]

At the investigative level, this case represented a watershed in naval espionage. Up until then, most subjects stole information using physical items such as paper copies or microfiche. In a limited way, Schwartz used diskettes in 1992 and Abu-Jihaad retyped classified information from a printed copy into an unclassified system. This next case demonstrated the near-total lack of control over some classified networks within military units. It should have been a wake-up call for the U.S. Department of Defense, but it was not. Five years later, a U.S. Army private would use the same type of access to compromise nearly 750,000 classified reports.[54]

---

[51] *The Russian Navy: A Historic Transition* (Suitland, MD: Office of Naval Intelligence, 2015), xix; Jacob W. Kipp, "Russian Naval Power under Vladimir Putin," in *The Russian Military in Contemporary Perspective*, ed. Stephen J. Blank (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2019); and Mikhail Vladimirovich Moskovenko, "Marine Doctrine of Russia: History and Present," Russian Navy, accessed 16 December 2023.

[52] *The People's Liberation Army Navy: A Modern Navy with Chinese Characteristics* (Suitland, MD: Office of Naval Intelligence, 2009), 16–30.

[53] Dorothy Denning, "Cyberwar: How Chinese Hackers Became a Major Threat to the U.S.," *Newsweek*, 5 October 2017; Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, 25 August 2005; and Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)," *Time*, 5 September 2005.

[54] Matt Sledge, "Bradley Manning Found Guilty of 19 Counts, Not Guilty of Aiding the Enemy," *Huffington Post*, 30 July 2013.

That was where this case began. An unhappy sailor was looking for a way to fund his desertion and decided to use his unfettered access to classified information systems as an enabler.

2005: Ariel J. Weinmann

Background

In 2005, Ariel J. Weinmann was a 22-year-old fire control technician third class aboard the nuclear attack submarine USS *Albuquerque* (SSN 706). Growing disillusioned with the Navy and having girlfriend problems, he decided to desert. Weinmann also objected to U.S. foreign policy and intelligence collection on U.S. allies. With his girlfriend now in boarding school in Switzerland, Weinmann, who was fluent in German, planned to desert, seek asylum in nearby Austria, and win her back.

Initiation and Espionage

In July 2005, Weinmann stole a government laptop, accessed the classified computer network aboard *Albuquerque*, downloaded several classified intelligence products about Austria that he thought he could use to apply for asylum as well as four classified Tomahawk cruise missile manuals, took his life savings of $7,000, and deserted.[55]

After abandoning his plans to win back his girlfriend and seek asylum in Austria, Weinmann walked into the Russian embassy in Vienna in October and attempted to trade the Tomahawk manuals for Russian citizenship and a university education. The Russians took the manuals but never recontacted him, so Weinmann shifted to planning to defect to Russia. Publicly available information sheds little light on his next

[55] Brock Vergakis, "Norfolk Is a Hotbed for Espionage Cases Involving the Navy," *Virginian-Pilot* (Norfolk, VA) , 14 April 2016.

Figure 73. Ariel J. Weinmann

Source: Wikimedia Commons.

U.S. Navy fire control technician third class Ariel J. Weinmann, ca. 2003.

moves, but Weinmann did travel to Mexico City, where he may have met with Russians again.[56]

Investigation and Punishment

In March 2006, while attempting to fly to Canada to visit his sister, Weinmann changed planes in Dallas, Texas, where U.S. Immigration and Customs Enforcement (ICE) detained him as a deserter. The ICE search of his belongings revealed cash and classified digital documents,

[56] Tim McGlone, "Sailor Sentenced to 12 Years in Prison for Espionage," *Virginian-Pilot* (Norfolk, VA), 7 December 2006.

so NCIS was alerted. In an extended series of interviews, Weinmann eventually confessed.[57]

Weinmann pled guilty to a variety of UCMJ violations including espionage. He was sentenced to 12 years and served 8. He pled not guilty to charges that he provided information to a foreign power in Bahrain during a port visit in 2005 and in Mexico City in 2006 while in deserter status.[58]

Significance

The Weinmann case was a strategically insignificant, militarily effective financial volunteer. Because he was a deserter, Weinmann never could have provided the routine, continuous access to sensitive information that the Russians likely sought. While he did compromise several technical manuals, NCIS was able to extract a confession, and then the Horton Clause ensured that Weinmann disclosed all his compromises, allowing the DON to adjust its plans accordingly. The Russian military probably did not achieve an *unexpected manner advantage* due to the compromise of the Tomahawk manuals.

Lessons Learned

Weinmann was the second of the DON's deserter-spies caught by U.S. Customs. Coberly, the Marine who deserted more than 20 years earlier, was the first. Weinmann was also the tenth espionage suspect in this study to conduct their initial approach overseas, and he was the first to commit all-digital naval espionage. Customs apprehensions

[57] Douglas Waller, "Did the Sailor Go Overboard?," *Time*, 9 August 2006; Barbara Starr, "Sources: Navy Sailor Suspected of Spying for Russia," CNN, 9 August 2006; Tim McGlone, "Why a Patriotic Teen Joined the Navy and Then Turned to Espionage," *Virginian-Pilot* (Norfolk, VA), 10 December 2006; Tim McGlone, "Navy Submariner Admits He Offered Military Secrets," *Virginian-Pilot* (Norfolk, VA), 5 December 2006; and Kate Wiltrout, "Recording Details Arrest of Sailor Accused of Espionage," *Virginian-Pilot* (Norfolk, VA), 11 August 2006.
[58] McGlone, "Sailor Sentenced to 12 Years in Prison for Espionage"; and "Ariel Weinmann-Rubino," Facebook, 18 May 2014.

of deserters was a rare but productive source of espionage leads. The DON overlooked the larger importance of the Weinmann case. Like Schwartz 13 years before, Weinmann downloaded classified without any oversight. The age of all-digital espionage had arrived, and authorities were still not placing limits on the ability of personnel to navigate and download material from classified systems without scrutiny. Another strategic warning was missed.

The Final Volunteer

The next case brief is also the last of this study. There is no definition of when events become history, but for the purposes of this study, the definition is approximately a decade. Events occurring less than a decade ago are difficult to examine without some prejudice. If events are any more current, personal involvement, actions of colleagues, and other issues make impartiality difficult. So, for the purposes of this study, 2010 was deemed the research limit for consideration of espionage cases.

Strategically, by 2009 the PLA Navy had deployed antipiracy task groups to the Gulf of Aden, and ONI optimistically noted that "none of these operations indicate a desire on the part of the PRC to develop a constant global presence."[59] Meanwhile, the Russian Navy gradually transformed into a twenty-first–century navy.[60]

[59] *The People's Liberation Army Navy*, 2; Jennifer Rice and Erik Robb, "The Origins of 'Near Seas Defense and Far Seas Protection'," U.S. Naval War College *China Maritime Report* no. 13 (February 2021): 13; and Andrew S. Erickson and Austin M. Strange, "China's Blue Soft Power," *Naval War College Review* 68, no. 1 (2015): 71–92.

[60] *The Russian Navy*, 16–17; O'Rourke, "China Naval Modernization"; and Andrew Bowen, *Russian Armed Forces: Capabilities* (Washington, DC: Congressional Research Service, 2020).

2010: Bryan M. Martin

Background

In 2010, Bryan M. Martin was a 22-year-old intelligence specialist third class in the Navy Reserve assigned to predeployment training at Fort Bragg, North Carolina, with U.S. Joint Special Operations Command.[61] Overextended due to gambling and prostitution debts, Martin was also recently engaged, and in an effort to shore up his personal finances to impress his father-in-law-to-be, he elected to steal and sell classified information.[62]

Investigation and Punishment

Martin decided to approach the PRC, thinking that they would pay the most for stolen classified information. He contacted the PRC and in return received a response from an FBI undercover agent. They arranged to meet in North Carolina.[63]

Like Lessenthien 14 years before, during the resulting meetings Martin made it clear that his motivation was financial. He told the undercover agent that he was seeking "long-term financial reimbursement" and that he could be very valuable over a 15- or 20-year career, which he expected would take him to the Defense Intelligence Agency.[64]

Martin was convicted of UCMJ espionage violations and sentenced to 48 years, reduced to 34 years for his cooperation in debriefing. As this case demonstrates, the Horton Clause was still in action 28 years later.[65]

---

[61] Tim McGlone, "Va. Beach-based Sailor Gets 34 Years in Espionage Case," *Virginian-Pilot* (Norfolk, VA), 11 May 2011. Note: Martin's Korean heritage was not a factor in his case.
[62] "Awareness in Action: Case Study: Bryan Martin," Defense Security Service, Center for Development of Security Excellence, accessed 9 February 2021.
[63] "U.S. Sailor Pleads Guilty to Attempted China Spying," Fox News, 19 May 2011.
[64] James Halpin, "NCIS: Sailor at Brag Sold Secret Documents," *Fayetteville* (*NC*) *Observer*, 4 December 2010.
[65] McGlone, "Va. Beach-based Sailor Gets 34 Years in Espionage Case."

Figure 74. Bryan M. Martin

Source: Defense Counterintelligence and Security Agency, Center for Development of Security Excellence.

U.S. Navy Reserve intelligence specialist third class Bryan M. Martin, 2010.

Significance

Martin was a strategically insignificant, militarily effective financial volunteer case. The FBI and NCIS interdicted Martin before he could compromise any information, thereby denying the PRC any *unexpected advantage*. The Horton Clause plea bargain ensured that Martin divulged any unobserved espionage contacts.

Lessons Learned

Martin was the fifth Navy or Marine Corps attempted espionage/undercover response case. The last such case had been 14 years earlier, but the FBI and NCIS did not miss a step in their response.

Naval Counterintelligence Pulls ahead, 1992–2010

In the aftermath of the Cold War, the United States faced no clear single adversary, and the espionage committed against the DON reflected that strategic ambiguity. At the beginning of this 18-year period, the espionage cases reflected fading Cold War adversaries, Russia and Cuba, as well as allies, South Korea and Saudi Arabia. As al-Qaeda emerged as an adversary, espionage followed, and as the PRC's military modernized, espionage followed again. This period followed the same pattern as others except with chaotic velocity. As the DON shifted from one adversary to another—former Soviet countries and allies to al-Qaeda and then to the PRC—naval counterintelligence followed and kept up with a bewildering array of new intelligence threats.

Strategically, none of the espionage conducted during this period was significant, and for the most part the cases were militarily effective, with naval counterintelligence generally doing a good job in working closely with the FBI and intelligence partners. Unlike previous periods in which naval counterintelligence could, at best, keep pace with the adversary, throughout the post-Cold War period through 2010, it was ahead of the adversary each time. The DON's persistent efforts to increase retention and recruiting in the Navy and Marine Corps likely further assisted naval counterintelligence by reducing financial and family pressures on its personnel.

Lessons Learned

NCIS did not forget the lessons learned in late-Cold War period and, understanding the degradation that might occur during such a period of strategic ambiguity, took steps to preserve its espionage investigative capability and capacity. Overall, during the 18 years of the post-Cold War period, naval counterintelligence continued to leverage

the Foreign Intelligence Surveillance Act, the Classified Information Procedures Act, and the Horton Clause to ensure that no adversary's advantage was *unexpected*. However, the DON continued to overlook the larger strategic shifts in espionage in response to naval innovations. The movement to internet-connected information systems by both the department and its contractors created a new vulnerability that the DON struggled to address.

Chapter 6
Lessons Learned: Toward Counterintelligence Operational Prioritization

Throughout the 112-year span of this study, espionage within the U.S. Department of the Navy (DON) was a low-probability, potentially high-impact problem that required constant attention. Espionage cases within the department were a relatively rare occurrence, with an average of one case every other year, but at times nearly a decade separated cases. However, even fewer of those cases were strategically significant enough to ascribe a true *unexpected time, place, or manner advantage* to an adversary of the United States. Only two cases, or 4 percent of the total, were strategically significant campaign-impacting espionage. Yoshikawa's successful observational espionage, which facilitated the surprise attack on Pearl Harbor, Hawaii, in 1941, was *unexpected* and gave a significant *time and place advantage* to the Imperial Japanese Navy (IJN) over the U.S. Navy's Pacific Fleet. On a much larger scale, Walker's successful espionage facilitated the Soviet Union's submarine development, which was *unexpected* and ascribed a theoretical *time and place advantage* over the DON. Those two cases occurred 24 years apart and concluded 44 years apart—low probability, high impact.

The Yoshikawa and Walker cases were strategically significant and surrounded in time by several espionage cases with engagement-impacting significance and many espionage cases with no significance

at all. However, nearly every espionage case had the potential to become strategically significant. A counterintelligence slip-up could have easily allowed a petty espionage attempt to blossom into another Walker case. For example, while Tobias made a hapless attempt at espionage in 1985, he had access to the same cryptographic material as Walker. If he had succeeded in making contact, the Soviets very likely could have used him to continue their decade of access to the DON's secure communications, with potentially disastrous results. Likewise, if Abu-Jihaad had succeeded in contacting al-Qaeda, he could have steered them toward several more USS *Cole* (DDG 67)-type attacks that would have had strategic impact on the Global War on Terrorism. Counterintelligence demands constant vigilance, no matter how distant the threat might appear.

Operational prioritization in any discipline requires a firm grasp of the tactical fundamentals, and counterintelligence is no exception. Without understanding espionage in its many manifestations within the DON, leaders cannot begin to structure a response that anticipates and neutralizes espionage before it can alter the outcome of a campaign. History can be a guide. By examining trends across more than a century of naval espionage, the DON can begin to anticipate future trends while also encouraging best practices that have succeeded in the past. Factors such as types of spies, security clearances, motivations, initiation, financial issues, detection, and military effectiveness have not changed for more than a century. Based on a firm understanding of those factors, the DON can begin to build an operational prioritization. This study's review of 57 historical naval espionage cases spanning from 1898 to 2010 has revealed some enduring lessons for naval counterintelligence.

Security Clearances and Espionage

While security clearances and espionage would appear to go together, this did not prove to be the case. Approximately one-third of all naval espionage subjects considered in this study did not have a security clearance, and more than one-half of them successfully gathered information, some of it classified. These cases generally fell into three groups: observational, thieves, and sensitive information.

- **Observational.** As previously discussed, these cases involved an asset that could simply observe a strategic site. For example, in 1941, in addition to Yoshikawa observing the U.S. Pacific Fleet at Pearl Harbor, Othmer observed Allied convoy departures from Norfolk, Virginia, for German naval intelligence. In the 1960s, Mak may have been observing the U.S. Pacific Fleet during port visits to Hong Kong for the People's Republic of China's (PRC) People's Liberation Army (PLA), an unproven allegation. In the 1990s, Guerrero was observing Naval Air Station (NAS) Key West, Florida, from within the fence line but without a clearance. As recently as 2022, Russian intelligence has allegedly been using the same tactic in Ukraine.[1]
- **Thieves.** Three naval espionage subjects considered in this study—Farnsworth, Thompson, and Pickering—did not have security clearances, but they took advantage of security lapses and stole unsecured classified information to sell. While this is a decidedly more difficult tactic, the technique is still used. For example, in 2017, a Russian military intelligence asset, a Ukrainian recruitment-in-place, accessed her supervisor's computer and stole classified information.[2]

[1] "The SBU Detained an Enemy Agent Who Was Collecting Intelligence for Missile Strikes on Odesa," Security Service of Ukraine, 4 July 2022.
[2] "National Guard Headquarters Clerk Recruited by Russian GRUshnik to Serve 4 Years," *Sud Reporter*, 27 January 2018.

- **Sensitive information.** Five naval espionage subjects considered in this study attempted to peddle sensitive but unclassified information, either their own observations or documents. Four of the five were Cold War-era Marines, all of whom were unsuccessful. The sixth was Mak, who provided vast numbers of sensitive but unclassified documents to his PLA handers and was the vanguard of today's cyber espionage.

Based on these findings, the lack of a security clearance should not preclude a counterintelligence investigation. Rather than simply gathering information for undefined future use, in wartime, observational spies such as Yoshikawa and Dickinson can direct strikes and provide battle damage assessment. Observers have the potential to be particularly dangerous because they can blend into the population and be very difficult to identify absent a suspension of civil rights that allows searches without probable cause.

Motivations for Espionage

A persistent question about espionage is motivation. For the cases considered in this study, the most elementary motivations were financial, ideological, and patriotism. Financial reward drove 60 percent of the subjects to initiate espionage, and two-thirds of those cases occurred between 1980 and 1990. Four convergent issues may have caused this spike in cases.

1. The U.S. Congress's efforts to address chronically low military pay in 1980–81 eroded during the next decade, leaving some sailors and Marines of the new all-volunteer force looking for ways to supplement their income.[3] As one Navy public affairs

[3] James R. Hosek, Christine E. Peterson, and Joanna Zorn Heilbrunn, *Military Pay Gaps and Caps* (Santa Monica, CA: Rand, 1994), 7.

officer said in 1986, "I think every enlisted man in the service has financial difficulties of some kind. Maybe all the recent publicity about spies and the big money they sold information for caused a young man to see some easy money out there."[4]

2. Family support programs had not kept pace with changing demographics in the all-volunteer force launched in 1974. The stresses placed on sailors and Marines and their families was significant.[5]
3. Substance abuse by military personnel increased indebtedness. Approximately one-third of the naval espionage subjects considered in this study abused drugs or alcohol, had a gambling problem, or had serious mental health issues.[6]
4. Changes in the law during 1979–81 made prosecuting espionage cases much easier.[7]

While it took a decade, pay increases for military servicemembers, drug testing, effective family support, and expanded counterintelligence authorities and expertise combined to suppress the 1980s espionage epidemic that plagued the DON. Despite those efforts, however, finances continued to loom large amongst espionage motivations during the post-Cold War period. Based on these historical cases, adversary intelligence services that did not accept volunteers, such as the Soviet Union in the early Cold War era and possibly the PRC, had a vastly reduced potential asset pool from within the U.S. Navy and Marine Corps.

---

[4] "Navy Concerned about Theft Motivation," *Journal Herald* (Dayton, OH), 12 March, 1986, 28NS.

[5] "40 Years of Meeting Your Needs . . . at Home and at Sea," Fleet and Family Support Center, 31 May 2019.

[6] "Military Drug Program Historical Timeline," Office of the Under Secretary of Defense for Personnel and Readiness, accessed 17 April 2021.

[7] Melanie Reid, "Secrets behind Secrets: Disclosure of Classified Information before and during Trial and Why CIPA Should Be Revamped," *Seton Hall Legislative Journal* 35, no. 2 (May 2011), 272–73.

A potentially problematic ideology motivated about 10 percent of the DON's espionage subjects considered in this study. From Dickinson, Souther, and Abu Jihaad's infatuation with the culture of a looming adversary to Pollard and Kim's divided loyalties with an ally, ideology pushed at least five subjects to espionage. However, all ideological cases considered in this study were similar in one respect: the subject's inordinate interests in a problematic ideology were well-known to their colleagues but ignored.

Espionage Instigation

Whatever the motivation, each of the DON's espionage subjects considered in this study initiated their espionage in one of two ways. Most, nearly 70 percent, initiated an approach to a foreign intelligence service, while the rest, about 30 percent, were sought out by a foreign intelligence service. Most of these subjects had no intelligence operations training or experience, which left them to either determine how to make an approach themselves or decide whether to trust the person who approached them. In general, approaches by the DON's espionage subjects took two forms: foreign establishments or existing relationships.

- **Foreign establishments.** Approximately one-third of all naval espionage subjects considered in this study approached a foreign diplomatic establishment, most seeking out the closest establishment, both within the United States and overseas. The exceptions were subjects who volunteered by mail. They often, but not exclusively, chose an adversary location overseas or otherwise far from their home. The foreign nation selected by these subjects was almost universally an adversary that was in the headlines at the time.
- **Existing relationships.** The other subjects became or attempted to become involved in espionage through some form of preexist-

ing nonintimate relationship. With one exception, none of these cases involved a spouse or lover. All were friends-of-friends or business contacts. Only one case, the unique case of Lonetree in Moscow during the Cold War, was the result of sexual entrapment.

Whatever their method of approach, more than one-half of all naval espionage subjects were arrested before committing espionage, and all of those were volunteers. The reason for their failure began first with the subject attempting to ineptly apply amateur espionage tradecraft. Then, U.S. counterintelligence authorities capitalized on these initial mistakes with rapid, effective investigative responses. While this failure rate was encouraging, it is important to remember that several levels of security and counterintelligence should have interdicted Walker, the most serious case in the DON's history, before he left the Soviet embassy in the back of a Soviet intelligence officer's automobile. Every case has the potential to be serious.

Espionage Profiles

A trend analysis of the DON's espionage cases considered in this study revealed that the subjects can be grouped according to two of the characteristics above: motivation and instigation. The trends indicate that four patterns of suspect motivation and instigation were often paired. These pairings suggest that the DON experienced four basic espionage profiles: financial volunteers, patriotic penetrations, ideological volunteers, and recruitments-in-place.

- **Financial volunteers.** Only approximately one-fifth of the financial volunteer espionage subjects considered in this study were successful, and only Japan and the Soviet Union/Russia ran them successfully. Japanese naval intelligence accepted financial volunteers as soon as war with the United States became a real

possibility, while the Soviets shifted to financial incentives by the 1960s only after the status of the American Communist Party plummeted and the Soviet Union's ideologically motivated asset pool diminished.[8] Although the case sample in this study is small, comprised only of Bergersen and Martin, this suggests that the PRC was either unwilling or unable to accept financial volunteers and preferred to approach espionage recruits themselves. The impact of financial volunteers during the Cold War was particularly acute because one of them, Walker, affected the strategic effectiveness of the U.S. Navy as a nuclear deterrent. This was because Walker did not only compromise the classified information in his possession but also enabled systemic Soviet access to classified information. That systemic access gave the Soviets 15 years of *unexpected time, place, and manner advantages.*

- **Ideological volunteers.** Ideological volunteers were also quite successful, with both Souther and Pollard compromising large quantities of classified information. However, Pollard's strategic impact was insignificant because, despite being *unexpected*, the information he compromised did not directly result in an adversary achieving *time, place, and manner advantages* that placed the U.S. Navy at a strategic disadvantage. Souther's strategic impact will never be certain because his case was militarily ineffective after his escape to the Soviet Union.
- **Patriotic penetrations and recruitments-in-place.** All patriotic penetrations and recruitments-in-place resulted in successful espionage, but the strategic impact was often minimal because while *unexpected*, their espionage did not result in *time, place, and manner advantages*. The assets' lack of placement and access limited the impact of patriotic penetrations because they gener-

[8] Frank Rafalko, ed., *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century* (Washington, DC: National Counterintelligence Center, 1998), 27; and John Barron, *KGB: The Secret Work of Soviet Secret Agents* (New York: Bantam Books, 1974), 472.

ally did not have security clearances. The exceptions were Yoshikawa, whose reporting from Hawaii lay the foundation for the Japan's surprise attack on Pearl Harbor, and Guerrero, because if the United States had attempted a surprise attack on Cuba, he might have been able to warn Cuba about it. Observer espionage appears to have limited impact in peace but was significant in war. That dichotomy should naturally lead to a continuous tension about naval counterintelligence operational prioritization.

In 1941, all navies had a limited ability to readily observe an adversary's base. While that capability may seem ubiquitous today, several potential adversaries of the United States who have developed over-the-horizon strike capabilities may not have developed the requisite remote surveillance capabilities. The Cuban intelligence operation involving Guerrero aboard NAS Key West in the early 1990s is an excellent example. A more recent example occurred in Ukraine in 2022, when Russian intelligence sought battle damage assessment (BDA) information from two recruitments-in-place during a Russian naval surface fire support campaign to destroy a strategic coastal bridge with long-range missiles.[9] As with the IJN's recruitment of Dickinson more than 60 years ago to provide BDA in the aftermath of the Pearl Harbor attack, Russian intelligence has continued to employ this rudimentary but time-tested technique during the Russo-Ukrainian War. Only the reporting technology changed; in 1941, it was an easily interpreted coded letter to a cover address in Peru that would have taken weeks to reach Japanese naval intelligence; and in 2022, it was a text message over an unbreakable encrypted messaging application that took seconds to reach Russian intelligence.

[9] "The SBU Detained an Enemy Agent Who Was Collecting Intelligence for Missile Strikes on Odesa"; and "The SBU Reported Suspicion to One of the Managers of Russia Today and Detained the Adjuster of the Missile Attacks in Odesa (Video)," Security Service of Ukraine, 18 June 2022.

Other than assets recruited solely for basic observation, adversary intelligence services often self-limited the impact of recruitments-in-place because of their perception of placement and access of their asset. For example, in 1937, the Soviets only extracted intelligence about Japan from Salich, while in 2008 the PRC pressed Bergersen solely for information about a single system that the United States intended to sell to Taiwan. The adversary intelligence service chose the assets for two attributes: they were known to the adversary intelligence service operative, and they had access to information that satisfied a specific information need. Perhaps the espionage could have expanded to other topics.

Espionage and Money

Another common perception is that espionage and money were analogous within the DON. This is an accurate observation. Fifty of the 58 naval espionage subjects considered in this study sought and/or received payment.

- **Financial volunteers.** As expected, virtually all financial volunteers considered in this study sought payment. The concept of financial inducement was central to this categorization.
- **Ideological volunteers.** Unexpectedly, ideological volunteers considered in this study were evenly split between seeking or eschewing payment. The difference appears to be specific to the individual and circumstances involved but could be the subject of additional study.
- **Recruitments-in-place.** Like financial volunteers, nearly all the recruitments-in-place considered in this study sought direct payment. However, the fraction that did not seek direct payment were instead recruited by an allied nation and sought indirect payment in the form of favorable treatment. The inducement was not always reflected in direct payment.

- **Patriotic penetrations.** Those who were recruited in their home country and then sent to specifically target the DON universally received no financial inducements. This may have been because they received a salary from their intelligence service, because their cover employment covered their costs, or possibly because they eschewed payment as a form of self-sacrifice for their cause.

Most espionage suspects considered in this study sought financial reward, suggesting that a suspect's finances were a central investigative topic. However, this study also suggests that if the suspect was a patriotic penetration or a recruitment-in-place, that review may not have been conclusive. Particularly for recruitments-in-place, this study suggests that investigators looked for indications of indirect payments in the form of favors.

Detecting Espionage

Most naval espionage cases were reported or discovered by agencies outside the DON, not by naval counterintelligence. Approximately one-third of the espionage subjects considered in this study were detected through source information such as Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) recruitments of foreign intelligence service personnel and criminal informants or through customs searches of deserters and spontaneous confessions. Less than one-fifth of the espionage subjects considered in this study were reported to the FBI or naval counterintelligence by coworkers or significant others, such as parents, spouses, lovers, and friends. Another 20 percent of the espionage subjects considered in this study became known after poor tradecraft by the foreign intelligence service was observed. A final 20 percent of the espionage subjects considered in this study were intercepted through surveillance of adversary intelligence services by the FBI domestically or by host nation services overseas.

With most of the espionage leads coming from outside the DON, this study suggests that to be effective, naval counterintelligence must be firmly connected with a wide variety of agencies and allies that can produce useful espionage leads. From a U.S. Customs agent in Dallas, Texas, to an FBI recruitment-in-place in Soviet military intelligence, all provided information that led to a successful prosecution and often a militarily effective conclusion that ensured that the DON did not suffer from an adversary's *unexpected advantage*. This study suggests that naval counterintelligence must be resourced to allow investment in the personnel and systems to ensure that flow of information.

Investigative Techniques

This study identified three advanced criminal investigative techniques—surveillance, interviewing, and undercover operations—that were pivotal in successfully concluding most naval espionage investigations. At least four other basic criminal investigative techniques identified in this study proved to be critical to successfully concluding a handful of naval espionage cases.

- **Surveillance.** Two-thirds of the investigations of espionage subjects considered in this study required technical and/or physical surveillance to resolve the allegations. This was because to prosecute the crime of espionage, the subject needed to be caught in the act. From the coverage of the Soviet consulate in San Francisco, California, that helped identify Ellis in 1983, to the physical surveillance by off-duty Washington, DC, police detectives that observed Farnsworth entering the Japanese naval attaché's apartment in 1935, surveillance of adversary intelligence officers and their potential assets produced the definitive information that forced defendants to plead guilty and agree to a polygraph for a reduced sentence. Surveillance was what made the Horton Clause workable and ensured that the DON did not suffer from

an adversary's *unexpected advantage*. Further, beyond traditional espionage, this study touched on how computer-based espionage presented the same training- and labor-intensive challenges for success. Both traditional and cyber surveillance were training- and labor-intensive capabilities that were critical to successful counterintelligence investigations.

- **Interview techniques.** Almost every successful espionage prosecution considered in this study involved some form of a subject interview to gain a confession. For that reason, skillful interviewing techniques were second to surveillance in espionage investigations. The topic of interviewing techniques is vast and has many nuances, but law enforcement professionals agree that it is the result of long hours of surveillance and investigation backed with a careful plan and substantial legal advice.[10] Rarely did the interview alone result in a confession that triggered Horton Clause negotiations, as in the case of deserter spies such as Slavens and Weinmann. Beyond traditional criminal interview techniques, this study suggests that a successful espionage case interview requires extensive understanding of classifications, adversary espionage tradecraft, the espionage statute, and other intelligence information. For example, in 1944 the FBI used the traditional criminal interview technique of rapport-building, eyewitness disclosures, and an FBI agent's knowledge of the German *Abwehr*'s use of the headache medication Pyramidon to enable the interviewer to successfully convince Othmer to confess. This study suggests that a solid basis in both criminal investigations and adversary espionage techniques were required for successful interviews by naval counterintelligence.

[10] James Orlando, "Interrogation Techniques," Connecticut General Assembly, Office of Legislative Research, 2014.

- **Undercover operations.** The third most critical investigative capability was undercover operations. Approximately one-sixth of the investigations of espionage subjects considered in this study were resolved using an undercover agent posing as a buyer. In some cases, the undercover agent posed as a foreign intelligence officer, while in other cases they posed as a civilian purchaser. The FBI led most of these cases, some with no involvement by NIS in the early 1980s. However, by the late 1980s, NIS successfully led several undercover espionage response operations.
- **Other criminal investigation techniques.** In addition to surveillance, interview techniques, and undercover operations, a host of traditional criminal investigation techniques used every day to solve crimes can be critical to proving espionage. For example, fingerprints were key to exposing Morison in 1983 and Garcia in 1985. A mundane trash cover yielded a torn-up PLA military intelligence tasking list during the Mak investigation in 2005. A mail cover revealed Downing's connection to Spanish naval intelligence in 1898 and Kim's connection to South Korean naval intelligence nearly a century later. Finally, in the post-Cold War era, investigators used digital evidence to prove Abu-Jihaad's duplicity in 2001. This study strongly indicates that counterespionage was, at its heart, a law enforcement function because to ensure that the *advantage* that an adversary gains through espionage in *not unexpected*, the DON must be able to bring the full weight of the law down on a suspect through use of the Horton Clause.

Military Effectiveness

This study suggests that the strategic basis of naval counterintelligence should be based on a modified definition of counterintelligence that is based on the nine principles of war which could be worded as: "Activ-

ities conducted to ensure that information obtained by an adversary does *not* result in an *unexpected advantage*."[11]

However, throughout its history, U.S. naval counterintelligence was often militarily ineffective because it failed to achieve that basic strategic definition of counterintelligence or because the intervention came too late to be militarily effective.

Overall, two-thirds of the investigations of the espionage subjects considered in this study were militarily effective, leaving a full one-third militarily ineffective. This tentatively suggests that in one-third of all espionage cases, the DON's adversaries held an *unexpected advantage* and could have achieved the eighth principle of war—surprise. Moreover, two of the militarily ineffective cases were quite serious: Yoshikawa and Walker. Further, the DON never fully understood the advantage gained by the Soviets in both the Drummond and Souther cases.

That said, those cases all occurred before the watershed event in U.S. naval counterintelligence history: the 1982 Horton case. With two new laws, the Foreign Intelligence Surveillance Act and the Classified Information Procedures Act, in place, the civilian and military justice system could introduce plea agreements and the opportunity for suspects to reduce their sentences through a full confession backed by a successful polygraph. Of the militarily ineffective espionage cases considered in this study, fewer than one-fifth took place after the introduction of the Horton Clause in 1982. Effective criminal investigation and prosecution of espionage, along with the Horton Clause, ensured that the DON rarely became the victim of an adversary's *unexpected advantage* once naval counterintelligence learned of a spy in its ranks.

[11] *Naval Warfare*, Naval Doctrine Publication 1 (Norfolk, VA: Naval Warfare Development Center, 2020), 57; and *Counterintelligence*, Secretary of the Navy Instruction 3850.2E (Washington, DC: Department of the Navy, January 2017), Encl. 2, 1.

A Century of Lessons Learned

For the DON and its naval counterintelligence practitioners, strategically significant espionage was a low-probability, potentially high-impact proposition that required eternal vigilance in the face of seemingly endless low-value, petty national security cases. The cases considered in this study suggest that financial rewards were the most frequent, but not sole, incentive for the DON's espionage suspects. Despite the department's best efforts to provide good pay and support for its servicemembers, a few of these suspects persisted, found holes in security, and attempted to evade counterintelligence. They often sought the nearest foreign establishment that they believed would pay and made a ham-fisted approach or fell victim to the enticement of a duplicitous associate. Often, a variety of means detected that approach or relationship. For the few that slipped through, U.S. and allied intelligence, facilitated by solid interagency ties, often discovered clues to their identity, and an ensuing intensive investigation cornered them. Facing long prison terms, each of these suspects agreed to a plea bargain, offering a full accounting of their crimes in exchange for leniency. The Horton Clause provides a militarily effective conclusion that leaves no room for an *unexpected advantage* by an adversary.

Given the broad swath of history included in this study, these naval espionage case trends can appear to be a jumble of facts, interesting anecdotes, and minute details that had no bearing on DON-wide counterintelligence operational prioritization. However, the results of this study can be categorized into a set of enduring truths. Based on the cases considered in this study:

- Counterintelligence was fundamentally a law enforcement activity. Per the Horton Clause, to be militarily effective, a reduced sentence in exchange for a full confession backed by a successful polygraph was the only way to ensure that the adversary has not acquired an *unexpected advantage* from an insider's espionage.

- Counterintelligence was also fundamentally an intelligence activity. Naval counterintelligence straddled both professions—law enforcement and intelligence—mutually deriving benefit from both and feeding both simultaneously.
- Financial and ideological concerns often influenced insider threats. A correlation appears to support the theory that efforts by the DON to increase recruitment and retention through better pay and increased personnel support may have had a magnified effect on reducing espionage by insiders.
- Despite the low probability of campaign-altering espionage, the DON should have maintained a robust, credible counterintelligence investigative capability, particularly in the face of capable foreign intelligence adversaries.
- Maintaining a robust, credible counterintelligence investigative capability was expensive. Effective counterintelligence personnel must be well trained and experienced in both law enforcement and intelligence to be effective. Effective counterintelligence was also labor intensive. Based on the cases considered in this study, investigators and surveillance assets sometimes spent months on a single investigation, with little or no results.

Following these five basic truths would have ensured an adequate DON response to allegations of espionage and its ability to leverage the law to ensure a militarily effective solution that guaranteed that an adversary's advantage gained was *not unexpected*. However, apathy, budgetary constraints, competing priorities, and unexpected events challenged the ability of the DON to adequately fund its naval counterintelligence force. Those challenges meant that the department needed to prioritize its counterintelligence efforts. However, with dozens or even hundreds of disparate stakeholders each seeking counterintelligence support, the DON did not develop an objective measure of relative criticality to its warfighting mission to establish priorities.

Only by settling on an objective, predictive measure of relative espionage impact could the DON have arrived at a flexible, enduring naval counterintelligence operational prioritization that effectively deployed its counterintelligence capability in support of its most critical capabilities and against the most potentially dangerous adversaries. A close examination of naval warfare fundamentals, history, and espionage pointed toward a prioritization that is enduring because that prioritization, and the resulting operational priorities, was not focused on an adversary but rather was focused on the DON's core mission: fighting and winning at sea.

Chapter 7
Toward a Lasting Naval Counterintelligence Operational Prioritization

Built on the solid foundation of Cold War naval counterintelligence, as of 2010, the U.S. Department of the Navy (DON) appeared to have been safer from insider espionage than at any other time in its history. A review of the espionage cases considered in this study suggests that for 24 years, the department had not experienced any espionage cases in which an active duty or civilian member compromised classified information to an adversary intelligence service without a full reckoning of the damage done.

However, the DON experienced two quite serious episodes of espionage during the period covered in this study, 1898–2010. The first was in 1941, when a dedicated Japanese espionage campaign facilitated the surprise attack on Pearl Harbor, Hawaii. Only the failure of the Imperial Japanese Navy to heed the resulting intelligence saved the U.S. Navy's Pacific Fleet from a crippling blow. The second serious episode was during the Cold War, when the Soviets compromised U.S. naval command and control for 15 years with serious implications for the submarine-launched ballistic missile component of the U.S. nuclear triad.

A third serious episode, unrelated to insider espionage, may have begun to unfold as the period of this study ended. A persistent and widespread cyber espionage campaign conducted by the People's Re-

public of China (PRC) compromised the sensitive but unclassified designs of dozens of U.S. weapons systems and may have saved the People's Liberation Army (PLA) billions in research and development costs and accelerated their modernization efforts.[1] The PRC cyber effort succeeded largely because it targeted information that did not trigger the Espionage Act and did not involve a recruited spy. While their actions were a violation of the 1986 Computer Fraud and Abuse Act, the United States did not use the law against PRC cyber actors until 2014, a decade after the first intrusion into U.S. military systems.[2] By then, an ecosystem of cyber espionage had begun to form in the PRC that no United States-based law could stop.[3] As in 1913 with the USS *Pennsylvania* (BB 38) case, in 2010 the DON's sensitive technical information was left relatively unsecure.

The DON's failure to predict how strategic shifts would change an adversary's posture and then to adequately forecast how its own new position would influence the espionage threat aggravated all three of these serious episodes.

- In 1941, the DON dismissed the concept of a Japanese attack as an irrational act and as a result failed to devote the necessary resources to counterintelligence efforts in the Hawaiian territory.[4]
- During the Cold War, the DON failed to recognized that U.S. submarine-launched intercontinental ballistic missiles would dramatically shift Soviet intelligence targeting, while simultaneously U.S. naval counterintelligence overrelied on background investigations despite a fundamental change in Soviet espionage

[1] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, 27 May 2013.
[2] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, 19 May 2014.
[3] Nicole Perlroth, "How China Transformed into a Prime Cyber Threat to the U.S.," *New York Times*, 19 July 2021.
[4] Elliot Carlson, *Joe Rochefort's War: The Odyssey of the Codebreaker Who Outwitted Yamamoto at Midway* (Annapolis, MD: Naval Institute Press, 2011), 69, 79.

tactics in the early 1960s from ideological to financial incentives.[5] In 1961, the DON was warned of this shift by the Drummond case, and in 1968 the department received 55 copies of a Soviet Committee for State Security (KGB) manual confirming the shift. In 1972, more than a decade after the first ballistic missile submarine (SSBN) deployed to Holy Loch in Scotland, the DON changed its tactics against Soviet espionage by shedding the background investigation mission. But this came too late, as Walker had already slipped through.[6]

- In the 2000s, the DON underestimated the intent and size of the PLA Navy's expansion plans while also overlooking the security of the internet-connected information systems of its contractors despite evidence of a PRC shift to cyber espionage.[7]

This combination of failures to accurately predict the counterintelligence implications of strategic shifts in the political-military situation resulted in serious implications for the DON three times. Without recognition of the challenge, it may happen again.

[5] *Naval Investigative Service Activities Report, 1966* (Washington, DC: Naval Investigative Service, 1967), C-3; John Barron, *KGB: The Secret Work of Soviet Secret Agents* (New York: Bantam Books, 1974), 472; and "Proposed Transmittal of KGB Training Manual," Central Intelligence Agency, 14 February 1968.

[6] H. Paul Mullis, ed., "A Brief History of the Naval Criminal Investigative Service," Naval Investigative Service Command History Project, 1997; "KGB Training Manual on Operations against Americans," Central Intelligence Agency, 5 June 1968; and "Deck Log Book, USS *Patrick Henry* (SSBN 599), 1–31 March 1961," Record Group 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: Patrick Henry (SSBN-599)–March 1961, NAID: 218495306, National Archives and Records Administration, College Park, MD, 20.

[7] *Military Power of the People's Republic of China, 2009: Annual Report to Congress* (Washington, DC: Department of Defense, 2009), 52.

Prioritizing Counterintelligence within the Department of the Navy

While the nine principles of war are silent about counterintelligence, together the principles of surprise and security sum up the problem well:

- **Surprise.** Strike the enemy at a time or place or in a manner for which they are unprepared.
- **Security.** Never permit the enemy to acquire unexpected advantage.

Together these two principles maintain that the DON must ensure that adversaries do not achieve surprise by maintaining its own security. The counterintelligence implication within the principle of surprise was that the adversary must fail to achieve surprise because their advantage was known and not unexpected. The key words in these two principles are *unexpected advantage*. Those two words form the basis of a postulated naval counterintelligence mission: "Activities conducted to ensure that information obtained by an adversary does *not* result in an *unexpected advantage*."

For much of the period covered in this study, U.S. naval counterintelligence struggled to ensure that the DON was aware of any adversary advantage gained through espionage and that it was *not unexpected*. They did not appreciate that the basic mission of naval counterintelligence could have been summed up as efforts to ensure that adversaries do not acquire *unexpected time, place, or manner advantages* through espionage.

In the broadest sense, naval espionage often centered on innovations in weapons technology matched with the resulting innovations in tactics to employ those weapons. Those innovations are *manner advantages*—in other words, how the force fights. At least four times

during the period covered in this study, the DON was surprised by adversary espionage that targeted a seminal naval warfare shift.

- In the early 1900s, the DON transitioned from a consumer of foreign technology to a victim of technology theft as it created better battleships, thought to be the great naval shift of the period. Despite several espionage cases, only World War I forced the DON to finally create a counterintelligence service.[8] However, in 1923 the director of the Office of Naval Intelligence (ONI) even admitted how poorly ONI performed during World War I while also admitting that naval counterintelligence was being mothballed. He noted in a speech,

> The functions of the Office of Naval Intelligence are frequently misunderstood. During the war we necessarily had thousands of agents whose business was to guard against spies and traitors. This was a war condition under which the just suffered with the unjust, for of course *many ludicrous mistakes were made by amateur agents*. But now in peace time all that work in the United States is handled by the Department of Justice. If we have information of activities against the government we hand it over to Justice. What men we employ occasionally in this country are solely for the purpose of naval administration.[9]

[8] Capt Wyman H. Packard, USN (Ret), *A Century of U.S. Naval Intelligence* (Washington, DC: Department of the Navy, 1996), 252–53.

[9] Capt Luke McNamee, USN, "Naval Intelligence," U.S. Naval Institute *Proceedings* 50, no. 9 (September 1924). This quote is part of a lecture delivered by Capt McNamee, director of naval intelligence, aboard USS *Henderson* (AP 1) at the Washington Navy Yard on 9 March 1923.

- In the 1930s, the DON was clear-eyed about the military threat posed to the United States by Japan but failed for a decade to adequately resource its fledgling counterintelligence service. As a result, prior to World War II, the Japanese successfully gathered intelligence about newly developed naval aviation capabilities and actionable intelligence about the disposition of U.S. forces in Hawaii, resulting in a serious *unexpected time and place advantage*.
- In the 1960s, as the DON innovated the first SSBNs and became a direct nuclear threat to the Soviet Union, naval counterintelligence remained relegated to conducting background investigations. Despite clear indications from the 1967 Ledbetter case that Soviet intelligence was focused on SSBNs and solid information in 1961 from the Drummond case and a 1968 KGB manual that the Soviets had shifted tactics to accept financial volunteers, U.S. naval counterintelligence does not appear to have reacted in time, and Walker slipped through to compromise U.S. naval command and control for the next 15 years, again resulting in myriad *unexpected time, place, and manner advantages*.
- In the early 2000s, as the DON rapidly expanded its use of internet-based services, U.S. naval counterintelligence kept pace, forming the Naval Criminal Investigative Service (NCIS) Computer Investigations and Operations Department in 1997.[10] The first PRC breach of a U.S. Navy information system occurred six years later.[11] Despite NCIS prescience and evidence of the PRC's intent, the DON struggled to secure its computer systems, par-

[10] L. Lanark Lockard, "Rapid Evolution of Information Technology Poses New Problems for Law Enforcement and Security," *U.S. Naval Criminal Investigative Service Bulletin* 2, no. 7 (December 1998): 2.

[11] Dorothy Denning, "Cyberwar: How Chinese Hackers became a Major Threat to the U.S.," *Newsweek*, 5 October 2017; Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, 25 August 2005; and Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)," *Time*, 5 September 2005.

ticularly at defense contractors, and the thefts continued, eclipsing all previous espionage efforts to steal the U.S. Navy's sensitive unclassified information and possibly helping to close the gap on several of the DON's *manner advantages* over the PLA Navy.[12]

Each of these incidents represented a strategic counterintelligence failure by the DON because it failed to grasp the counterintelligence implications of its shifts and the corresponding shift in adversary espionage. Each time, an adversary was able to collect significant quantities of data long before the DON acted to adequately secure the information. While the DON often leads the world in naval warfare, this inability to consider the security and counterintelligence implications of these strategic shifts cost billions and courted misfortune several times. Unless the DON addresses this inability, it will continue to encounter such misfortunes.

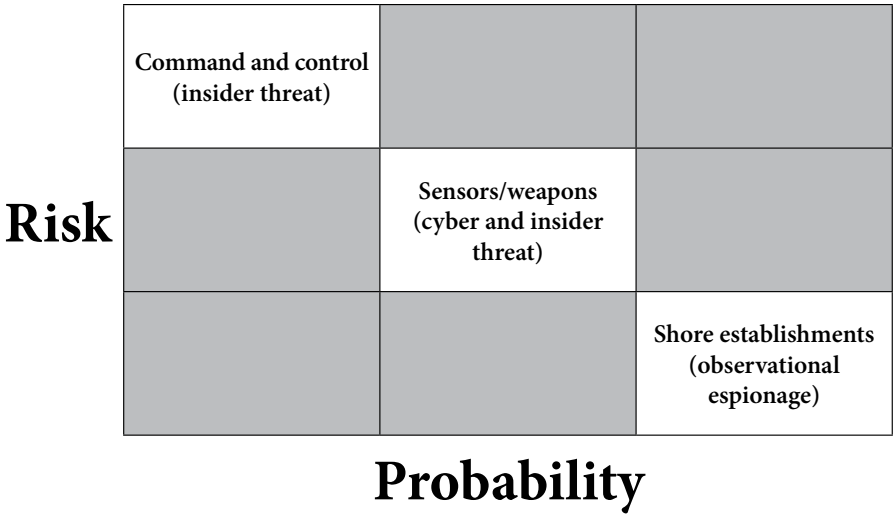
To meet the strategic imperatives of the future, as the U.S. Navy and Marine Corps move into their next chapter—great power competition—all facets of the DON including naval counterintelligence should consider the missed strategic shifts of the past, identify similar queues occurring today, and drive the changes that will ensure that adversaries of the United States do not *unexpectedly acquire time, place, and manner advantages*.

Strategic Queues of the Future

Based on the impact of the cases considered in this study on naval operations, the three basic elements of naval warfare can be arranged according to probability, risk, and likely type of espionage as in the following chart.

[12] Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, 8 June 2018.

Figure 75. U.S. Department of the Navy future espionage probability/risk matrix



Source: Courtesy of the author, adapted by MCUP.

Command and Control

As Schmidt was for the German *Kriegsmarine* in World War II, Walker was the most damaging U.S. Navy case because for 15 years he compromised the Service's *command-and-control system* (both cryptographic machines and codes) vice just individual documents. While future cases that involve the *entire system* are low-probability, high-impact events, naval counterintelligence must be poised to detect and neutralize them. The Schmidt and Walker cases highlight that to compromise the modern cryptographic systems, an adversary needs two things: the machine and the codes that make them work.

A more modern example of this was the Edison Kuok case. U.S. Immigration and Customs Enforcement arrested Kuok in 2009 for attempting purchase a KG-175 TACLANE, which secures data transmissions. Kuok was specifically interested in buying the device "if it came with a particular key" and admitted that he was working on behalf

of the PRC's signals intelligence agency.[13] Like Schmidt and Walker, Kuok was attempting to compromise both the machine and the codes. No matter who the adversary and what the naval innovation of the period, another command-and-control case would be equally as serious due to the *unexpected time, place, and manner advantages* such espionage provides.

For the future, the trend analysis from this study suggests that just as in the Cold War, despite a constant trickle of petty espionage, the type of espionage case with the lowest probability of occurrence but the highest strategic impact would be another Schmidt or Walker—a person who provides systemic access to classified information vice only the classified information that they themselves can directly acquire. As in the 1940s and the 1960s, an adversary could only achieve that type of systemic access to classified information through compromise of the means by which U.S. command-and-control systems are secured.

The arrest of Kuok in 2009 revealed that PLA signals intelligence had been seeking U.S. cryptographic machines since at least 1999. When U.S. authorities arrested him in 2009, Kuok was attempting purchase both a KG-175 TACLANE and its key codes. Similarly, during the Cold War the Soviets obtained the machines from the North Korean capture of a U.S. Navy ship while Walker provided the key codes.[14]

The most potentially damaging future espionage for the U.S. Navy would be a modern version of the Walker case combined with a more

[13] Kevin Poulsen, "Chinese Spying Claimed in Purchases of NSA Crypto Gear," *Wired*, 9 July 2009; and Greg Moran, "Chinese Man Gets 8 Years in Spy Case," *San Diego (CA) Union-Tribune*, 12 September 2010.

[14] Robert E. Newton, *The Capture of the USS* Pueblo *and Its Effect on SIGINT Operations* (Fort Meade, MD: National Security Agency Center for Cryptologic History, 1992), 167. This report, declassified in 2023, describes the effect of the Walker compromises on U.S. communications and signals intelligence operations. See also Maj Laura J. Heath, USA, "An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967–1974, as Exploited by CWO John Walker" (thesis, US Army Command and General Staff College, 2005), 53–55.

successful version of the Kuok case because it will provide *unexpected time, place, and manner advantages*.

Sensors and Weapons

With the exception of the Walker case, all of the espionage cases considered in this study combined do not amount to a fraction of the sensitive technical information stolen from the DON through PRC computer intrusions. Mak was a pioneer in bulk theft of the DON's sensitive technical information, but government-sponsored PRC cyber theft was a quantum leap which may have *unexpectedly closing the gap on several manner advantages*.[15]

Through sheer volume, the PRC appears to have raised the theft of sensitive technical information from a strategically insignificant minor espionage case such as Farnsworth into a Walker-like broad swath of damaging compromises.

Mak represented the "old school" PRC effort to steal ship design and systems information. By the time of his arrest, he was printing digital documents and then scanning them back into digital form to be couriered back to the PRC on a disk. The entire operation was slow and risky. The PLA found a better way—to steal the original digital document.

However, even before the Federal Bureau of Investigation (FBI) and NCIS arrested Mak, the first publicly acknowledged PLA cyber theft of sensitive but unclassified information occurred in 2003. Within 10 years, the PLA had compromised all or significant parts of the Aegis ballistic-missile defense system, the McDonnell Douglas F/A-18 Hornet fighter, the Bell Boeing V-22 Osprey tiltrotor aircraft, the littoral combat ship, and the Lockheed Martin F-35 Lightning II Joint

[15] Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies."

Strike Fighter.[16] No adversary in history has stolen as much U.S. Navy technical information as the PLA.

Worryingly, the "Kotani-shift," described in chapter 2, from technology theft to operational intelligence collection in preparation for war that was seen before World War II may already be occurring with the PLA.[17] The last acknowledged PLA cyber theft of DON technology was in 2018, but in 2023 the United States reportedly discovered malicious software within U.S. military affiliated information systems that "could give China the power to interrupt or slow American military deployments or resupply operations by cutting off power, water and communications to U.S. military bases" including the DON's facilities in Guam.[18] Whether or not these events reflect the Kotani-shift remains to be seen.

Other than the low-probability, high-impact Walker case, the most damaging espionage for the DON was the repeated instances of compromise of ship designs and shipboard systems. In the 1930s, Farnsworth and possibly Danielsen and Guellich compromised new ship designs, and during the early Cold War Drummond compromised a wide range of ships' electronic systems. Those cases likely provided the United States' adversaries a degree of *unexpected manner advantages*, but none of them appeared to have had a significant impact on the DON's mission.

[16] Denning, "Cyberwar"; Thornburgh, "Inside the Chinese Hack Attack"; Thornburgh, "The Invasion of the Chinese Cyberspies"; and Nakashima and Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare."
[17] Ken Kotani, *Japanese Intelligence in World War II* (New York: Osprey, 2009), 79–86.
[18] David Sanger and Julian Barnes, "U.S. Hunts Chinese Malware that Could Disrupt American Military Operations," *New York Times*, 29 July 2023; and Pukhraj Singh, "Recent Chinese Cyber Intrusions Signal a Strategic Shift," *Strategist*, Australian Strategic Policy Institute, 5 July 2023.

Shore Establishments

Approximately one-sixth of the espionage subjects considered in this study involved observational espionage of shore establishments. Most of these cases occurred in the period just prior to or at the beginning of World War II. The advent of satellite imagery would appear to have rendered these operations obsolete, but the Soviets and Cubans maintained the practice with Dorschel in Scotland in the 1960s and Guerrero in Key West, Florida, in the 1990s. Even Kunkle volunteered to conduct observational espionage in Norfolk, Virginia, in the 1980s.

What all these observational espionage missions had in common was that they were tethered to some form of secure communications. Kuehn and Yoshikawa were tethered to the secure communications of the Japanese consulate in Honolulu, Hawaii, while Othmer, Dickinson, and Dorschel were tethered to coded letters sent to overseas accommodation addresses. In contrast, in the 1990s Guerrero relied on his Miami-based handler's clandestine radio communications with Havana. The requirement to use secure communications limited the utility of all these observational espionage operations because the requirement for secure communications created a single point of failure. For example, Yoshikawa could have been unmasked if the FBI and ONI had surveilled him doggedly. Othmer, Dickinson, and Dorschel's coded letters were a slow process and subject to intercept. In Guerrero's case, a single radio operator, once detected, could have snared the entire network, as happened with the Duquesne Spy Ring in New York in the 1940s.

However, since Guerrero's arrest in 1998, the world has experienced a communications revolution with the widespread use of smart mobile telephones and encrypted communications applications. As of 2022, approximately 8 billion people carried a secure communica-

tions, photography, and mapping device in their pocket.[19] The result is that in an operational mobile telephone network combat environment, the observational espionage threat is manifestly more challenging for naval counterintelligence and dangerous for operational forces.

Focused primarily on the PRC and Russia, in 2022 the *Chief of Naval Operations Navigation Plan* emphasized the concept of counter-C5ISRT (command, control, computing, communications, cyber, intelligence, surveillance, reconnaissance, and targeting) as a key warfighting capability being developed to support naval units operating inside adversary weapons engagement zones, focusing on full-spectrum sensing and signature management.[20] Explanations of counter-C5ISRT tend to emphasize signals and data, but with the rapid shift of tactical and operational espionage from bulky radio sets or slow moving letters to highly portable, instantaneous, and ubiquitous mobile telephones, one end of that full-spectrum sensing is now simply handheld photography accompanied by text and marked maps transmitted by observational espionage assets. The first concrete example of this phenomenon in action began in Ukraine in 2022, where locally recruited pro-Russian observational espionage assets hunted Ukrainian antiship missile systems and collected bomb damage assessment information, reporting their results over encrypted mobile telephone applications.[21] With the advent of ubiquitous mobile secure communications, observational espionage of shore establishments,

[19] Felix Richter, "Charted: There Are More Mobile Phones than People in the World," World Economic Forum, 11 April 2023.
[20] Adm Michael M. Gilday, USN, *Chief of Naval Operations Navigation Plan, 2022* (Washington, DC: Department of the Navy, 2022), 19.
[21] "The SBU Detained an Enemy Agent Who Was Collecting Intelligence for Missile Strikes on Odesa," Security Service of Ukraine, 4 July 2022; "The SBU Reported Suspicion to One of the Managers of Russia Today and Detained the Adjuster of the Missile Attacks in Odesa (Video)," Security Service of Ukraine, 18 June 2022; and "The SBU Detained a Russian Agent in Odesa Who Was Scouting the Positions of Anti-ship Systems of the Armed Forces of Ukraine (Video)," Security Service of Ukraine, 11 July 2022.

even expeditionary shore establishments, will almost certainly emerge as a critical warfighting issue for naval counterintelligence.

Naval Counterintelligence Operational Prioritization

This survey of historical espionage trends that have affected the DON suggests that an overarching counterintelligence operational prioritization is necessary to avoid a repetition of the strategic surprises of the past. The foundation of any operational prioritization should be a mission statement. As described several times in the preceding pages, for naval counterintelligence, this study suggests that the mission is: To ensure that information obtained by an adversary does *not* result in an *unexpected advantage*.

With that mission in mind, naval counterintelligence should prepare for shifts in the adversary's espionage by continuously identifying and adapting to two main foci:

- Shifts in adversary espionage in response to shifts in U.S. naval strategy and tactics. Examples include the introduction of hypersonic missiles into naval arsenals around the globe or the creation of coastal antiship missile units such as the U.S. Marine littoral regiment.[22]
- Strategic shifts in adversary espionage doctrine. For example, the new Russian reliance on encrypted mobile telephone applications may be an espionage doctrine shift. Or, in theory, PRC in-

[22] Tomasz Grotnik, "Russia Doubles down on Frigates with Tsirkon Hypersonic Missiles," *Naval News*, 15 December 2023; Tanmay Kadam, "Russia Says Zircon Hypersonic Missiles Can Now Be Fired from Mobile Launchers; Developer Says 'Intensifying Work'," *Eurasian Times*, 18 December 2023; "The China Threat," *Air and Space Forces Magazine*, 31 August 2023; Andrew Feickert, *U.S. Marine Corps Force Design 2030 Initiative: Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2023); and Col T. X. Hammes, USMC (Ret), "Adapt Marine Littoral Regiments for the Surveillance Era," U.S. Naval Institute *Proceedings* 148, no. 11 (November 2022).

telligence could someday capitalize on financial volunteers such as the 2010 Martin case.

The potential interplay between a naval innovation such as distributed maritime operations (DMO) and an adversary espionage shift such as the employment of encrypted mobile telephone applications in observational espionage operations, and their potential employment by adversary intelligence assets to find and fix U.S. coastal defense units, can serve as an example of how the DON must continuously recognize and adapt its naval counterintelligence to naval innovations and espionage shifts.

In response to the growth of the antiaccess/area-denial (A2/AD) capabilities of several adversaries, the DON innovated a response, DMO. In 2022, a microcosm of the DMO concept played out around Ukraine's Snake Island in the war between Russia and Ukraine. That ongoing conflict provides a good example of how naval counterintelligence operational priorities could help the DON ensure that an innovation does not result in surprise because of espionage.

Broadly speaking, the DMO concept involves "small, dispersed land and sea detachments [that] threaten the ability of adversary forces to concentrate from within their anti-access/area denial umbrella."[23] The concept pits small detachments of friendly forces armed with long-range missiles against larger, conventional, and similarly armed adversary forces with the net effect intended to deny the adversary the benefit of their A2/AD umbrella.

Richard Mosier, writing for the Center for International Maritime Security, summed up DMO as "based on three bedrock tenets: the distributed force must be hard-to-find, hard-to-kill, and lethal." *Hard-to-find* refers to one of the nine principles of war, surprise, the aim of which is to achieve a *time and place advantage* over an adver-

[23] "Distributed Maritime Operations (DMO)," U.S. Marine Corps, 2 August 2021.

sary. Mosier's article went on to describe how a U.S. force could deny an adversary that *time and place advantage*.[24] His analysis included many forms of adversary sensors including visual. However, his descriptions were largely technical and did not address observational espionage.

While observational espionage may seem benign, Yoshikawa in Hawaii in 1941 and the U.S. Navy in Korea in 1950 demonstrated that observational espionage can be campaign-altering.[25] Moreover, during World War II, Australia and New Zealand organized an extensive observational espionage agent network across Melanesia and Polynesia to report on Japanese military movements. Based on the Australian Coast Watching Service, first organized in 1919 and run by the Royal Australian Navy's Intelligence Division, the organization fielded hundreds of observational espionage assets, mostly Australians and New Zealanders and local inhabitants who remained loyal to the British crown. These Australian and New Zealand officers, who could not blend in with the local population, relied on local loyalists and stealth to radio observations of enemy activity to decision makers.[26] During the Solomon Islands campaign in 1942–44, the coastwatchers usually provided the 40-minute forewarning of the approach of Japanese aircraft required to scramble U.S. naval aviation assets based ashore.[27] Twenty years in the making, the Coastwatching Service proved its value during the Solomon Islands campaign by providing repeated warnings of Japanese movements that accorded the Allies campaign-altering *unexpected time and place advantages*.

[24] Richard Mosier, "Distributed Maritime Operations—Becoming Hard-to-Find," Center for International Maritime Security, 12 May 2022.
[25] See Inchon, South Korea, 1950, in appendix E for details.
[26] Capt Michael Van Liew, USMC, "The Coastwatchers: Intelligence Lessons Learned for the Future Single Naval Battle," Center for International Maritime Security, 31 March 2021; and Mackenzie J. Gregory, "Coastwatching in the Pacific—Solomon Islands," *Naval Historical Review* (April 1993).
[27] James D. Hornfischer, *Neptune's Inferno: The U.S. Navy at Guadalcanal* (New York: Bantam Books, 2011), 124.

Adversary intelligence services are embracing the rapid advances in telecommunications technology, resulting in a strategic shift in adversary tactical espionage doctrine that could challenge some aspects of DMO. As previously mentioned, observational espionage requires rapid, secure communications. Yoshikawa in 1941 was tethered to the Japanese consulate in Hawaii; the Coastwatching Service in 1942–44 was tethered to bulky radio sets; and Guerrero in Key West in 1998 was tethered to his Miami-based case officer, whose clandestine encrypted radio communications passed information to Havana.[28] However, the rapid advances in mobile communications during the past 20 years changed that paradigm. Nearly every human on the planet now has direct access to encrypted long distance communications. The Russo-Ukrainian War illustrates how adapting a technological advance can dramatically shift espionage doctrine. Near Odesa in Ukraine, two observational espionage Russian assets provided BDA for attacks on a bridge over a tidal inlet, and the Russian Federal Security Service tasked another with creating an agent network to detect antiship missile systems along the Black Sea coast. All three Russian intelligence assets appear to have used encrypted messaging applications on mobile telephones.[29] The effectiveness of this shift in espionage doctrine is uncertain, but the Russian "coastwatcher operation" is an example of an emerging adversary espionage doctrine shift that, if left unaddressed, could result in campaign-altering *unexpected time and place advantages*. In the words of the commanding general of the

[28] "Five Cubans Convicted of Espionage for Castro," *Tampa Bay (FL) Times*, 9 June 2001.
[29] "The SBU Detained an Enemy Agent Who Was Collecting Intelligence for Missile Strikes on Odesa"; "The SBU Reported Suspicion to One of the Managers of Russia Today and Detained the Adjuster of the Missile Attacks in Odesa (Video)"; and "The SBU Detained a Russian Agent in Odesa Who Was Scouting the Positions of Anti-ship Systems of the Armed Forces of Ukraine (Video)."

U.S. Army's National Training Center in January 2024, "This device [mobile telephone] is going to get our soldiers killed."[30]

Given the potential for a long-term adversary effort to challenge DMO by building tactical observational espionage agent networks in potentially contested littorals, an enduring, forward-looking, and comprehensive naval counterintelligence operational prioritization should trigger an examination of those shifts to adjust force structure, force posture, and information gathering activities to meet the challenge. As with the U.S. Pacific Fleet's move to Pearl Harbor in 1940, the introduction of SSBNs to the United States' nuclear triad in 1960, and the shift to networked information systems in the 2000s, failure to both appreciate the impact of a major shift or innovation on an adversary and anticipate their espionage response can result in serious implications.

Into the Future from Shades of the Past

For naval counterintelligence, technology left the DON in nearly the identical position it was in almost a century ago. In both the 1930s and the 2020s, the department faced an expanding, potentially powerful naval adversary in Asia and a largely landlocked but belligerent adversary in Europe. To face the threat in the 1930s, the department rapidly innovated but, as happened with the *Pennsylvania* plans in 1913, the Farnsworth case in the 1930s, the Drummond case in the 1960s, and the Mak case in 1980s and 1990s, the apparently suboptimal security of the department and its contractors did not stop a steady leak of sensitive technical information. Simply moving the volume of paper limited the damage of past cases. With advent of digital espionage, the

[30] Alex Horton, "What the Pentagon Has Learned from Two Years of War in Ukraine," *Washington Post*, 22 February 2024.

leaks are not physical but virtual, and their sheer volume alone may strategically challenge the DON's ability to maintain a technical edge.

At the same time, tactically, mobile encrypted communications technology expanded the observational espionage threat far beyond anything Yoshikawa, Othmer, or Dickinson in the 1940s, Dorschel in the 1960s, or Guerrero in the 1990s could have hoped for. The exploits of Russian intelligence along the Black Sea coast in 2022 are only just becoming known and may become a pattern for future adversaries. If deftly deployed by an adversary but poorly contested by naval counterintelligence, tactical observational espionage in the littorals could also pose a campaign-altering challenge for the DON and challenge a DMO-based campaign.

Finally, lurking behind both of those challenges is another Walker case—low-probability, high-impact espionage-enabled signals intelligence that compromises the DON's command-and-control system. Bookended by the 1915 USS *Hull* (DD 7) case and the 2009 Kuok case, the adversaries in all three cases aimed to compromise the DON's command and control. These three cases demonstrate that adversaries of the United States have consistently attempted to steal the equipment and/or the coding material used to secure the DON's command and control and suggest that they will continue to do so into the future. As happened to both the Germans and Japanese during World War II, and as could have theoretically happened to the United States during the Cold War, this type of compromise was unreservedly strategic and campaign altering. However, because the full scope of the espionage that led to the German and Japanese naval catastrophes during World War II took decades to reveal itself, espionage involving encrypted communications requires a long-term, persistent counterintelligence effort to neutralize.

Given the mission of ensuring that information obtained by an adversary does not result in an unexpected advantage and a flexible, enduring, and predictive operational prioritization that recognizes the

impact of major naval innovations on an adversary and anticipates their espionage response, a final naval counterintelligence prioritization should be based on the elements of naval warfare and how an unexpected adversary advantage in each of those elements affected the warfighting capacity of the DON in the past. The review of those factors in the preceding chapters suggests the following priorities:

1. Espionage involving command and control.
2. Espionage involving sensors and weapons.
3. Observational espionage of shore establishments.

A reactive operational prioritization that treats each aspect of naval warfare equally, as was apparently often employed by the DON, repeatedly resulted in surprise. To ensure that campaign-altering espionage does not occur in a future conflict, the DON should prioritize the activities of its counterintelligence assets. Command-and-control espionage, left unchecked, repeatedly resulted in several lost U.S., Japanese, and German naval campaigns from the American Civil War through World War II and theoretically the Cold War.[31] Moreover, readers will recall that the full fruits of espionage-enabled signals intelligence took decades to become apparent, long after serious damage occurred. This type of espionage was a low-probability but high-impact form of espionage. Maintaining a focus on command-and-control espionage is a major reason for implementing an enduring naval counterintelligence operational prioritization because institutionally it is easy to lose focus when these critical command-and-control espionage cases are separated by decades of unrelated petty espionage.

Engagement-altering espionage resulting from sensor and weapons espionage was a secondary concern because the DON generally recovered and rectified its effects through technology and tactics before combat began or soon after the vulnerability became apparent.

[31] See Charleston, 1863; New York, 1923; and Berlin, 1931, in appendix E.

Finally, observational espionage of specific shore establishments should be a tertiary concern because its effects were generally tactical and operational commanders should have assumed it was occurring. However, the DON should continue to strive to be prepared to neutralize tactical observational espionage wherever and whenever possible because the introduction of encrypted mobile telephone communications applications is shifting adversary espionage doctrine in ways just beginning to be ascertained. Moreover, some tactical situations can suddenly emerge as strategic concerns. The Japanese attack on Pearl Harbor in 1941 and the Russian attack on a key coastal bridge in Ukraine in 2022 are pointed examples of tactical observational espionage with potential strategic impact.

This data-driven analytic study forms the basis for a flexible, enduring, and predictive counterintelligence operational prioritization that is focused on averting campaign-altering surprise by anticipating adversary intelligence reactions and designating priorities based on naval warfighting fundamentals with a clear-eyed view of the threat. The historical perspective and lessons learned offered by the 57 DON espionage cases analyzed in this study suggests that establishing such operational priorities is an imperative because without them, the department may blunder into another avoidable surprise. Moreover, with such operational prioritization, naval counterintelligence can evolve from a historically reactive stance to a proactive posture and continue with its core mission, to ensure that the DON remains free from concerns about an adversary's *unexpected advantage*.

Questions for Further Study

Since the 1980s, better counterintelligence, security, military pay, and military family support services slashed the number of espionage cases in the DON. Competitive pay and family support services were positive motivators that help avoid the financial pitfalls that lead to

a variety of crimes, including espionage. Conversely, security and counterintelligence served as negative incentives for would-be spies. Security ensured that theft of classified information was as difficult as operational necessity allowed while counterintelligence was poised in the background to investigate any espionage allegation. Together, these four entities were a sturdy bulwark against the resurgence of the DON's espionage peak of the 1980s.

This study's data set was used to draw several correlations but did not explore causation. The starkest and potentially most fruitful of these correlations was the potential relationship between personnel support programs and espionage. Conceived to increase retention, these programs appear to also serve as a deterrent to espionage.

Personnel Support as an Espionage Deterrent

The U.S. naval espionage data set covered in this study suggests that the introduction of Family Service Centers across the DON reduced the number of naval espionage financial volunteers. As the Family Service Center concept spread throughout the department during the 1980s, cases of espionage in the department peaked in 1985 and then dropped precipitously.[32] This occurred despite an overall erosion of U.S. military pay after the significant increases in 1980–81.[33] The correlation of these two factors suggests that family support was a more significant factor than pay in a sailor or Marine's espionage calculus.

The naval espionage data set also suggests an inverse relationship between family support services and espionage. After the U.S. military's shift to an all-volunteer force in 1974, the number of young

[32] "40 Years of Meeting Your Needs . . . at Home and at Sea," Fleet and Family Support Center, 31 May 2019.
[33] James R. Hosek, Christine E. Peterson, and Joanna Zorn Heilbrunn, *Military Pay Gaps and Caps* (Santa Monica, CA: Rand, 1994), 7.

families in the Navy grew enormously, and family support programs began to assist them in a focused way starting in 1979.[34] Twenty-two years later, in 2001, the U.S. Navy changed the name from Navy Family Service Centers to Fleet and Family Support Centers to emphasize support for unmarried personnel as well.

The support that married personnel received from the DON after the inauguration of family support programs in 1979 appears to have made a significant impact on espionage. Prior to 1980, 75 percent of all the department's financial volunteer espionage subjects were married. That figure perhaps reflects the stresses of service without a dedicated family support program. Significantly, after 1980 that figure was reversed, with 75 percent of all financial volunteer subjects being unmarried. While far from conclusive, these figures suggest that family support programs slashed espionage amongst married personnel but had less effect on espionage committed by single sailors and Marines.

However, these correlations do not necessarily reflect causation, and further study would be required to determine how much effect the Family Service Center concept had on preventing espionage.

Resolving Ambiguity: The One that Got Away

Finally, any review of espionage will generate questions about "the one that got away." This study only accounts for cases that the DON made public and primarily includes investigations that resulted in prosecutions. Taking that fact into account, the "one that got away" argument was to prove a negative—to prove that an unidentified espionage case does not exist.

This exact issue faced the U.S. European Command's Joint Analysis Center in Molesworth, England, in 1999, during the Yugoslav Wars.

[34] "Building Now for the Future," *All Hands* (October 1979), 40.

At the time, the ability of the Serbian military to avoid North Atlantic Treaty Organization (NATO) air attacks caused serious concerns that espionage had compromised the daily air tasking order for the NATO air campaign.[35] A counterintelligence team was tasked with helping to resolve those allegations and tackled the problem through a dual approach. First, they assessed the ability of the Serbian intelligence service to conduct an espionage operation of the alleged magnitude and tempo. Second, they looked for alternative explanations for the Serbian behavior.

In the end, the counterintelligence team determined that Serbian intelligence was unlikely to have been able to conduct a clandestine intelligence operation that moved such a quantity of information in time to be of military utility. They also determined that NATO air forces were not properly using the secure communications equipment available to them during the air campaign. NATO aircrew often transmitted targeting information over unencrypted radios in sufficient time for mobile Serbian targets to relocate.[36] So, while the team could never rule out the one that got away, command-and-control issues were much more likely to be the culprit than an espionage operation.

In the same way, one can look at the overall scope of United States naval history and see that the potential advantage that the Soviet Union gained over U.S. SSBNs in the 1970s was the one of the most significant crises for the U.S. Navy in the twentieth century. With hundreds of investigations from the 1960s through the 1980s, Walker's espionage emerged as the most likely reason for the increased effectiveness of Soviet submarines. As with Serbia in 1999, counterintelligence can never

[35] Allan Little and Richard Norton-Taylor, "NATO Spy Leaked Bombing Raid Plans to the Serbs," *Guardian*, 9 March 2000; "Serbian Spy Report Does Exist, NATO Admits," *Globe and Mail*, 10 March 2000; and Robert Suro and Thomas E. Ricks, "Pentagon Acknowledges Leaks of NATO Kosovo Air War Data," *Washington Post*, 10 March 2000.

[36] "Operations Security (OPSEC)," Navy Information Warfighting Development Command, September 2017, 2–4.

absolutely prove the negative—the one that got away—but a reasoned assessment is possible.

This study is, of course, not complete. Many cases have been lost to history, the case files destroyed. Those cases, the ones that got away, should not detract from the trends that this study identifies nor the facts of the cases that remain. These are all valuable lessons for the future—lessons that the U.S. Navy and Marine Corps ignore at their peril.

Appendix A
Chronology of U.S. Naval Counterintelligence Events, 1882–2010

This chart depicts the relationship in time between the U.S. Department of the Navy's (DON) espionage cases and major events in military and counterintelligence history. Espionage case information is light gray; military and counterintelligence history events are dark gray; major DON events are black; and major adversary intelligence events are white.

1882	The Office of Naval Intelligence (ONI) is formed.
1889	Germany begins planning for conflict with the United States in the Pacific.
1898	The Spanish-American War begins.
	George A. Downing volunteers to spy for Spain.
	The Harbor Defenses And Fortifications Protection Act passes.
	The Spanish-American War ends; the United States gains Caribbean and Pacific possessions.
1909	Kurt Albert Jahnke, a suspected German naval intelligence agent, joins the U.S. Marine Corps and deploys to the Pacific region.
	The DON makes its first attempt at security classification.

1910	**Major shift. The U.S. Navy commissions its first dreadnought battleships, USS *South Carolina* (BB 26) and USS *Michigan* (BB 27); these are targets for technology-related espionage.**
1911	The Defense Secrets Act of 1911 is signed into law.
1913	USS *Pennsylvania* (BB 38) blueprints are stolen; no suspects are found.
1914	World War I begins in Europe.
1915	A U.S. Navy battle signal book is stolen from USS *Hull* (DD 7); the security of U.S. Navy command and control is at risk; no suspects are found.
	ONI begins counterintelligence missions.
1916	A replacement U.S. Navy battle signal book is issued.
	An unidentified chief petty officer with the U.S. Atlantic Fleet is investigated as a German asset; this is confirmed by signals intelligence.
	German intelligence focuses on U.S. reinforcement of the Allies in France.
1917	George Roenitz is mistakenly identified as a German asset.
	German assets Josephine Alvarez and Victorine Fauche are arrested in Nantes.
	The United States enters World War I.
	The unidentified Atlantic Fleet chief is removed from fleet duties.
	The DON adopts a version of the British and French security classification systems.
1918	World War I ends.
1923	Frederick J. Rutland, a former Royal Air Force officer, volunteers to spy for Japan.
1927	The Imperial Japanese Navy begins Pearl Harbor, HI, tabletop exercises.
1933	Rutland targets the U.S. Navy for Japan.
	John S. Farnsworth volunteers to spy for Japan; he compromises USS *Ranger* (CV 4) plans.

1934	**Major shift. The U.S. Navy commissions the first purpose-built aircraft carrier *Ranger*; the Navy again becomes a technology-related espionage target.**
	Christian F. Danielsen allegedly compromises *Farragut*-class destroyer design to Germany; this is disputed.
	Gustav E. Guellich allegedly volunteers as a German asset; this is disputed.
	Harry T. Thompson volunteers as a Japanese asset in California; he is arrested.
1935	Rutland is tasked to target Hawaii; he fails.
	Bernard J. O. Kuehn is recruited to target Hawaii for Japan; he moves to Hawaii from Germany; he fails.
1936	Farnsworth is arrested.
	The Japanese Naval Staff College recommends a surprise attack on Pearl Harbor if U.S. aircraft carriers are present.
	Maximilian G. Waldemar Othmer volunteers to spy for the German *Abwehr*.
1937	Hafis Salich volunteers to spy for the Soviet Union.
1938	The Drummond brothers attempt to compromise the Douglas SBD Dauntless dive bomber prototype; they are arrested.
	Salich is arrested.
1939	World War II begins in Europe.
	Simon Emil Koedel volunteers to spy for the *Abwehr* in New York.
1940	Othmer moves to Norfolk, VA; he works at the U.S. naval base there.
	Major shift. The U.S. Fleet moves from California to Hawaii; Pearl Harbor becomes a major Japanese espionage target.
1941	Takeo Yoshikawa arrives in Hawaii and provides precise reporting on Pearl Harbor.
	Velvalee M. Dickinson is recruited as a Japanese stay-behind asset.

	Japan attacks the United States and Allies in Hawaii, the Philippines, and Southeast Asia.
	The United States enters World War II.
	Yoshikawa is detained; he returns to Japan.
	Rutland is arrested in Great Britain.
	Kuehn is arrested in Hawaii.
1944	Othmer and Koedel are arrested.
	Dickinson is arrested.
1945	World War II ends.
1947	The Cold War begins.
1950	The Korean War begins.
1953	The Korean War armistice is signed.
1957	Nelson C. Drummond volunteers to spy for the Soviet Union for money.
1960	**Major shift. The first Polaris intercontinental ballistic missile is launched from a submerged submarine; the U.S. Navy becomes part of the U.S. nuclear triad and Soviet intelligence target.**
	Soviet military intelligence places an asset at Holy Loch, Scotland.
1961	U.S. Navy ballistic missile submarines (SSBN) begin refitting at Holy Loch.
1962	Drummond is arrested.
1963	The Soviet Committee for State Security (KGB) shifts from ideological to financial incentives.
1964	U.S. ground troops begin fighting in Vietnam.
1967	The Soviet asset Peter Dorschel is directed to Holy Loch.
	Gary L. Ledbetter offers to sell a SSBN piping manual to Dorschel; both are arrested.
	John A. Walker volunteers to spy for the Soviet Union; U.S. Navy command and control is compromised.
1968	Edward H. Wine contemplates espionage; he is arrested. U.S. Navy command and control remains compromised.

	The United States is warned about a KBG incentive shift
1971	The War on Drugs begins.
1972	The background investigation mission is moved from the Naval Investigative Service to the Defense Investigative Service.
1973	The U.S. Navy's Sound Surveillance System begins to miss Soviet Navy submarines; U.S. Navy command and control remains compromised.
	U.S. ground troops leave Vietnam.
1974	U.S. military conscription ends; the all-volunteer force begins.
1978	The Foreign Intelligence and Surveillance Act is signed into law.
1979	Lee E. Madsen attempts espionage on behalf of a drug smuggler; he is arrested.
	An Expanded Navy Family Service Center opens in Norfolk, VA.
1980	The Classified Information Procedures Act is signed into law.
	Glenn M. Souther volunteers to spy for the Soviet Union; U.S. Navy command and control remains compromised.
1981	Stephen A. Baba attempts espionage for South Africa; he is arrested; classified microfiche is stolen.
1982	Walker provides final tranche of crypto; U.S. Navy command and control is secure again
	Brian P. Horton attempts espionage for the Soviet Union; he is arrested.
	The "Horton clause" is introduced.
	Alan D. Coberly contemplates espionage; he is arrested.
	Brian E. Slavens attempts espionage; he is arrested.
	Jeffrey L. Pickering steals classified microfiche.
1983	Hans P. Wold contemplates espionage; he is arrested.
	Pickering spontaneously confesses; he is arrested.

	Robert W. Ellis attempts to volunteer to the Soviet Union; he is arrested.
1984	Robert E. Cordrey attempts espionage with Warsaw Pact countries.
	Samuel L. Morison compromises satellite imagery.
	Michael T. Tobias attempts espionage with the Soviet Union; this involves crypto; he is arrested.
	Jay C. Wolff attempts espionage with a "businessman"; he is arrested.
	Jonathan J. Pollard volunteers to spy for Israel.
1985	Chi Mak emigrates to the United States.
	Walker is arrested.
	Pollard is arrested.
	Calyton J. Lonetree is recruited by the Soviet Union.
	Wilfredo M. Garcia attempts espionage; he fails.
	Michael H. Allen volunteers to spy for the Philippines.
1986	Souther escapes to the Soviet Union.
	Robert D. Haguewood attempts espionage; he is arrested.
	Allen is arrested.
1988	Garcia is arrested.
	James R. Wilmoth and Russell P. Brown are recruited by Soviet Union; they fail.
	Randall S. Bush attempts espionage; he is arrested.
	Craig D. Kunkle attempts espionage.
1989	Kunkle is arrested.
	Donald W. King and Ronald D. Graf attempt espionage; they are arrested.
	Wilmoth and Brown are arrested.
	Frank A. Nesbitt volunteers to spy for the Soviet Union.
	Charles E. Schoof and John J. Haeger attempt espionage; they are arrested.
1990	Charles F. L. Anzalone attempts espionage; he is arrested.
	The Gulf War begins.

1991	The Gulf War ends.
1992	The Cold War ends.
	Michael S. Schwartz compromises classified material to Saudi Arabia.
1993	Antonio Guerrero begins his mission in Key West, FL, for Cuban intelligence.
	Al-Qaeda bombs the World Trade Center in New York City.
1995	The People's Republic of China (PRC) begins naval modernization.
1996	Robert C. Kim commits espionage for South Korea; he is arrested.
	Kurt G. Lessenthien attempts espionage for Russia; he is arrested.
1998	Guerrero is arrested.
2001	Hassan Abu-Jihaad compromises classified material to al-Qaeda.
	Al-Qaeda attacks the United States; the Afghanistan War begins.
	Major shift. The Defense Travel System is introduced; mass movement of information to online systems begins in the U.S. Navy; computer systems become an espionage target.
2003	The PRC compromises U.S. Navy computers for the first time.
	The Iraq War begins.
2005	Mak is arrested.
	Ariel J. Weinmann deserts the U.S. Navy; volunteers to spy for Russia.
2006	Weinmann is arrested.
2008	Abu-Jihaad is convicted.
2010	Bryan M. Martin attempts to commit espionage for the PRC; he is arrested.

Appendix B
Department of the Navy Counterintelligence Lessons Learned, 1898–2010

The list below summarizes U.S. naval counterintelligence lessons learned during each major period of time presented in this study. If the lesson appears to have been forgotten and relearned in a later period, a notation in parentheses is included.

Early Modern Period, 1898–1918

- The Department of the Navy (DON) needed a well-resourced counterintelligence capability.
- The DON needed an information security classification system.
- The DON's technology was an adversary target.
- The DON's command and control was an adversary target.
- An undercover agent was useful.
- Signals intelligence (SIGINT) provided a useful lead.
- Effective counterintelligence required a legal framework to operate.
- Liaison with allied counterintelligence was vital to success.
- Penetration of adversary intelligence services could uncover espionage.
- Ethnic profiling was an ineffective counterintelligence tool.

World War II Period, 1919–45

- The DON needed well-resourced counterintelligence capability (second time).
- The DON's counterintelligence capability must be trained and experienced.
- Effective counterintelligence required a legal framework to operate (second time).
- Liaison with allied counterintelligence was vital to success (second time).
- Solid liaison with the Federal Bureau of Investigation (FBI) and other military Service counterintelligence was vital to success.
- SIGINT provided useful espionage leads (second time).
- Significant others provided useful espionage leads.
- Surveillance assets were vital to success.
- Navy contractor information security required detailed oversight.
- Espionage suspects were difficult to turn into double agents.
- Intimate knowledge of adversary espionage techniques was vital to success.
- Confirmation bias by counterintelligence analysts was a fatal flaw.

Early Cold War Period, 1946–79

- The DON needed well-resourced counterintelligence capability (third time).
- The DON's counterintelligence capability must be trained and experienced (second time).
- Solid liaison with the FBI was vital to success (second time).
- The polygraph was fallible.
- Penetrations of adversary intelligence provided good espionage leads (second time).
- Technology assisted surveillance.

- Close liaison with allied counterintelligence was vital (third time).
- Criminals served as intermediaries.
- Poorly paid personnel could turn to espionage.
- The DON's command and control was an adversary target (second time).
- Significant others provided useful espionage leads (second time).
- Surveillance assets were vital to success (second time).
- Witting accomplices could be involved in an espionage scheme.
- Informants were useful in espionage investigations.
- Classified hoarders sometimes turned to espionage.
- An undercover agent was useful (second time).

Late Cold War Period, 1980–92

- Espionage allegations should be pursued aggressively.
- Significant others provided useful espionage leads (third time).
- Undercover agents were useful (third time).
- Deserters turned to espionage to fund their escapes.
- Surveillance of adversary diplomatic establishments was a last layer of defense.
- Access to classified material was not a prerequisite for espionage.
- Close liaison with allied counterintelligence was vital (fourth time).
- Close liaison with other agencies' counterintelligence elements was vital (second time).
- A subject volunteered to multiple adversaries at the same time.
- Basic criminal investigative techniques could be applied to espionage.
- Espionage sometimes involved two or more coconspirators.
- Criminals served as intermediaries (second time).
- Allies sometimes elected to accept espionage volunteers.
- Subjects committed espionage from classified memories.

Post-Cold War Period, 1993–2010

- Some espionage involved a false flag.
- Deserters turned to espionage to fund their escapes (second time).

Appendix C
Glossary of Select Terms

Abwehr. The German intelligence and counterintelligence service from 1920–45. This was divided into five departments: overt foreign intelligence, espionage, sabotage/subversion, counterintelligence, and administration. Department II (espionage) failed to control any worthwhile agents in the United Kingdom or the United States. During the latter stages of World War II, the *Abwehr* became a center for anti-Adolf Hitler conspiracies.[1]

accommodation address. An address where regular posted mail, or sometimes another type of communication, is received and then held for pickup or forwarded, transmitted, or relayed to a member of an intelligence service who does not occupy the premises. This is sometimes called a mail drop.[2]

agent. A person who engages in clandestine intelligence activities under the direction of an intelligence organization but is not an officer, employee, or co-opted worker of that organization.[3]

allied espionage. A concept that evolved from an analysis of the espionage investigations considered in this study. Allied espionage is a human intelligence operation conducted by an ostensible ally or defense partner of the victim country.

---

[1] Richard Holmes, ed., *The Oxford Companion to Military History* (Oxford, UK: Oxford University Press, 2001), 2.
[2] Col Mark L. Reagan, USA (Ret), ed., *Counterintelligence Glossary: Terms and Definitions of Interest for Counterintelligence Professionals* (Washington, DC: Department of Defense, 2014), 3.
[3] Reagan, *Counterintelligence Glossary*, 8.

asset. An individual who has been subject to a successful deliberate and calculating effort by an intelligence or counterintelligence service to induce them to furnish information or to carry out tasks. An asset is a recruited source.[4]

backstopping. Arrangements made to support a protective guise used by a person, organization, or installation to conceal true affiliation with clandestine or other sensitive activities so that inquiries about those arrangements will elicit responses that make them appear to be true.[5]

battle signal book. Issued in 1913, this was the U.S. Navy's radio codebook for transmitting tactical and battle orders. It used a transposition cipher to scramble Morse code messages sent between ships at sea. Published as a "strictly confidential" registered publication, physical security and accountability measures applied consisted of limiting issue of the book to officers only.[6]

black bag job. A surreptitious entry operation. This includes any entry into a guarded or locked area or container and a departure therefrom without leaving a trace that such entry was made.[7]

brush pass. A brief operational encounter (seconds or less) in which the case officer passes something (verbally or physically) to or receives something from the agent.[8]

campaign-altering espionage. A concept that evolved from an analysis of the espionage investigations considered in this study. Campaign-altering espionage has the potential to materially change the outcome of a military campaign. The impact of the espionage may not become apparent for months, years, or even decades afterward. This type of espionage results in strategic sur-

[4] Reagan, *Counterintelligence Glossary*, 18.
[5] Reagan, *Counterintelligence Glossary*, 21.
[6] Capt Linwood S. Howeth, USN (Ret), *History of Communications-Electronics in the United States Navy* (Washington, DC: Government Printing Office, 1963), 200.
[7] Reagan, *Counterintelligence Glossary*, 24.
[8] Reagan, *Counterintelligence Glossary*, 27.

prise because the adversary's advantage is unexpected. The link between the espionage and its impact on a military campaign is often not understood at the time and potentially overlooked for years or decades afterwards. Examples include the Confederate espionage operation at Charleston, South Carolina, in 1863, Yoshikawa's espionage in Hawaii in 1941, and the Walker case during 1967–85. However, if the espionage threat is precluded or proximately neutralized, then the counterintelligence effort can be seen as an overreaction. See also *paradox of warning*.

case officer. A professional employee of an intelligence or counterintelligence organization who is responsible for providing directions for an agent operation and/or handling intelligence assets.[9]

Central Intelligence Agency (CIA). An independent U.S. government agency responsible for providing national security intelligence to senior U.S. policymakers. Its primary mission is to collect, analyze, evaluate, and disseminate foreign intelligence to assist the president and senior government policymakers in making decisions relating to national security.[10]

Classified Information Procedures Act (CIPA) of 1980. The tool with which the proper protection of classified information may be ensured in indicted cases. After a criminal indictment becomes public, the prosecutor remains responsible for taking reasonable precautions against the unauthorized disclosure of classified information during the case. This responsibility applies both when the government intends to use classified information in its case as well as when the defendant seeks to use classified information in their defense. The procedural protections of CIPA protect unnecessary disclosure of classified information. The primary purpose was to limit the practice of "gray mail" by crim-

[9] Reagan, *Counterintelligence Glossary*, 29.
[10] Reagan, *Counterintelligence Glossary*, 30.

inal defendants in possession of sensitive government secrets. *Gray mail* refers to the threat by a criminal defendant to disclose classified information during a trial. The gray mailing defendant essentially presented the government with a "Hobson's choice" to either allow disclosure of the classified information or dismiss the indictment.[11]

coded letter. A letter that uses an open code to obscure its true meaning. See also *open code*.[12]

communications security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.[13]

compartmentalization (or compartmentation). The establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties.[14]

confirmation bias. The tendency to process information by looking for, or interpreting, information that is consistent with one's existing beliefs. This biased approach to decision making is largely unintentional and often results in ignoring inconsistent information. Existing beliefs can include one's expectations in each situation and predictions about a particular outcome. People are especially likely to process information to support their own beliefs when the issue is highly important or self-relevant.[15]

---

[11] Reagan, *Counterintelligence Glossary*, 35–36; and "Classified Information Procedures Act," Pub. L. No. 96-456, 94 Stat. 2025, 1980.
[12] *Basic Cryptologic Glossary* (Washington, DC: National Security Agency, 1955), 24.
[13] Reagan, *Counterintelligence Glossary*, 43–44.
[14] Reagan, *Counterintelligence Glossary*, 44–45.
[15] Bettina Casad, "Confirmation Bias," in *Encyclopedia of Social Psychology*, ed. Roy F. Baumeister and Kathleen D. Vohs (Thousand Oaks, CA: Sage, 2007), 162–63.

cover address. See *accommodation address*.

cover provider. An existing government agency or private company that agrees to allow intelligence officers to masquerade as employees to facilitate intelligence operations.[16] A cover provider is distinct from a front, which is a legitimate operation created by an intelligence organization as a cover for its operatives.[17]

cutout. An intermediary or device used to obviate direct contact between members of a clandestine organization.[18]

cyber espionage. Officially known as *computer network exploitation* (CNE), this is intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks.[19]

dead drop. A clandestine communications technique that allows agents to exchange messages and other items without the need for a meeting that might attract the attention of hostile surveillance. The dead drop is usually an innocuous, prearranged site where a package can be secreted temporarily so it can be recovered by the addressee. Ideally, the location is sufficiently innocent to enable both parties to visit it, at different times, without compromising themselves. Dead drops are usually associated with a remote signaling arrangement so that both sides can indicate to the other when a particular drop is ready for servicing. The objective is to obviate the need for personal contact that in denied areas is high risk.[20]

Defense Secrets Act of 1911. The first statute that stipulated that obtaining national defense information through unauthorized entry of any place connected with defense was a crime. Receipt and

[16] David G. Marwell, "CIA Employees," Central Intelligence Agency memorandum, 15 April 1997, 5.
[17] Reagan, *Counterintelligence Glossary*, 149.
[18] Reagan, *Counterintelligence Glossary*, 88.
[19] Reagan, *Counterintelligence Glossary*, 90.
[20] Reagan, *Counterintelligence Glossary*, 101.

further transmission of the information was also criminalized. The law was loosely based on the British Official Secrets Act.[21]

deserter spy. A profile that evolved from an analysis of the espionage investigations considered in this study. This is espionage committed by active-duty military personnel who attempt to permanently remove themselves from military service without authorization. The espionage is often committed to fund the deserter's outlaw existence. The information proffered is either memories or hoarded prior to desertion.

disinformation. Carefully contrived misinformation prepared by an intelligence or counterintelligence service for the purpose of misleading, deluding, disrupting, or undermining confidence in individuals, organizations, or governments.[22]

double agent. An agent in contact with two opposing intelligence services, only one of which is aware of the double contact.[23]

dual-use. Technology and articles that can be potentially used either for commercial/civilian purposes or for military, defense, or defense-related purposes.[24]

engagement-altering espionage. A concept that evolved from an analysis of the espionage investigations considered in this study. Engagement-altering espionage is a case that has the potential to materially change the outcome of a military engagement. This espionage can take place months, years, or decades prior to the engagement and results in tactical or operational surprise, but the surprise is readily apparent and can be rectified relatively swiftly. An old example is the U.S. espionage during the American Civil War that revealed the extent of Confederate preparation of the

[21] Ken G. Robertson, ed., *British and American Approaches to Intelligence* (New York: St. Martin's Press, 1987), 254.
[22] Reagan, *Counterintelligence Glossary*, 119.
[23] Reagan, *Counterintelligence Glossary*, 122–24.
[24] Reagan, *Counterintelligence Glossary*, 125.

armored surface combatant CSS *Virginia*, which allowed for a more rapid employment of USS *Monitor* in response. A more recent example is U.S. espionage in the late 1960s that revealed information about the Soviet SS-N-2 Styx antiship missile, which, in the aftermath of the sinking of INS *Eliat* in 1967, prompted the U.S. Navy to develop the close-in weapon system (CIWS) that is mounted on most U.S. Navy ships today.

Espionage Act of 1917. A U.S. federal law passed in June 1917, shortly after the U.S. entry into World War I. It prohibited any attempt to interfere with military operations, to support enemies of the United States during wartime, to promote insubordination in the military, or to interfere with military recruitment. The law was further strengthened by the Espionage and Sabotage Act of 1954, which authorized the death penalty or life imprisonment for espionage or sabotage in peacetime as well as during wartime. The act requires agents of foreign governments to register with the U.S. government. It also suspended the statute of limitations for treason. In 1958, the scope of the act was broadened to cover Americans engaged in espionage against the United States while overseas.[25]

Executive Order 12333 (United States Intelligence Activities). Issued by President Ronald W. Reagan in 1981, this executive order codified the organization of the U.S. intelligence community. Regarding counterintelligence, the opening paragraph of the executive order noted: "Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests." It also specifically directs the U.S. Navy and Marine Corps to conduct counterintelligence ac-

[25] Reagan, *Counterintelligence Glossary*, 132–33; and Espionage Act of 1917, Pub. L. 65–24, 40 Stat. 217 (1917).

tivities and designates naval counterintelligence organizations as part of the U.S. intelligence community.[26]

false flag. When an individual is recruited believing that they are cooperating with an intelligence service of a specific country but, actually, they have been deceived and are cooperating with an intelligence service of another country. This is also an approach by a hostile intelligence officer who misrepresents themselves as a citizen of a friendly country or organization. The person who is approached may give up sensitive information, believing that it is going to an ally rather than a hostile power.[27]

Federal Bureau of Investigation (FBI). The primary investigative arm of the U.S. Department of Justice with jurisdiction over violations of more than 200 categories of federal law and a statutory member of the U.S. intelligence community. The FBI's mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies, and partners.[28]

financial volunteer. A profile that evolved from an analysis of the espionage investigations considered in this study. It is comprised of the motive and means by which the espionage subject approached a foreign intelligence service. Financial volunteers composed more than half of all the espionage subjects considered in this study. Nearly all exhibited financial and personal problems and substance abuse. They tended to be either civilian employees of the Department of the Navy (DON) or junior

[26] "Executive Order 12333: United States intelligence activities," National Archives and Records Administration, accessed 1 October 2022. Note: the definition of *counterintelligence* in Executive Order 12333 and Secretary of the Navy Instruction 3850.2E are identical.
[27] Reagan, *Counterintelligence Glossary*, 137.
[28] Reagan, *Counterintelligence Glossary*, 138.

enlisted active-duty Marines or sailors. The civilians tended to be older, while the Marines and sailors tended to be younger. The financial volunteers in this study turned to whatever country was in the news as the major "threat" to the United States because they often thought that country would pay more. They almost always approached the nearest diplomatic establishment and saw the information entrusted to them as a commodity that they could sell. Most were caught quickly because they used only the tradecraft they contrived themselves. Gaps in counterintelligence coverage of foreign diplomatic establishments allowed some to slip through. Financial volunteers often acted irrationally and spent conspicuously.

Foreign Intelligence Surveillance Act (FISA) of 1978. The legal authority authorizing and regulating electronic surveillance within the United States for foreign intelligence or counterintelligence purposes and physical searches within the United States for foreign intelligence purposes. The act sets out the application, order, and report process to be followed.[29]

German American Bund. The *Amerikadeutscher Volksbund*, or German American Bund, was formed in 1936 as "an organization of patriotic Americans of German stock," operating about 20 youth and training camps and eventually expanding its membership to tens of thousands of people among 70 regional divisions across the United States. On 20 February 1939, the Bund held an "Americanization" rally in New York's Madison Square Garden, denouncing Jewish conspiracies, President Franklin D. Roosevelt, and others. The rally, attended by 20,000 supporters and members, was protested by huge crowds of anti-Nazis, who were held back by 1,500 New York City police officers. When World War II began in 1939, the German American Bund fell

[29] Reagan, *Counterintelligence Glossary*, 145–46.

apart, many of its assets were seized, and its leader arrested for embezzlement and later deported to Germany.[30]

***Glavnoye Razvedyvatel'noye Upravlenie* (GRU).** The Chief Intelligence Directorate of the General Staff (a.k.a. Soviet and Russian military intelligence).[31]

handler. An intelligence officer or principal agent who directly manages an agent or agent network. They are also known as a case officer.[32]

hoarder espionage. A profile that evolved from an analysis of the espionage investigations considered in this study. Several espionage subjects described in this study hoarded classified information in an unauthorized location for a variety of reasons not related to espionage and then later attempted to use that information to commit espionage. Hoarder espionage subjects were often financial volunteers.

Horton Clause. A legal strategy that uses evidence accumulated during an investigation to convince the subject to plead guilty under a pretrial agreement that includes a post-trial grant of immunity, allowing investigators to continue to question the subject to ensure a complete damage assessment. This legal strategy was first employed by the DON in 1982 during the Brian Horton case.[33]

ideological volunteer. A profile that evolved from an analysis of the espionage investigations considered in this study. An ideological volunteer initiates contact with a foreign intelligence service because of their commitment to a competing political or economic system and/or intellectual or emotional commitments to anoth-

[30] Alan Taylor, "American Nazis in the 1930s: The German American Bund," *Atlantic*, 5 June 2017.
[31] Kevin P. Riehle, *Russian Intelligence: A Case-based Study of Russian Services and Missions Past and Present* (Bethesda, MD: National Intelligence Press, 2022), 46.
[32] Reagan, *Counterintelligence Glossary*, 156.
[33] *Espionage* (Washington, DC: Naval Investigative Service Command, 1989), 11.

er country through birth, family ties, or cultural affinity.[34] Ideological volunteers composed less than one-sixth of espionage subjects considered in this study. They were mostly active-duty military servicemembers who adopted a foreign culture as their own. Like financial volunteers, they generally adopted a foreign culture in the news at the time and tended to try to find the nearest "official" representative they could locate. Unlike financial volunteers, they did not look for the biggest payoff, instead looking for the information that they thought would help the foreign entity the most. Ideological volunteers were difficult to detect because they tended to be in some sort of relationship with the foreign culture before the espionage relationship began. Among the espionage cases examined in this study, ideological volunteers tended to be detected through a handler mistake vice any actions by U.S. counterintelligence.

indication and warning. Intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intentions. This is also known as warning intelligence.[35]

informant. A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police.[36]

invisible ink. Special inks to write messages clandestinely by rendering the writing invisible. The use of special inks is known as the "wet system." Also known as secret writing.[37]

***Komitet Gosudarstvennoy Bezopasnosti* (KGB).** The Soviet Committee for State Security that was officially disbanded in 1991. The KGB was the civilian intelligence and internal security agency of the Soviet Union. In Russia today, the KGB's intelligence func-

[34] Reagan, *Counterintelligence Glossary*, 221.
[35] Reagan, *Counterintelligence Glossary*, 343.
[36] Reagan, *Counterintelligence Glossary*, 172.
[37] Reagan, *Counterintelligence Glossary*, 281–82.

tions are performed by the Foreign Intelligence Service, while its internal security functions are performed by the Federal Security Service.[38]

Kotani-shift. A theory, advanced by Japanese historian Ken Kotani in 2009, that during the 1930s, Japanese intelligence shifted from technology to strategic intelligence in the final years before the start of the Pacific war in 1941.[39] This study noted the same shift in German intelligence prior to the entry of the United States into World War II, and recent evidence could be interpreted as suggesting that the People's Republic of China entered the same shift in the mid-2020s.

legend. A coherent and plausible account of an individual's background, living arrangements, employment, daily activities, and family given by a foreign intelligence service by an illegal or agent. Often the legend will be supported by fraudulent documents.[40]

mail cover. The process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the postal service.[41]

Morse code. A system for representing letters of the alphabet, numerals, and punctuation marks by an arrangement of dots, dashes, and spaces. The codes are transmitted as electrical pulses of varied lengths or analogous mechanical or visual signals, such as flashing lights. The system was invented by American artist and inventor Samuel F. B. Morse during the 1830s for electrical telegraphy.[42]

---

[38] Riehle, *Russian Intelligence*, 36.
[39] Ken Kotani, *Japanese Intelligence in World War II* (New York: Osprey, 2009), 79–86.
[40] Reagan, *Counterintelligence Glossary*, 206.
[41] Reagan, *Counterintelligence Glossary*, 210.
[42] "Morse Code," Britannica, accessed 1 October 2022.

Nachrichtenstelle. The informal name for German naval intelligence in the early 1900s. The full name in German was the *Marine Nachrichtenstelle* or N-stelle.[43]

Naval Criminal Investigative Service (NCIS). Led by a senior executive service civilian criminal investigator and subordinate to the U.S. secretary of the Navy since 1992. The reorganization was prompted by two controversial criminal investigations. NCIS continued the NIS mission to serve as the DON's counterintelligence and criminal investigations agency.[44]

Naval Investigative Service (NIS). The DON's counterintelligence and criminal investigations agency, which focused heavily on background investigations and was commanded by a Navy captain subordinate to the director of naval intelligence from 1966 to 1985. In 1972, the Defense Investigative Service (DIS) was formed and assumed responsibility for conducting all security background investigations. One-half of NIS's 1,000 special agents were immediately transferred to DIS. From 1985 to 1992, an admiral, usually a judge advocate flag officer, commanded NIS and was subordinate to the chief of naval operations. From 1988 to 1992, NIS was redesignated the Naval Investigative Service Command.[45]

nonofficial cover. A term used by case officers who operate overseas outside the usual diplomatic cover.[46]

observational espionage. A concept that evolved from an analysis of the espionage investigations considered in this study. Several espionage subjects described in this study intentionally gathered information without being detected through observation, pho-

---

[43] Richard B. Spence, "K. A. Jahnke and German Sabotage Campaign in the United States and Mexico, 1914–1918," *Historian* 59, no. 1 (Fall 1996): 89–112.
[44] Mullis, *A Brief History of the Naval Criminal Investigative Service*, 8.
[45] H. Paul Mullis, ed., *A Brief History of the Naval Criminal Investigative Service* (Washington, DC: Naval Criminal Investigative Service, 1997), 7.
[46] Reagan, *Counterintelligence Glossary*, 238.

tography, mapping, and/or describing a specific location and then reported that information to a foreign entity.

Office of Naval Intelligence (ONI). Formed in 1882 after a U.S. naval officer in the Bureau of Navigation persuaded the secretary of the Navy to create an "Office of Naval Intelligence" for the purpose of "collecting and recording such Naval information as may be useful to the Department in time of war as well as peace." In 1915, the DON assigned ONI the job of collecting information on domestic threats, and by 1917 ONI had organized a nationwide counterintelligence capability. From 1916 to 1937, most ONI counterintelligence personnel were active-duty servicemembers. From 1937 to 1969, ONI and NIS hired civilian investigators on short-term contracts. However, in 1969, NIS received authority to hire investigators as permanent government employees.[47]

open code. A system of disguised secret writing in which units of plain text are used as the code equivalents for letters, numbers, words, phrases, or sentences. The code equivalents themselves, usually words or phrases, can be combined to form the intelligible text of apparently innocent messages.[48]

operations security (OPSEC). A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; to determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries and determine which of these represent an unacceptable risk; and to then select and execute countermeasures that eliminate the risk

[47] Mullis, *A Brief History of the Naval Criminal Investigative Service*, 3.
[48] *Basic Cryptologic Glossary*, 24.

to friendly actions and operations or reduce it to an acceptable level.[49]

paradox of warning. Enemy counteraction based on action taken because of a warning that alters the enemy's initially intended course of action. The warning appears to be wrong because of the change in enemy action. Also known as the "warning paradox."[50]

partner espionage. A profile that evolved from an analysis of the espionage investigations considered in this study. Several espionage cases described in this study involved two or more coconspirators excluding foreign intelligence operatives. Partner espionage often involved one individual with a security clearance who stole classified information and a second person without a security clearance who proffered the information to a foreign intelligence service.

patriotic penetration. A profile that evolved from an analysis of the espionage investigations considered in this study. Foreign intelligence services placed several espionage subjects described in this study in a target area in territory hostile to them with the intention of acquiring access to a specific government agency or military command. These individuals appeared to be motivated by patriotism and were recruited by their native country and targeted a specific foreign institution by joining that institution. They usually held low-level positions with little or no access to classified information and joined or were employed after a period of life experience rather than directly from school. They constituted only a fraction of the espionage subjects considered in this study.

---

[49] Reagan, *Counterintelligence Glossary*, 245–46; and *Operations Security (OPSEC)*, Navy Tactical Techniques and Procedures 3-13.3M; Marine Corps Tactical Publication 3-32B (Washington, DC: Department of the Navy, 2017).

[50] *Intelligence Warning Terminology* (Washington, DC: Joint Military Intelligence College, 2001), 28.

People's Liberation Army (PLA). The military arm of the Chinese Communist Party established in 1927. Initially solely ground forces, in 1949 the PLA expanded to include the PLA Navy and the PLA Air Force. As of 2019, the PLA was seeking to develop into a world-class military force with global reach.[51]

petty espionage. This term emerged from an analysis of the espionage investigations considered in this study. Approximately one-fifth of the espionage case subjects considered in this study launched their bid based on ill-conceived plans and/or conspiracies that were easily detected by U.S. counterintelligence before or immediately after the first contact with a foreign intelligence service. These cases were, by their nature, strategically insignificant. However, if U.S. counterintelligence had not detected these cases, they could have developed into strategically significant cases. These cases were petty only in hindsight, not at the time.

physical surveillance. The systematic observation of persons, places, or things by visual or photographic means.[52]

reactive double agent. An agent in contact with two opposing intelligence services, only one of which is aware of the double contact, that is initiated in response to a foreign intelligence operative's contact.[53]

recruitment-in-place. An official who overtly continued to work for their government and clandestinely provided information of intelligence value to a foreign government; in many instances they legitimately interacted with a foreign government.[54] These officials were sought out by foreign intelligence for their access to specific information of interest. More than one-quarter of the espionage

[51] *China Military Power: Modernizing a Force to Fight and Win* (Washington, DC: Defense Intelligence Agency, 2019).
[52] Jan Goldman, *Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats* (Lanham, MD: Scarecrow Press, 2011), 243.
[53] Reagan, *Counterintelligence Glossary*, 268.
[54] Reagan, *Counterintelligence Glossary*, 272.

subjects considered in this study were recruitments-in-place. However, one-third were recruited by a friend or family member who was already engaged in or contemplating espionage, not a foreign intelligence officer. A foreign intelligence officer directly recruited about one-fifth of the total number of espionage subjects considered. These agents often met the intelligence officer through a legitimate interaction. Then, once the intelligence officer realized their placement, access, and, most importantly, their motivation, the recruitment began. Like patriotic penetrations, the recruitments-in-place considered in this study received specific tasking and tended to provide just that information.

security classification. A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. Defined by Executive Order 12356. There are three categories of security classification:

- **Top Secret.** National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; compromise of vital national defense plans or complex cryptologic and communications intelligence systems; revelation of sensitive intelligence operations; and disclosure of scientific or technological developments vital to national security.
- **Secret.** National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be ex-

pected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

- **Confidential.** National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.[55]

signals intelligence (SIGINT). The collection and exploitation of signals transmitted from communication systems, radars, and weapon systems. SIGINT consists of communications intelligence, which is technical and intelligence information derived from intercept of foreign communications; electronic intelligence, which is information collected from systems such as radars and other weapons systems; and foreign instrumentation signals intelligence, which is signals detected from weapons under testing and development.[56]

stay behind (a.k.a. sleeper). An agent or agent organization established in a given country to be activated in the event of hostile overrun or other circumstances under which normal access would be denied.[57]

surveillance detection route. A carefully crafted route, of varying lengths and complexity depending on the operational environment, used by a case officer and/or an agent to get to a meeting

[55] "Executive Order 12356: National Security Information," National Archives and Records Administration, accessed 1 October 2022; and Reagan, *Counterintelligence Glossary*, 285.
[56] Reagan, *Counterintelligence Glossary*, 292.
[57] Reagan, *Counterintelligence Glossary*, 302.

site, and to determine that the case officer and/or agent are not under surveillance prior to and after the meeting.[58]

technical surveillance. Undetected observation using various forms of visual, auditory, and electronic aids in covering a designated target.[59]

tradecraft. Specialized methods and equipment used in the organization and activity of intelligence organizations, especially techniques and methods for handling communications with agents. Operational practices and skills used in the performance of intelligence related duties.[60]

trash cover. The intentional search of a specific person's trash (that is located at the place of collection), whether from a home or business, designed to find information relevant to an ongoing investigation when no reasonable expectation of privacy exists. A trash cover is a targeted effort to gather information regarding a particular person or entity by reviewing that person or entity's refuse.[61]

undercover agent. A counterintelligence investigative technique used to determine whether a suspected spy intends to or has committed espionage or other national security crimes against the United States. This is a form of false flag operation in which a U.S. counterintelligence or law enforcement officer poses as an intelligence operative of a foreign power in an undercover operation.[62]

walk-in. An unsolicited contact who voluntarily provides information.[63]

---

[58] Reagan, *Counterintelligence Glossary*, 311–12.
[59] Reagan, *Counterintelligence Glossary*, 310–11.
[60] Reagan, *Counterintelligence Glossary*, 326–27.
[61] Reagan, *Counterintelligence Glossary*, 329.
[62] Reagan, *Counterintelligence Glossary*, 137–38.
[63] Reagan, *Counterintelligence Glossary*, 342.

Warsaw Pact. A military alliance comprising eight countries—Albania, Bulgaria, Czechoslovakia, East Germany, Hungary, Poland, Romania, and the Soviet Union—in 1955–91. The alliance was led by the Soviet Union and throughout its 35-year history was the principal opponent of and military threat to the North Atlantic Treaty Organization. Also known as the Warsaw Treaty Organization.[64]

[64] Holmes, *The Oxford Companion to Military History*, 984.

Appendix D
Department of the Navy Espionage Subjects Chronological Bibliography

George A. Downing. 1898. Former commissary yeoman, USN. Volunteered to spy for Spain at the start of the Spanish-American War to report on U.S. Navy activities. Arrested and committed suicide in prison.

"An Alleged Spy Suicides." *Evening Bee* (Sacramento, CA), 12 May 1898.

"Challenged to a Duel." *New York Times*, 26 April 1898.

"Doings of Senor Polo." *Evening Star* (Toronto, ON), 25 April 1898.

"Letter from U.S. Secretary of the Treasury Lyman J. Gage to U.S. Secretary of State John Sherman regarding surveillance of Carranza, 6 July 1898." Record Group 59: General Records of the Department of State, Series: Letters Received, File Unit: M179–Miscellaneous Letters of the Department of State, 1789–1906, Item, July 1–11, 1898, NAID: 153522163, National Archives and Records Administration, College Park, MD.

"Letter from U.S. Secretary of War Russell A. Alger to U.S. Secretary of State John Sherman regarding disposition of personal effects of George Downing, 6 July 1898." Record Group 59: General Records of the Department of State, Series: Letters Received, File Unit: M179–Miscellaneous Letters of the Department of State,

1789–1906, NAID: 153522163, National Archives and Records Administration, College Park, MD.
"Our Military Secret Service." *New York Times*, 10 May 1898.
"Suspected Spy, George Downing." *Evening Bee* (Sacramento, CA), 11 May 1898.
The American-Spanish War: A History by War Leaders. Norwich, CT: Chas. C. Haskell & Son, 1899.

Kurt A. Jahnke. 1909. Private, USMC. Allegedly joined the Marine Corps on the orders of German naval intelligence to report on U.S. activities in the Pacific. Undetected.

"Albert Kurt Jahnke: Request for Marine Corp [*sic*] Records of." Washington, DC: Bureau of Investigation, Department of Justice, 27 April 1923.
Landau, Henry. *The Enemy Within: The Inside Story of German Sabotage in America*. New York: G. P. Putnam's Sons, 1937.
Spence, Richard B. "K. A. Jahnke and German Sabotage Campaign in the United States and Mexico, 1914–1918." *Historian* 59, no. 1 (Fall 1996): 89–112.

Unidentified Chief. 1916. Chief petty officer (rate unknown), USN. Allegedly in contact with German intelligence to report on U.S. Atlantic Fleet. Never tried.

Packard, Capt Wyman H., USN (Ret). *A Century of U.S. Naval Intelligence*. Washington, DC: Department of the Navy, 1996.

Josephine Alvarez and Victorine Faucher. 1917. French civilians. In contact with German intelligence to report on U.S. arrivals in French ports. Arrested by French authorities and executed.

Charles Munn: Blindfolding the Hun. Office of Naval Investigation Attaché Report. File 10848, Box 704, Record Group 38: Records of the Office of the Chief of Naval Operations, National Archives and Records Administration, Washington, DC.

"Espionnes fusillées [Spies Shot]: Joséphine Alvarez-Victorine Faucher." *Guillotine*, 8 February 2012.

"Lt. C. A. Munn." World War I Investigative Files, Formerly Confidential General Correspondence, 1913–1924. File 25100-603, Box 91, Entries 78 and 78A, Record Group 38: Records of the Office of the Chief of Naval Operations, National Archives and Records Administration, Washington, DC.

War Records of the Knickerbocker Club, 1914–1918. New York: Knickerbocker Club, 1922.

George Roenitz. 1917. Civilian, chief clerk, U.S. Naval Station Pearl Harbor, HI. Allegedly committed espionage; pled guilty to mishandling classified information. Suspected case of ethnically motivated prosecution.

"Former Naval Clerk Held as German Spy," *San Francisco (CA) Examiner*, 23 May 1917, 8.

"Memo from the Aid for Information to the Director of the Office of Naval Intelligence, dated July 2, 1918: Subject: George Roenitz." World War I Investigative Files, Formerly Confidential General Correspondence, 1913–1924. File 20940-11, Box 1, Entry 78A, Record Group 38: Records of the Office of the Chief of Naval Operations, National Archives and Records Administration, Washington, DC.

Wagner-Seavey, Sandra E. "The Effect of World War I on the German Community in Hawaii." *Hawaiian Journal of History* 14 (1980): 109–40.

Frederick J. Rutland. 1923–40. Former squadron leader, British Royal Air Force. A carrier aviation pioneer who collaborated with Japanese naval aviation from 1923 to 1932. Subsequently recruited to spy on the U.S. Navy in California. Detained by British authorities in the United States in 1940 and interned in the United Kingdom until 1943.

"Frederick Joseph Rutland, Spare Copy as Sent to SIS, undated." Records of the [British] Security Service. Rutland, Frederick Joseph, Case PF 37996 Volume 11, [British] National Archives, Kew, Richmond, UK, KV-2-333.

"Home Office Internment Appeal Meeting Transcript, dated 15 January 1942," 21–24. Records of the [British] Security Service. Rutland, Frederick Joseph, Case PF 37996 Volume 7, [British] National Archives, Kew, Richmond, UK, KV-2-333.

"Letter from American Embassy (Thurston) to British Security Service (Gibbs), dated 10 July 1943." Records of the [British] Security Service. Rutland, Frederick Joseph, Case PF 37996 Volume 10, [British] National Archives, Kew, Richmond, UK, KV-2-336.

"Memo Re: Frederick J. Rutland, dated 18 April 1942." Records of the [British] Security Service. Rutland, Frederick Joseph, Case PF 37996 Volume 8, [British] National Archives, Kew, Richmond, UK, KV-2-334.

"Notes Comparing MI5 Information to Rutland Confession, undated." Records of the [British] Security Service. Rutland, Frederick Joseph, Case PF 37996 Volume 5, [British] National Archives, Kew, Richmond, UK, KV-2-331.

Records of the [British] Security Service. Rutland, Frederick Joseph, Case PF 37,996 Volume 5, [British] National Archives, Kew, Richmond, UK, KV-2-331-092.

"Security Coordination Washington letter, dated 30 October 1941." Records of the [British] Security Service. Rutland, Frederick Jo-

seph, Case PF 37996 Volume 8, [British] National Archives, Kew, Richmond, UK, KV-2-334.

John S. Farnsworth. 1933–36. Former lieutenant commander, USN. A disgraced former naval aviator defense contractor who volunteered to spy for Japan for money. Arrested and served eight years in prison.

Alexander, John. "Spy." *Front Page Detective* (September 1937): 54–59, 106.

Booth, James. "Smashing the Japanese Spy Menace." *Real Detective* 40, no. 4 (June 1937): 28.

"Farnsworth, John S., Case No. 67865." Record Group 125: Records of the Office of the Judge Advocate General (Navy) Series: Card Index to U.S. Navy General Court Martial Files, File Unit Farm, 135–36, NAID: 117324283, National Archives and Records Administration, Washington, DC.

"John Semar Farnsworth." Washington, DC: Federal Bureau of Investigation, File # 65-632. Author's records received per FBI Freedom of Information Act no. 1158286.

Mangil, William. "Snaring Farnsworth: Betrayer of the Navy." *True Detective* 28, no. 5 (August 1937): 4–9, 80–86.

Christian F. Danielsen. 1936. Defense contractor, draughtsman, Bath Iron Works. Detained in 1938 as a material witness in a German espionage case. In 1972, he was accused of compromising *Farragut*-class destroyer designs in a questionable account of World War II German espionage.

"Bath Draftsman in Nazi Spy Case Testifies He Was Asked to Leave U.S." *Portland (ME) Press Herald*, 5 November 1938, 1.

"Bath Iron Works Notes and Gossip." *Bath* (*ME*) *Daily Times*, 11 April 1939, 4.

"Danielson Cleared of All Suspicion." *Bath* (*ME*) *Daily Times*, 8 November 1938, 8.

"Danielson Employed 18 Months at Bath." *Lewiston* (*ME*) *Daily Sun*, 4 June 1938, 4.

Farago, Ladislas. *The Game of Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II*. New York: David McKay, 1971.

History of the SIS Division. Washington, DC: Federal Bureau of Investigation, 1947.

"Interim Report in the Case of Erich Pheiffer." Appendix 21: "Some General Contacts of Korv. Kpt. Dr. Erich Pheiffer–Abwehr Officers: Agents: Other Contacts." Records of the [British] Security Service. Pheiffer, Erich, Case PF 46969 Volume 1," [British] National Archives, Kew, Richmond, UK, KV-2-267_4.

"Interim Report in the Case of Erich Pheiffer." Records of the [British] Security Service. Pheiffer, Erich, Case PF 46969 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-267_1.

"Office of Strategic Services Semi-Monthly Operations Report for 15–30 September 1945, dated 1 October 1945." Central Intelligence Agency, Langley, VA.

"Recent Books: The Game of the Foxes: The Untold Story of German Espionage in the United States and Great Britain During World War II, by Ladislas Farago." *Studies in Intelligence*. Record Group 263, Records of the Central Intelligence Agency, 1894–2002, Articles from "Studies in Intelligence," Fall 1972, 1955–1992. NAID: 7282944, National Archives and Records Administration, College Park, MD.

Snow, Ralph L. *Bath Iron Works: The First Hundred Years*. Portland, ME: Anthoensen Press, 1987.

"The City Record: Officials and Employees of the Departments, Bureaus and Offices of the City of New York and of the Counties

Contained Therein." 10, no. 11927. New York: City of New York, 31 July 1912.
"U.S. Navy in Europe." Naval History and Heritage Command, accessed 10 November 2023.

Gustav E. Guellich. 1934. Defense contractor metallurgist, Federal Shipbuilding and Drydock Company. Provided open-source information to Nazi Party authorities and was publicly denounced as a former Nazi Party member in 1946. In 1972, he was accused of compromising *Benham*-class destroyer designs in a questionable account of World War II German espionage.

Chemisches Zentralblatt [Chemical Central Journal] 2, no. 24. Berlin: Deutsche Chemische Gesellschaft, 1932.
Farago, Ladislas. *The Game of Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II*. New York: David McKay, 1971.
"Federal Shipbuilding and Drydock Company." Destroyer History Foundation, accessed April 2021.
"Four from Paterson Area Named as Nazis in Captured Records." *Paterson* (*NJ*) *Evening News*, 12 March 1946.
Gimbel, John. *Science, Technology, and Reparations: Exploitation and Plunder in Postwar Germany*. Stanford, CA: Stanford University Press, 1990.
———. "U.S. Policy and German Scientists: The Early Cold War." *Political Science Quarterly* 101, no. 3 (1986): 433–51.
Guellich, Gustav. "Process of Making Optical Devices." Patent 2,399,799, 7 May 1946.
Guellich, Gustav, and David Lowber. "Pantographic Sighting Apparatus for Forming Machines." Patent 2,553,099, 15 May 1951.
"Gustave E. Guellich, 47; Physicist and Engineer." *Buffalo* (*NY*) *Evening News*, 18 July 1953.

Mühlfriedel, Wolfgang, and Edith Hellmuth. "The Company's History of ZEISS—At a Glance." Zeiss International, 1996.

Nazi Party Membership Records, Submitted by the War Department to the Subcommittee on War Mobilization of the Committee on Military Affairs, United States Senate. Pt. 1. Washington, DC: Government Printing Office, 1946.

"NSDAP." European Holocaust Research Infrastructure Portal, accessed 10 November 2023.

"Recent Books: The Game of the Foxes: The Untold Story of German Espionage in the United States and Great Britain During World War II, by Ladislas Farago." *Studies in Intelligence*. Record Group 263, Records of the Central Intelligence Agency, 1894–2002, Articles from "Studies in Intelligence," Fall 1972, 1955–1992. NAID: 7282944, National Archives and Records Administration, College Park, MD.

Transactions of the American Institute of Mining and Metallurgical Engineers, Iron and Steel Division. Vol. 100. New York: American Institute of Mining and Metallurgical Engineers, 1932.

Harry T. Thompson. 1934–35. Former yeoman first class, USN. In 1934, wrote to the Japanese embassy volunteering to commit espionage. Stole classified information by impersonating a U.S. Navy yeoman.

Carlson, Elliot. *Joe Rochefort's War: The Odyssey of the Codebreaker Who Outwitted Yamamoto at Midway*. Annapolis, MD: Naval Institute Press, 2011.

"Re: Harry Thomas Thompson. Espionage. L.A. File 65-7, dated 14 December 1935." Washington, DC: Federal Bureau of Investigation, File # 65-615. Author's records received per FBI Freedom of Information Act no. 1158285.

"Sought: In Spy Plot." *Honolulu* (*HI*) *Advertiser*, 19 July 1936. 7.

Bernard J. O. Kuehn. 1935. Former German navy counterintelligence officer. An avowed Nazi recruited by Japanese naval intelligence to gather intelligence on the Hawaiian island of Oahu. Detained at the start of World War II and deported in 1948.

"Bernard Julius Otto Kuehn." Washington, DC: Federal Bureau of Investigation, File # 65-1574. Author's records.

"Exhibit 52 (Confinement of Bernard Julius Otto Kuehn)." Files Relating to Hearings and Investigations, 1944–45, Records of the War Department General and Special Staffs, 1860–1952, Record Group 165, National Archives and Records Administration, College Park, MD.

Fiehn, John. "Widow of Man Convicted as P.H. Spy Sues U.S." *Honolulu* (*HI*) *Star Bulletin*, 24 July 1962, 1.

Kotani, Ken. *Japanese Intelligence in World War II*. New York: Osprey, 2009.

Norwood, Ryan. "None Dare Call It Treason: The Constitutionality of the Death Penalty for Peacetime Espionage." *Cornell Law Review* 87, no. 3 (March 2002): 820–52.

Maximilian G. Waldemar Othmer. 1936. Defense contractor construction worker. An avowed Nazi recruited by German naval intelligence to spy on U.S. and British naval activities on the east coast of the United States. Reported from Norfolk, VA, 1940–41 (and possibly 1943). Arrested in 1944 and served approximately seven years.

"Bund Meeting Given Approval at Trenton." *Morning Post* (Camden, NJ), 25 March 1938.

"Chronological Survey, Derived from War Room Sources, on Johannes Bischoff." Records of the [British] Security Service. Bischoff, Johannes W., Case PF 601785 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-2749.

"Congressman Samuel Dickstein (D-NY) Speaking about Un-American Activities." 75th Cong., 1st Sess. *Congressional Record* (1937): 8150.

"Denaturalization Suit against Othmer Dropped." *Knoxville* (*TN*) *Journal*, 29 September 1944, 12.

"Dickstein Names Nazi 'Agitators'." *Asbury Park* (*NJ*) *Press*, 4 August 1937.

"Families Cherish Traditions for Keeping the Christmas." *Richmond* (*VA*) *Times Dispatch*, 18 December 1955, 8C.

"Former Bund Leader Is Arrested Here by FBI as Suspected Spy." *Knoxville* (*TN*) *News-Sentinel*, 20 July 1944, 1.

"German-born U.S. Citizen, Spy against Britain Here, Othmer Sentenced to 20 Years in Prison." *Norfolk Virginian-Pilot*, 1 August 1944.

History of the SIS Division. Washington, DC: Federal Bureau of Investigation, 1947.

"Interim Report in the Case of Erich Pheiffer." Appendix 21: "Some General Contacts of Korv. Kpt. Dr. Erich Pheiffer–Abwehr Officers: Agents: Other Contacts." Records of the [British] Security Service. Pheiffer, Erich, Case PF 46969 Volume 1," [British] National Archives, Kew, Richmond, UK, KV-2-267_4.

Neely, Jack. "The Night the FBI Collared a Nazi Spy at the YMCA." *Knoxville* (*TN*) *Mercury*, 29 July 2015.

"One-Time Nazi Bund Leader, Former Richmonder, Arrested." *Richmond* (*VA*) *Times Dispatch*, 21 July 1944, 11.

"Othmer Given 20-Year Term on Charges of Espionage." *Richmond* (*VA*) *Times Dispatch*, 1 August 1944, 7.

Othmer, Siegfried. "Stranger in the South." *Medium*, 22 August 2018.

"Re: Dr. Carl Hermann Nicolaus Bensmann; May 4, 1945." Records of the [British] Security Service. Bischoff, Johannes W., Case PF 601785 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-2749.

"Summary of Information Obtained from Bischoff." Records of the [British] Security Service. Bischoff, Johannes W., Case PF 601785 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-2749.

"Waldemar Othmer." Washington, DC: Federal Bureau of Investigation, File # 100-30234. Author's records received per National Archives and Records Administration Freedom of Information Act no. RD 781276.

Woodward, Bob. *The Secret Man: The Story of Watergate's Deep Throat*. New York: Simon & Schuster, 2005.

Hafis Salich. 1937–38. Office of Naval Intelligence civilian investigator. Former citizen of the Soviet Union. Coerced to provide intelligence about Japanese-Americans to Soviet intelligence. Arrested and served less than three years, released, and then served in the U.S. Army during World War II. Granted amnesty in 1946.

"Convicted Spy Wins Amnesty for War Duty." *Los Angeles Times*, 8 June 1946, 1.

"Defense Issue to Be Defined." *Los Angeles Times*, 27 February 1939, 4.

Maximenkov, Leonid, and Christopher Barnes. "Boris Pasternak in August 1936: An NKVD Memorandum." *Toronto Slavic Quarterly* (Fall 2019).

"Navy Officers to Testify in Trio's Espionage Trial." *Los Angeles Times*, 23 February 1939. 6.

"Russian Convicted Here as Spy Files Plea for Probation." *Los Angeles Times*, 21 March 1939, 14.

"Russians Convicted as Spies; Wife of One Acquitted by Jury." *Los Angeles Times*, 11 March 1939, 1.

"Russians Go on Trial as Spies; Sale of Navy Secrets Charged." *Los Angeles Times*, 22 February 1939, 1.

"Sabotage Plot Laid to Japan." *Los Angeles Times*, 2 March 1939, 1.

"Spy Case Appeal Contends Data Sold Russia Not Vital." *Los Angeles Times*, 16 February 1940, 12.
"Spy Suspect Tells of Deals." *Los Angeles Times*, 1 March 1939, 2.
Testimony of Ismail Ege before the U.S. Senate Committee on the Judiciary. In *Interlocking Subversion in Government Departments*, pt. 15. Washington, DC: Government Printing Office, 1953.
Young, James. "State Department Appeasement Freed Convicted Russian Spy." *Miami* (*FL*) *News*, 29 March 1946, 15-A.
Zacharias, Capt Ellis M., USN. *Secret Missions: The Story of an Intelligence Officer*. New York: Van Rees Press, 1946.

Karl A. Drummond. 1938. Defense contractor, El Segundo Division of the Douglas Aircraft Company. Stole plans for a U.S. Navy dive bomber prototype and tried to sell them to Japanese intelligence. Arrested and served two years.

"Aircraft Worker Accused as Spy." Associated Press, 1 December 1938.
"Karl Allen Drummond." Washington, DC: Federal Bureau of Investigation, File # 65-1080. Author's records received per FBI Freedom of Information Act no. 1158287.

Simon Emil Koedel. 1939–41 (and possibly 1943). A former U.S. Army noncommissioned officer and German army captain. Volunteered to spy for Germany in New York by mail. Arrested in 1944 and sentenced to 15 years. Assisted by his foster daughter, Marie, who was also arrested and sentenced to seven and a half years.

"Daughter Denies Spying with Father, Is Held on Bail." *Richmond* (*VA*) *Times-Dispatch*, 24 October 1944.
"Exhibit List." Records of the [British] Security Service. Bischoff, Johannes W., Case PF 601785 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-2749.

"German Ex-Officer Held as Nazi Spy." *New York Times*, 24 October 24, 1944.

"Girl Denies Spying, Held in $25,000 Bail on U.S. Charge." *St. Louis* (*MO*) *Globe-Democrat*, 24 October 1944.

History of the SIS Division. Washington, DC: Federal Bureau of Investigation, 1947.

"Interim Report in the Case of Erich Pheiffer." Appendix 21: "Some General Contacts of Korv. Kpt. Dr. Erich Pheiffer–Abwehr Officers: Agents: Other Contacts." Records of the [British] Security Service. Pheiffer, Erich, Case PF 46969 Volume 1," [British] National Archives, Kew, Richmond, UK, KV-2-267_4.

"Interim Report in the Case of Erich Pheiffer." Records of the [British] Security Service. Pheiffer, Erich, Case PF 46969 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-267_1.

"Koedel Halts Spy Plot Trial to Plead Guilty." *Brooklyn* (*NY*) *Daily Eagle*, 15 February 1945.

"Koedel Receives Term of 15 Years as Spy." *Evening Star* (Washington, DC), 1 March 1945, B1.

"Summary of War Room Traces in PT/601785." Records of the [British] Security Service. Bischoff, Johannes W., Case PF 601785 Volume 1, [British] National Archives, Kew, Richmond, UK, KV-2-2749.

Takeo Yoshikawa. 1940–41. Ensign, Imperial Japanese Navy. A former naval aviator and U.S. Navy specialist in Japanese naval intelligence. Dispatched under diplomatic cover to Oahu, HI, to report order of battle and movement information for the U.S. Pacific Fleet. Detained at the start of World War II and repatriated in 1942.

Cook, Lynn. "Teahouse of Intrigue." *HanaHou!: The Magazine of Hawaiian Airlines* (August/September 2011).

Deac, Wil. "Takeo Yoshikawa: World War II Japanese Pearl Harbor Spy." *World War II* (May 1997).

Laytner, Ron. "The Rising Sun Never Shines for Pearl Harbor Spy." *Chicago Tribune*, 1 December 1979, 13.
Naylor, Roger. "Pearl Harbor Spy Was Detained at Triangle T Ranch." Azcentral, 17 July 2015.
Prange, Gordon. *At Dawn We Slept: The Untold Story of Pearl Harbor*. New York: Penguin, 1981.
Stinnett, Robert B. *Day of Deceit*. New York: Touchstone, 2000.
Yoshikawa, Takeo, with LtCol Norman Stanford, USMC. "Top Secret Assignment." U.S. Naval Institute *Proceedings* 86, no. 12 (December 1960).

Velvalee M. Dickinson. 1941. Civilian. A Japanophile recruited by the Japanese naval attaché in Washington, DC, to provide post-Pearl Harbor battle damage assessment information to Japanese naval intelligence after the start of World War II. Arrested in 1944 and pled guilty to violating censorship laws. Served six years.

"Velvalee Dickinson." Washington, DC: Federal Bureau of Investigation, File # 65-11186. Author's records received per FBI Freedom of Information Act no 1158288.

Nelson C. Drummond. 1957–62. Yeoman first class, USN, U.S. Naval Forces Eastern Atlantic and Mediterranean in London. Volunteered to Soviet intelligence for money. Later, in Newport, RI, compromised dozens of weapon and sensor systems.

Blakemore, Erin. "The Spy Who Kept the Cold War from Boiling Over." History Channel, 15 July 2019.
"Drummond Gets Life Sentence." *Baltimore* (*MD*) *Sun*, 16 August 1963, 7.
"Drummond, Nelson Cornelious." Office of Naval Intelligence, 1971. Cited portion declassified by the Naval Criminal Investigative

Service (NCIS) per NCIS Memo 3850 Ser 22/21U0253 dated 19 August 2021.
Espionage. Washington, DC: Naval Investigative Service, 1989.
FBI Annual Report, Fiscal Year 1964. Washington, DC: Federal Bureau of Investigation, 1964.
Guide for Security Orientation, Education and Training. Washington, DC: Office of Naval Intelligence, 1965.
Haslam, Jonathan. *Near and Distant Neighbors: A New History of Soviet Intelligence*. New York: Farrar, Straus and Giroux, 2015.
Huss, Pierre J., and George Carpozi Jr. *Red Spies in the UN*. New York: Coward-McCann, 1965.
"United States, Appellee, v. Nelson Cornelious Drummond, Appellant, 354 F.2d 132 (2d Cir. 1965)." U.S. Court of Appeals for the Second Circuit, 26 May 1965.

Gary L. Ledbetter. 1967. Shipfitter second class, USN, USS *Simon Lake* (AS 33). Sold part of a nuclear submarine maintenance manual to a British national, who sold it on to East German national Peter Dorschel, a Soviet military intelligence asset placed in Scotland to observe U.S. ballistic missile submarine (SSBN) order of battle and movements. Court martialed and served six months. Charges against the British national were dropped, but Dorschel pled guilty in British court, served three years, and was then deported.

"Charge under Secrets Act Dropped." *Guardian*, 6 September 1967, 3.
"Couple Wed in Woodlawn EUB Church." *Bucyrus* (*OH*) *Telegraph-Forum*, 23 March 1961, 4.
"Deck Log Book, USS *Simon Lake* (AS 33) 1–31 August 1967." Record Group 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Simon Lake* (AS 33)–August 1967, NAID: 215545799, National Archives and Records Administration, College Park, MD.

"Deck Log Book, USS *Simon Lake* (AS 33) 1–31 July 1966." Record Group 24: Records of the Bureau of Naval Personnel, Series: Logbooks of U.S. Navy Ships and Stations, File Unit: *Simon Lake* (AS 33)–July 1966, NAID: 215129454, National Archives and Records Administration, College Park, MD.

"Dorschel Gives Evidence in Camera." *Guardian*, 25 August 1967, 16.

"E. German Gets 7 Yrs. as Polaris Sub Spy." *Evening Journal*, 23 June 1967, 26.

Houghton, Harry. "I Betrayed My Country—And the Woman I Love: The Lonsdale Spy Ring." *Ottawa* (*ON*) *Citizen*, 9 September 1961, 41.

"MacAffer Says He Spied for Britain and U.S." *Glasgow* (*UK*) *Herald*, 6 September 1967, 7.

"Midnight Questions on Polaris." *Guardian*, 26 August 1967, 12.

"Notice for Service of Summons by Publication in Common Pleas Court of Crawford County, Ohio." *Bucyrus* (*OH*) *Telegraph-Form*, 2 December 1967, 11.

"Sailor Denies Anti-Security Allegations." *Arizona Daily Star*, 25 August 1967, 15.

"Seven Years for 'Little Fish' Spy." *Guardian*, 24 June 1967, 3.

"Spy's Wife Awarded Decree." *Guardian*, 23 October 1970, 7.

"U.S. Sailor Convicted of Charge." *Daily Herald* (Provo, UT), 27 August 1967.

John A. Walker. 1967–85. Chief warrant officer, USN, Commander Submarine Forces Atlantic. For 17 years, compromised to Soviet intelligence the encryption system used for U.S. Navy radio communications in exchange for money. Recruited his brother, son, and shipmate to assist. The single worst espionage case in U.S. Navy history. Arrested, sentenced to life, and died in prison in 2014. His son served 15 years. His brother was also sentenced to life and died in prison. His shipmate is serving a life sentence.

"Convicted U.S. Spy Arthur Walker Dies in Prison." Associated Press, 10 July 2014.

Earley, Pete. *Family of Spies: Inside the John Walker Spy Ring*. New York: Bantam Books, 1988.

———. "Interview with the Spy Master." *Washington Post*, 23 April 1995,

Espionage. Washington, DC: Naval Investigative Service, 1989.

"Find an Inmate: Jerry Alfred Whitworth." Bureau of Prisons, accessed 25 February 2021.

"Find an Inmate: Michael Lance Walker." Bureau of Prisons, accessed 25 February 2021.

Heath, Maj Laura J., USA. "An Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967–1974, as Exploited by CWO John Walker." Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2005.

"A History of U.S. Communications Security Post World War II." Washington, DC: National Security Agency, 77–82.

"John Walker." Federal Bureau of Investigation, accessed 2 September 2023.

Poole, Robert. *Explorer's House: National Geographic and the World It Made*. New York: Penguin, 2004.

"Property of Convicted Spy to Be Sold at Public Auction." *Index Journal* (Greenwood, SC), 5 February 1987, 17.

Toth, Robert C. "Change in Soviets' Sub Tactics Tied to Spy Case." *Los Angeles Times*, 17 June 1985.

"Walker with Wilkinson." Associated Press, 1965.

Weil, Martin. "John A. Walker Jr., Who Led Family Spy Ring, Dies at 77." *Washington Post*, 30 August 2014.

West, Nigel. *Historical Dictionary of Cold War Counterintelligence*. Lanham, MD: Scarecrow Press, 2007.

"Whitworth Gets 365 Years—Eligible for Parole in 60: 'I'm Sorry,' Navy Spy Tells Judge." *Los Angeles Times*, 28 August 1986.

Wilson, George C. "Soviet Submarines 'Have Closed the Gap.'" *Washington Post*, 3 April 1987.

Edward H. Wine. 1968. Sonar technician first class, USN, USS *Skate* (SSN 578). Conspired but failed to compromise classified notes to Soviet intelligence. Court-martialed for mishandling classified information, served one year, and returned to active duty.

"Brothers Held in Grill Fight." *Hartford* (*CT*) *Courant*, 22 December 1964, 3.

Espionage. Washington, DC: Naval Investigative Service, 1989.

Failla, Thomas. "Tipster Has Troubles." *Daily Times-Mail* (Bedford, IN), 13 November 1974, 21.

Gombossy, George, and Paul Frisman. "Ex-Husband Cleared in Double Strangling." *Hartford* (*CT*) *Courant*, 19 October 1974, 10.

Healion, James. "Navy Petty Officer Denies Any Intention of Selling Secrets." *Naugatuck* (*CT*) *Daily News*, 24 March 1969, 5.

"State Sailor Is Serving Term for 'Mishandling' Secret Data." *Bridgeport* (*CT*) *Post*, 24 March 1969, B IX.

Lee E. Madsen. 1979. Yeoman third class, USN, Defense Intelligence Agency. Conspired but failed to compromise classified information to narcotics traffickers for money. Pled guilty to violating the Espionage Act and served four years.

"Ex-Security Guard at Pentagon Gets Eight Years for Espionage." *Miami* (*FL*) *Herald*, 27 October 1979, 18-A.

"Find an Inmate: Lee Eugene Madsen." Bureau of Prisons, accessed 24 February 2021.

"Man Gets 8 Years for Espionage." *Tampa Bay* (FL) *Times*, 27 October 1979, 3A.

Mansfield, Stephanie. "Sailor Accused of Espionage Wanted to 'Buy Things'." *Washington Post*, 16 August 1979.
Meyers, Robert. "Sailor Receives 8 Years in Jail for Espionage." *Washington Post*, 27 October 1979.
"Pentagon Is Unnerved by Spying Indictment." *Daily Advertiser* (Lafayette, LA), 16 August 1979, 10.
"Sold Secrets." *Daily News* (Lebanon, PA), 16 August 1979, 60.

Glenn M. Souther. 1980. Photographer's mate first class, USN, Sixth Fleet and Fleet Intelligence Center, Europe and Atlantic. Volunteered to spy for Soviet intelligence while stationed in Italy. Compromised unknown amounts of information and, when detected, fled to the Soviet Union, where he later committed suicide.

"A Recruiting Virtuoso." *Nezavisimoye Voyennoye Obozreniye* [Independent Military Review], 2 June 2006.
Earley, Pete. "Interview with the Spy Master." *Washington Post*, 23 April 1995.
Haslam, Jonathan. *Near and Distant Neighbors: A New History of Soviet Intelligence*. Oxford, UK: Oxford University Press, 2015.
Kessler, Ronald. *The Spy in the Russian Club*. New York: Charles Scribner's Sons, 1990.
Rafalko, Frank, ed. *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century*. Washington, DC: National Counterintelligence Center, 1998.

Stephen A. Baba. 1981. Ensign, USN, USS *Lang* (FF 1060). Volunteered to spy for South Africa for money. Reported by the South Africans. Court-martialed and served two years.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney.

Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

" 'Brilliant' Naval Officer Faces Spying Charges." *Arizona Daily Star*, 22 December 1981, A7.

"Ensign Receives 8-year Sentence." *St. Joseph* (*MO*) *Gazette*, 21 January 1982, 6A.

Espionage. Washington, DC: Naval Investigative Service, 1989.

Ray, Nancy. "Ensign Pleads Guilty to Disclosing Secrets; Navy Officer Asks Forgiveness in Case Tied to a Love Affair in the Philippines." *Los Angeles Times*, 20 January 1982, CC/Part II, 1.

Brian P. Horton. 1982. Intelligence specialist second class, USN, Fleet Intelligence Center, Europe and Atlantic. Contacted Soviet intelligence and attempted to compromise classified information. Court-martialed and sentenced to six years.

Counterintelligence and National Security Information: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-Ninth Congress, First Session, June 17, 1985. Washington, DC: Government Printing Office, 1985.

Department of Defense Appropriations for 1986: Hearing before a Subcommittee of the Committee on Appropriations, House of Representatives, Ninety-Ninth Congress, First Session, pt. 4. Washington, DC: Government Printing Office, 1985.

Espionage. Washington, DC: Naval Investigative Service, 1989.

Rafalko, Frank, ed. *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century*. Washington, DC: National Counterintelligence Center, 1998.

Smith, Philip. "Sailor Sentenced after Bid to Sell Plans to Soviets." *Washington Post*, 14 January 1983.

Wise, David. "The FBI's Fake Russian Agent Reveals His Secrets." *Smithsonian Magazine*, November 2016.

Brian E. Slavens. Private first class, USMC, Marine Security Force, Adak, AK. Deserted and approached Soviet intelligence for money but was turned away. Court-martialed and served 18 months.

Counterintelligence and National Security Information: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-Ninth Congress, First Session, June 17, 1985. Washington, DC: Government Printing Office, 1985.

Franklin, Ben. "Lonetree Will Fault Sentence by Citing Earlier Spy Cases." *Advocate-Messenger* (Danville, KY), 30 August 1987, 5.

Rafalko, Frank, ed. *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century*. Washington, DC: National Counterintelligence Center, 1998.

Hans P. Wold. 1983. Intelligence specialist third class, USN, USS *Ranger* (CV 61). Deserter who photographed a classified document with a vague intention of compromising it to Soviet intelligence in exchange for money. Caught before he could make the attempt. Pled guilty and served just under two years.

Counterintelligence and National Security Information: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-Ninth Congress, First Session, June 17, 1985. Washington, DC: Government Printing Office, 1985.

Espionage. Washington, DC: Naval Investigative Service, 1989.

WESTPAC '82: 25 Years for Freedom. USS *Ranger* (CV 61), 1982.

Alan D. Coberly. 1983. Private first class, USMC, 3d Battalion, 1st Marine Regiment. Deserter who visited the Soviet embassy in Manila, the Philippines, to attempt to commit espionage to fund his return to the United States. He was rejected. Detained as a deserter after arrival in the United States, which revealed incriminating information. Pled guilty to desertion and sentenced to 18 months.

Department of Defense Appropriations for 1986: Hearing before a Subcommittee of the Committee on Appropriations, House of Representatives, Ninety-Ninth Congress, First Session, pt. 4. Washington, DC: Government Printing Office, 1985.

Jeffery L. Pickering. 1983. Hospital corpsman, USN, USS *Fanning* (FF 1076). Stole unsecured classified microfiche and attempted to sell it to Soviet intelligence. Spontaneously confessed. Pled guilty and sentenced to five years.

"Man Charged in Clinton Bomb Threat." *Albany* (*OR*) *Democrat-Herald*, 16 October 1998, A4.

"Man Sentenced for Clinton Threat." Associated Press, 7 June 2000.

"A Navy Hospital Corpsman Who Said He Stole 'Out of Curiosity." United Press International, 4 October 1983.

"Phony Vet, Would-be Assassin Given Increased Prison Term." *Army Times*, 11 May 2001.

Rafalko, Frank, ed. *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century*. Washington, DC: National Counterintelligence Center, 1998.

Robert W. Ellis. 1983. Aviation antisubmarine warfare operator second class, USN, Patrol Squadron 46, Naval Air Station (NAS) Moffett

Field, CA. Attempted to sell classified information to Soviet intelligence. Intercepted by an FBI undercover operation. Pled guilty to unauthorized disclosure of classified information and sentenced to three years.

Department of Defense Appropriations for 1986: Hearing before a Subcommittee of the Committee on Appropriations, House of Representatives, Ninety-Ninth Congress, First Session, pt. 4. Washington, DC: Government Printing Office, 1985.

Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008. Monterey, CA: Defense Personnel Security Research Center, 2009.

Mickolus, Edward. *The Counterintelligence Chronology: Spying by and against the United States from the 1700s through 2014*. Jefferson, NC: McFarland, 2015.

Robert E. Cordrey. Private, USMC, Nuclear, Biological and Chemical Defense School, Fleet Marine Force, Atlantic. Contacted the Soviet, Czechoslovakian, Polish, East German, and West German embassies in a bid to sell unclassified official documents and manuals. Met a Czechoslovakian intelligence officer. Pled guilty to failing to report contacts with a citizen of a Communist-controlled country.

Counterintelligence and National Security Information: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-Ninth Congress, First Session, June 17, 1985. Washington, DC: Government Printing Office, 1985.

Department of Defense Appropriations for 1986: Hearing before a Subcommittee of the Committee on Appropriations, House of Representatives, Ninety-Ninth Congress, First Session, pt. 4. Washington, DC: Government Printing Office, 1985.

"Family Court, Sussex County [Delaware]: Divorce Decrees." *Morning News* (Wilmington, DE), 19 April 1985, B8.
Hager, Jerry. "State Marine Guilty of Trying to Sell Info." *Morning News* (Wilmington, DE), 9 January 1985, A1.
"Marine Gets 12 Years at Spy Court-Martial." *New York Times*, 10 January 1985.

Samuel L. Morison. Civilian employee, Naval Intelligence Support Center. Compromised classified information to a journalist. Convicted of espionage and served eight months. Later pardoned.

"The Dark Side of Moonlighting." In *Security Awareness in the 1980s*, 81–92. Richmond, VA: Department of Defense Security Institute, 1989.
Duncan, Ian. "Navy Veteran Accused of Stealing from Files of Famed Historian Grandfather." *Baltimore* (*MD*) *Sun*, 10 June 2014.
Gresko, Jessica. "Man Once Convicted of Spying Pleads Guilty to Naval Archive Document Theft." *Navy Times*, 12 March 2015.
"Pardon: Samuel Loring Morison—Collection Finding Aid." Clinton Digital Library, accessed 23 January 2024.

Michael T. Tobias. 1984. Radioman third class, USN, USS *Peoria* (LST 1183). Attempted to compromise cryptographic material to Soviet intelligence for money. When he was unable to contact the Soviets, he, his cousin, and two others attempted to sell the material back to the U.S. government. Unable to fully account for all the material, he was ineligible for a plea arrangement. Stood trial, was convicted, and served 12 years.

"2 More Are Accused of Theft of Navy Codes." *New York Times*, 25 August 1984, 1.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

"Chula Vistans Arrested in Navy Code Card Stealing." *Imperial Beach* (*CA*) *Star-News*, 30 August 1984, B-3.

Espionage. Washington, DC: Naval Investigative Service, 1989.

"Espionage Raps Pend in Decoder Case." *Petaluma* (*CA*) *Argus-Courier*, 24 August 1984, 2A.

"Navy Man Guilty of Code Thefts." *San Bernardino County (CA) Sun*, 15 August 1985, A-9.

Olive, Ronald J. *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice*. Annapolis, MD: Naval Institute Press, 2006.

Rafalko, Frank, ed. *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century*. Washington, DC: National Counterintelligence Center, 1998.

"Suspect Pleads Guilty in Theft of Code Cards." *Sacramento (CA) Bee*, 8 August 1985, B10.

"United States, Plaintiff-Appellee v. Michael Tobias." U.S. Court of Appeals, Ninth Circuit, 6 January 1988.

Jay C. Wolff. Former storekeeper, helmsman, and planesman, USN, USS *Rayburn* (SSGN 635). While awaiting a general discharge for drug violations, stole classified information which he later attempted to sell to an FBI undercover agent. Arrested and served three years.

"Find an Inmate: Jay Wolff." Bureau of Prisons, accessed 17 February 2021.

Nathanson, Rick. "Gallup Man Charged with Selling Classified Papers." *Albuquerque (NM) Journal*, 18 December 1984, B2.
"Navy Concerned about Theft Motivation." *Journal Herald* (Dayton, OH), 12 March 1986, 28NS.
"N.M. Man Guilty of Selling Secrets." *Albuquerque (NM) Journal*, 18 May 1985, 14.
Pagano, Rosanne. "Man Sentenced for Selling Classified Papers." *Albuquerque (NM) Journal*, 29 June 1985, 21.
Ripp, Bart. "Secrets on Sale in Albuquerque?." *Albuquerque (NM) Tribune*, 8 February 1985, 1.
Sarbin, Theodore R., Ralph M. Carney, and Carson Eoyang, eds. *Citizen Espionage: Studies in Trust and Betrayal*. Westport CT: Praeger, 1994.

Jonathan J. Pollard. 1984–85. Civilian employee, Office of Naval Intelligence and Naval Investigative Service. Compromised hundreds of highly classified intelligence publications to Israeli intelligence for ideological reasons. Pled guilty to espionage, served 30 years, and was released in 2015.

Gotkine, Elliot. "Jonathan Pollard, Spy Who Passed U.S. Secrets to Israel, Arrives in Jewish State to Start New Life." CNN, 30 December 2020.
"The Jonathan Jay Pollard Espionage Case: A Damage Assessment." Langley, VA: Central Intelligence Agency, 30 October 1987.
"Letter from Attorney General Janet Reno to President Clinton." Records of the Office of the Counsel to the President (Clinton Administration), Series: Mary Smith's Files, File Unit: Pollard, [Jonathan], NAID: 40435991, William J. Clinton Library, Little Rock, AR.

"Notes on April 1976 South African Visit to Israeli Scientific and Technical Intelligence Organization (LAKAM)." Wilson Center Digital Archive, June 1976.

Olive, Ronald J. *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice*. Annapolis, MD: Naval Institute Press, 2006.

Raviv, Dan, and Yossi Melman. *Every Spy a Prince: The Complete History of Israel's Intelligence Community*. Boston, MA: Houghton Mifflin, 1989.

Chi Mak. 1985–2005, possibly as early as the 1960s. Defense contractor engineer. Recruited by People's Republic of China (PRC) military intelligence to whom he provided sensitive but unclassified technical information. Found guilty of conspiracy, attempting to violate export control laws, failing to register as a foreign agent, and lying to federal investigators and was sentenced to 24.5 years.

Bhattacharjee, Yudhijit. "How the F.B.I. Cracked a Chinese Spy Ring." *New Yorker*, 12 May 2014.

Gertz, Bill. "Enemies." *Washington Times*, 18 September 2006.

Roche, Edward M. *Snake Fish: The Chi Mak Spy Ring*. New York: Barraclough, 2008.

"United States, Plaintiff, v. Chi Mak et al." U.S. District Court for the Central District of California, October 2005.

Clayton J. Lonetree. 1985–86. Sergeant, USMC, U.S. Marine Security Guard Detachment, Moscow, Russia. Entrapped by Soviet counterintelligence, compromised the identities and activities of U.S. intelligence personnel in the U.S. embassy. Spontaneously confessed and served nine years.

Barker, Rodney. *Dancing with the Devil: Sex, Espionage, and the U.S. Marines: The Clayton Lonetree Story*. New York: Simon & Schuster, 1996.

"Marine to Leave Prison, but He Won't Shed Legacy." *Deseret News* (Salt Lake City, UT), 25 February 1996.

Oberdorfer, Don. "Spy Scandal Snowballed, Melted Away." *Washington Post*, 17 January 1988.

Rempel, William. " 'He Was Walter Mitty,' Lawyer Says: Accused Marine Spy Lived out Fantasy." *Los Angeles Times*, 16 April 1987.

Wilfredo M. Garcia. 1985–87. Master-at-arms first class, USN, Mare Island Naval Shipyard, Vallejo, CA. Attempted to sell classified information that he stole from unsecured spaces. The middleman who was intended to sell the information to Soviet intelligence instead reported Garcia to the FBI. Pled guilty and served seven years.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

Norwitz, Jeff. "Operation Touchdown: The Story of the Wilfredo Garcia Espionage Case." *NCIS Gold Shield*, May 2013.

Robert D. Haguewood. 1986. Aviation ordnanceman third class, USN, Pacific Missile Test Center, Point Mugu, CA. Attempted to sell part of what he believed to be a classified document to an undercover police officer. Pled guilty to mishandling documents and was sentenced to two years.

Corwin, Miles. "Petty Officer Arrested in Sale of Secret Documents." *Los Angeles Times*, 11 March 1986.
"Debt-driven Sailor Admits Selling Government Papers." *Santa Cruz (CA) Sentinel*, 20 June 1986, A-14.
"Espionage Case Charge Reduced." *Albuquerque (NM) Journal*, 19 June 1986, C10.
"Navy Man Gets 2-year Sentence for Selling 'Secret' Documents." (Spokane, WA) *Spokesman-Review*, 20 June 1986.
"The Region: UCLA Bone Marrow Surgeon Honored." *Los Angeles Times*, 20 June 1986, 2.

Michael H. Allen. 1985. Retired senior chief radioman and civilian photocopy clerk in the Navy Telecommunications Center at NAS Cubi Point, Philippines. Compromised classified intelligence reports to Philippine security officials to facilitate private business ventures.

"Caught by Candid Camera: The Case of Michael Allen." In *Security Awareness in the 1980s*, 95–97. Richmond, VA: Department of Defense Security Institute, 1989.
Evje, Mark. "Trial Begins for Navy Man Charged with Espionage." United Press International, 5 August 1987.
Gutierrez, Hector. "Bid to Move Military Spy Case to Civilian Court Fails." *Los Angeles Times*, 7 April 1987, pt. 2, 2.
Schachter, Jim. "Linked to Filipinos: Ex-Navy Man Found Guilty on 10 Spy Charges." *Los Angeles Times*, 15 August 1987.

James R. Wilmoth and **Russell P. Brown**. 1988–89. Airman recruit and electronic warfare technician seaman, USN, USS *Midway* (CVN 41). Attempted to compromise classified information to Russian intelligence. Pled guilty to attempted espionage and conspiracy to transfer classified information, failure to report contact with a Soviet, and distribution and possession of hashish.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

"Court Convicts Nebraskan for Selling Military Secrets: Navy Airman Gets 35 years in Prison." *Lincoln (NE) Journal Star*, 5 October 1989, 15.

Schafer, Susanne. "Second Nebraska Sailor Convicted of Espionage." Associated Press, 26 October 1989.

"United States v. James R. Wilmoth, Airman Recruit (E-1), U.S. Naval Reserve." U.S. Navy–Marine Corps Court of Military Review, 23 December 1991.

Randall S. Bush. 1988. Radioman, USN (rank and duty station unknown). Attempted to compromise classified counternarcotics intelligence to an undercover agent he believed to be a narcotics trafficker. Served 13 years.

"Espionage." Naval Criminal Investigative Service, 1995, video.

Espionage. Washington, DC: Naval Investigative Service, 1989.

"Find an Inmate: Randall Bush." Bureau of Prisons, accessed 14 May 2020.

Rafalko, Frank, ed. *A Counterintelligence Reader*, vol. 3, *Post-World War II to Closing the 20th Century*. Washington, DC: National Counterintelligence Center, 1998.

Craig D. Kunkle. 1988. Civilian security guard, former aviation antisubmarine warfare operator chief, USN. Discharged under less-than-honorable conditions and attempted to compromise classified

notes recounted from memory to Soviet intelligence. Pled guilty and served 10 years.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

Ashley, Douglas. "Spy Suspect Asks Judge to Move Trial from Area." *Daily Press* (Newport News, VA), 27 January 1989, B4.

Becker, Robert. "Information Could Have Helped Soviet Subs." *Daily Press* (Newport News, VA), 11 January 1989. A6.

Cook, Nancy. "Beach Man Charged with Espionage. Sting Yields Documents on Sub Tracking." *Daily Press* (Newport News, VA), 11 January 1989, 1.

"Ex-sailor Arrested in Bid to Sell Secrets: Calls to Soviet Embassy Monitored." *Pittsburgh (PA) Post-Gazette*, 11 January 1989, 1.

Miller, Michell. "Former Seaman Pleads Guilty to Espionage Charge." United Press International, 4 May 1989.

Wise, David. "The FBI's Fake Russian Agent Reveals His Secrets." *Smithsonian Magazine*, November 2016.

Donald W. King and **Ronald D. Graf**. 1989. Both aviation storekeeper airmen, USN, Patrol Squadron 94, NAS Belle Chase, New Orleans, LA. Attempted to sell aircraft parts, including classified parts, to an undercover agent. Pled guilty to espionage and sentenced to 10 and 5 years, respectively.

"2 at New Orleans Base Accused of Espionage." *New York Times*, 6 March 1989.

"Abilenian Arrested, Accused of Espionage." *Abilene (TX) Reporter-News*, 11 March 1989, 12.
"Grand Island Man Accused of Trying to Sell Data on Bombers." *Lincoln (NE) Star*, 11 March 1989, 17.
"Navy Accuses 2 of Espionage, Theft." *Sacramento (CA) Bee*, 5 March 1989, A5.
"Navy Airmen Sentenced in Spy Case." United Press International, 7 July 1989.

Frank A. Nesbitt. 1989. Former chief warrant officer, USMC, 1st Radio Battalion/unemployed. While traveling in Latin America after abandoning his family and job, volunteered to compromise his dated knowledge of the U.S. signals intelligence system to Soviet intelligence for money. Spontaneously confessed upon his return. Pled guilty and served 10 years in a psychiatric facility.

"15 SNCO's Selected for DCP." *Marine Corps Gazette* 59, no. 8 (August 1975): 2.
"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.
"Arrested Would-be Spy Says He Wanted to Cross Soviets." *Palm Beach (FL) Post*, 16 October 1989, 5A.
Congressional Record–Senate, August 25–September 12, 1978, vol. 124, pt. 21. Washington, DC: Government Printing Office, 1978.
"Find an Inmate: Frank Arnold Nesbitt." Bureau of Prisons, accessed 18 May 2020.

"Frank Arnold Nesbitt, Petitioner, v. United States of America, Respondent." U.S. District Court for the Eastern District of Virginia, 6 September 1991.

"Germany Is First Residence." *Fresno (CA) Bee Republican*, 12 October 1965, 15-A.

"K-Bay Salutes." *Windward Marine*, 11 June 1971, 6.

Memorandum for the Honorable Charles F.C. Ruff, Counsel to the President. "Recommended Denials of Executive Clemency—16 Petitions for Commutation Sentence." Washington, DC: Department of Justice Pardon Attorney, 19 March 1997.

"Recruiters Say: Strike Boosts Enlistments." *Eugene (OR) Guard*, 9 August 1963, 6B.

York, Michael. "Odyssey of a Suspected Spy." *Washington Post*, 15 October 1989.

Charles E. Schoof and **John J. Haeger**. 1989. Both operations specialists third class, USN, USS *Fairfax County* (LST 1193). Conspired to compromise classified information to Soviet intelligence for money. Reported by a shipmate. Pled guilty to conspiracy to commit espionage, attempted espionage, wrongful use of cocaine (Schoof only, two specifications), and solicitation to aid and abet espionage (Schoof only) and were sentenced to 25 years and 19 years, respectively. Both were eligible for parole in 1996 after seven years' incarceration.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.

"Espionage." Naval Criminal Investigative Service, 1995, video.

"Ex-sailor Who Helped Navy Crack Latest Spy Case Miffed." *Daily News Leader* (Staunton, VA), 5 February 1990, A3.
"John J. Haeger, Petitioner-Appellant v. Michael A. Lansing, Commandant, [United States Disciplinary Barracks]–Ft. Leavenworth, Kansas, Respondent-Appellee." U.S. Court of Appeals Tenth Circuit, 9 February 2001.
"United States v. Charles E. Schoof, Operations Specialist Third Class (E-4), U.S. Navy." U.S. Navy–Marine Corps Court of Military Review, 30 January 1992.

Charles F. L. Anzalone. 1990. Corporal, USMC, Marine Corps Air Station Yuma, AZ. Attempted to compromised sensitive but unclassified information to an undercover agent posing as a Soviet intelligence officer in exchange for money. Convicted and sentenced to 15 years, which was later reduced to 8. Maintains that he was entrapped by the FBI.

"Appendix: II. Chart of Sentences Imposed in Espionage Cases, 1975–1996." Department of Justice, Office of the Pardon Attorney. Collection WJC-OCP: Records of the Office of the Counsel to the President (Clinton Administration), Series: Dawn Chirwa's Files, File Unit: Pollard Correspondence [2], NAID: 40436158, William J. Clinton Library, Little Rock, AR.
"Charles Anzalone." Facebook, accessed 12 May 2020.
Montgomery, David. "Jamestown Marine Is Granted Clemency: Accused Spy Anzalone Now Eligible for Parole This Year." *Buffalo (NY) News*, 15 January 1993.
———. "Sucker or Spy: The Court Martial of Cpl. Charles Anzalone." *Buffalo (NY) News*, 18 January 1992.
Tessler, Ray. "Video of Hotel Meeting Shown at Spy Trial." *Los Angeles Times*, 2 May 1991.

Michael S. Schwartz. 1992. Lieutenant commander, USN, U.S. military training mission to Saudi Arabia. Compromised classified information to the Saudi Navy. Initially accused of espionage but the charges were reduced to mishandling classified information in a plea agreement. Forced to resign with no retirement.

"American Naval Officer Is Accused of Passing Secrets to Saudi Arabia." *Los Angeles Times*, 25 May 1995.

"El Pasoan Saw Executions in Kuwait." *El Paso (TX) Times*, 13 December 1990, 2B.

Espionage Cases, 1975–2004: Summaries and Sources. Monterey, CA: Defense Personnel Security Research Center, 2004, 41.

"Norfolk Naval Officer Faces Court-Martial in Espionage Case." *Washington Post*, 13 September 1995.

"Our Men in Service." *El Paso (TX) Times*, 26 December 1971, 8B.

Perez, Janet. "With Son in Kuwait, El Paso Family Keeps an Optimistic Outlook." *El Paso (TX) Times*, 18 August 1990, 2B.

Teitelbaum, Joshua. "Saudi Arabia." In *Middle East Contemporary Survey*, ed. Bruce Maddy-Weitzman. Boulder, CO: Westview Press, 1995, 546.

Westermeyer, Paul W. *U.S. Marines in the Gulf War, 1990–1991: Liberating Kuwait*. Quantico, VA: Marine Corps History Division, 2014, 25–31, 55, 101.

Antonio Guerrero. 1993–98. Civilian, public works, NAS Boca Chica, Key West, FL. Cuban intelligence asset recruited and sent to the United States specifically to penetrate NAS Boca Chica. Discovered through compromised Cuban agent communications. Sentenced to life but eventually exchanged for U.S. intelligence assets imprisoned in Cuba.

Anderson, Curt. "Cuban Spy Gets Reduced Sentence of about 22 years." *San Diego (CA) Union-Tribune*, 13 October 2009.
Carter, Wayne. "A Look at the 'Cuban Five' Agents Jailed in the U.S." *Dallas (TX) Morning News*, 17 December 2014.
Collie, Tim. "A Glimpse Inside the Lives of Suspected Cuban Spies," *Chicago Tribune*, 16 September 1998.
Groll, Elias. "Agent at Center of Spy Swap Was Cuban Crypto Expert." *Foreign Policy*, 19 December 2014.
Nielsen, Kirk. "Inside the Wasp's Nest." *Miami (FL) New Times*, 22 February 2001.
"U.S. Wins Big with Release of Blue Chip Spy Held in Cuba." *CBS Miami*, 17 December 2014.
Williams, Carol. "Cuban-Born Spy Credited with Exposing Fidel Castro's U.S. Operatives." *Los Angeles Times*, 18 December 2014.

Robert C. Kim. 1995–96. Computer specialist, Office of Naval Intelligence. Compromised classified information to South Korea with the hope of arranging a retirement job there. Pled guilty and served seven years.

Demick, Barbara. "Bitter South Koreans Rally behind Spy Convicted in U.S." *Los Angeles Times*, 8 June 2004.
"Find an Inmate: Robert Kim." Bureau of Prisons, accessed 11 February 2021.
Hall, Charles W. "Kim Allegedly Sought Job with S. Korea." *Washington Post*, 2 October 1996.
Hall, Charles W., and Dana Priest. "Navy Worker Is Accused of Passing Secrets." *Washington Post*, 26 September 1996.
Keil, Richard. "U.S. Military Worker Arrested after Passing Documents to S. Korea." Associated Press, 26 September 1996.
Masters, Brooke A. "Va. Man Sentenced to 9 Years in Spy Case." *Washington Post*, 12 July 1997.

Oh, Dongryong. "Former Naval Officer to the U.S., Baek Dong-il, Took off His Military Uniform in the 'Robert Kim Incident'." *Chosun Pub*, 1 November 2016.

"Robert Kim's American Passion." Korean Broadcasting System, 29 August 2018.

"Two From NCIS Receive DoD FCI Awards." *U.S. Naval Criminal Investigative Service Bulletin* 2, no. 6 (October 1998), 15.

Kurt G. Lessenthien. 1996. Machinist's mate first class, USN, Naval Nuclear Power School, Orlando, FL. Attempted to compromise classified nuclear submarine to an undercover FBI agent. Pled guilty to espionage charges and served 15 years.

"18 Cats Die, 16 Survive Fire at Jacksonville Veteran's Home." News-4Jax, 11 January 2020.

Burns, Robert. "Navy Man Arrested on Spy Charge Offered Secrets to Russia." Associated Press, 24 April 1996.

"Kurt Lessenthien." LinkedIn, accessed 11 February 2021.

Leusner, Jim, and Tom Leithauser. "Orlando Sailor in Spy Arrest." *Orlando (FL) Sentinel*, 24 April 1996.

McMichael, William. "Would-be Spy Did All for Love." *Daily Press* (Newport News, VA), 25 October 1996.

"Navy Prosecutor Seeks Life in Prison for Spy." *Daily Press* (Newport News, VA), 25 October 1996, A5.

"Would-be Spy Gets 27 Years behind Bars." *Deseret News* (Salt Lake City, UT), 29 October 1996.

Hasan Abu-Jihaad. 2001. Signalman third class, USN, USS *Benfold* (DDG 65). Compromised classified information to British extremist propagandists in the hope that al-Qaeda would use the information to conduct an attack. Not detected until 2003, after he had left the Navy.

Convicted of violating the espionage statute and material support to terrorism and served eight years.

Kravitz, Mark. "Court Analyses Material Support to Terrorists—United States v. Abu-Jihaad No. 3:07CR57 (D. Conn. 03/04/2009)." U.S. District Court, District of Connecticut, 4 March 2009.
"Passing Secrets at Sea—To Terrorists, No Less." Federal Bureau of Investigation, 10 March 2008.
"United States v. Hassan Abu-Jihaad." U.S. Attorney's Office, District of Connecticut, 18 March 2015.
"The 'Unremarkable' Life of a Sailor Turned Terror Suspect." *Hartford (CT) Courant*, 24 February 2008.
"USS *Benfold* (DDG 65) Command History for CY 2001." Department of the Navy, 5 March 2002.

Gregg W. Bergersen. 2004–8. Navy International Programs Office and Defense Security Cooperation Agency. Compromised classified information to an asset of PRC military intelligence. Pled guilty to violating the espionage statute and served three years.

"Espionage: Stealing America's Secrets." *CBS News*, YouTube video 13:23, 29 August 2010.
"Find an Inmate: Gregg Bergersen." Bureau of Prisons, accessed 31 May 2020.
"Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation." U.S. Department of Justice, 11 July 2008.
Gaskell, Stephanie, and Corky Siemaszko. "Spy Suspect Just an 'American Dad'." *New York Daily News*, 13 February 2008.
Gertz, Bill. "Chinese Spy Buy Caught on Surveillance Video." *Washington Times*, 1 March 2010.
"Gregg Bergersen." LinkedIn, accessed 16 February 2016.

Grier, Peter. "Four Arrested on Charges of Spying for China." *Christian Science Monitor*, 13 February 2008.
"How a Networking Immigrant Became a Chinese Spy." *CBS News*, 9 May 2011.
"Link 16 Products." BAE Systems, accessed 16 December 2023.
Major, David. "Testimony before the U.S.-China Economic and Security Review Commission." 9 June 2016, 6–7.
"United States v. Tai Shen Kuo, Gregg William Bergersen, and Yu Xin Kang." U.S. District Court for the Eastern District of Virginia, Alexandria Division.
Wise, David. *Tiger Trap: America's Secret Spy War with China*. Boston, MA: Houghton Mifflin Harcourt, 2011, 223–24.

Ariel J. Weinmann. 2005–6. Fire control technician third class, USN, USS *Albuquerque* (SSN 706). Stole a classified laptop and deserted. In Austria, compromised classified information from the laptop to Russian intelligence for money. Detained after his return to the United States and served eight years.

"Ariel Weinmann-Rubino." Facebook, 18 May 2014.
McGlone, Tim. "Navy Submariner Admits He Offered Military Secrets." *Virginian-Pilot* (Norfolk, VA), 5 December 2006.
———. "Sailor Sentenced to 12 Years in Prison for Espionage." *Virginian-Pilot* (Norfolk, VA), 7 December 2006.
———. "Why a Patriotic Teen Joined the Navy and then Turned to Espionage." *Virginian-Pilot* (Norfolk, VA), 10 December 2006.
Starr, Barbara. "Sources: Navy Sailor Suspected of Spying for Russia." CNN, August 9, 2006.
Vergakis, Brock. "Norfolk Is a Hotbed for Espionage Cases Involving the Navy." *Virginian-Pilot* (Norfolk, VA), 14 April 2016.
Waller, Douglas. "Did the Sailor Go Overboard?." *Time*, 9 August 2006.

Wiltrout, Kate. "Recording Details Arrest of Sailor Accused of Espionage." *Virginian-Pilot* (Norfolk, VA), 11 August 2006.

Bryan M. Martin. 2010. Intelligence specialist third class, USNR, Joint Special Operations Command. Attempted to compromise classified information for money to an undercover FBI agent posing as a PRC intelligence officer. Pled guilty to espionage and sentenced to 34 years.

"Awareness in Action: Case Study: Bryan Martin." Defense Security Service, Center for Development of Security Excellence, accessed 9 February 2021.

Halpin, James. "NCIS: Sailor at Brag Sold Secret Documents." *Fayetteville (NC) Observer*, 4 December 2010.

McGlone, Tim "Va. Beach-based Sailor Gets 34 Years in Espionage Case." *Virginian-Pilot* (Norfolk, VA), 11 May 2011.

"U.S. Sailor Pleads Guilty to Attempted China Spying." *Fox News*, 19 May 2011.

Appendix E
Additional Historical Examples of Naval Espionage, Listed by Domain

Command and Control

Campaign-winning *time, place, or manner advantages* due to information gathered through signals intelligence (SIGINT) are the result of the long and difficult work of decoding messages. Most importantly for naval counterintelligence, decoding efforts are often enabled by espionage. Four espionage operations—a Confederate false flag, a German volunteer to French intelligence, a U.S. Navy black-bag job, and an American volunteer to Soviet intelligence (addressed in chapter 3)—provided material that was essential to the successful decoding operations that led to naval campaign victories. Historically, SIGINT, enabled by espionage, has been the most damaging form of adversary intelligence gathering for navies around the world.

Charleston, South Carolina, 1863

In 1862, the American Civil War was going badly for the United States, with some Americans beginning to suggest a negotiated peace with the Confederacy. Consequently, President Abraham Lincoln pressed the U.S. Army and Navy for a victory to boost morale. The Navy responded with a plan to occupy Charleston, South Carolina, where the

revolt first started. Occupying Charleston would be a huge symbolic victory for the United States.[1]

Throughout the ensuing 1863 Charleston campaign, the Navy provided gunfire support to Army units attempting to take the forts defending Charleston Harbor. Ship-to-shore communications used a coded flag system that the Confederates could intercept but not understand.[2]

A Union prisoner revealed to his Confederate captors that U.S. Signal Corps officers memorized the code settings. So, in a targeted raid, Confederate guerrillas captured a Signal Corps officer from a remote signal station on Hilton Head Island. The Confederates then used a false flag operation in the Charleston prison that held the officer to elicit the code. With the information from that espionage operation, the Confederates began to decode the U.S. flag signals almost immediately. Despite the capture of the Signals Corps officer, the Union did not change the code.[3]

Loss of the code gave the Confederates an *unexpected time and place advantage*. This advantage was the reason that assaults by the U.S. Army's 54th Massachusetts Infantry Regiment on Fort Wagner

[1] Stephen C. Ruder, "A Confederate Intelligence Coup Won the Siege of Charleston Harbor," *Civil War Quarterly* 5, no. 1 (Early Spring 2015): 70–77.

[2] See Gen P. G. T. Beauregard, CSA, to James A. Seddon, Confederate States Secretary of War, 13 April 1863, in *Official Records of the Union and Confederate Navies in the War of the Rebellion*, ser. 1, vol. 14, *South Atlantic Blockading Squadron* (Washington, DC: Government Printing Office, 1902), 689, hereafter *South Atlantic Blockading Squadron*. This letter notes the Confederate capability to intercept and decode U.S. flag signals.

[3] See *The War of the Rebellion: A Compilation of the Official Records of the Union and Confederate Armies*, ser. 1, vol. 28, pt. 1 (Washington, DC: Government Printing Office, 1890), 117, 119, 120, 122. This contains references to intercepted flag signals exchanged by U.S. forces in preparation for assaults on Fort Sumter and Battery Gregg outside Charleston. See also *The War of the Rebellion: A Compilation of the Official Records of the Union and Confederate Armies*, ser. 1, vol. 28, pt. 2 (Washington, DC: Government Printing Office, 1890), 206–7, 328. This contains references to intercepted flag signals exchanged by U.S. forces in preparation for an assault on Fort Wagner outside Charleston in July 1863 and a naval assault on Fort Sumter in September 1863. See also *South Atlantic Blockading Squadron*, 635. An officer involved in the amphibious assault on Fort Sumter believed that the Confederates had an "expectation of an attack" that resulted in their repulse of the assault.

and U.S. Marines on Fort Sumter both failed with heavy casualties. The Union never took Charleston; it only surrendered at the end of the war.

New York City, New York, 1920

When Japan first began to create a modern navy in the late 1800s, their strategy was to purchase as much modern technology as possible and then reverse engineer the equipment to be able to produce it themselves. Accordingly, the Imperial Japanese Navy (IJN) established naval inspector's offices in the United Kingdom, France, Germany, Italy, and the United States to arrange contracts and supervise the production of ships and equipment for Japan. These offices naturally reported on world naval developments, information which gradually included intelligence information.[4]

The IJN established its U.S. office circa 1918 in the Metropolitan Life Building in Manhattan. Two years later, the Bureau of Investigation, the New York Police Department, and the Office of Naval Intelligence (ONI) conducted a surreptitious entry operation at the Japanese consul general's office in New York, discovering a copy of the 1918 IJN secret operating code.[5] They photographed the entire book during several visits. During the course of several years, ONI translated the book and included updates via other operations at the naval inspector's office in 1926–27.[6]

---

[4] John Prados, *The Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II* (Annapolis, MD: Naval Institute Press, 1995), 65–66.

[5] "Camden to Build Big Jap Warship," *Philadelphia (PA) Inquirer*, 18 May 1921, 10; "Japanese Officers to Study Aviation in United States," *Washington Post*, 25 April 1919, 3; Prados, *The Combined Fleet Decoded*, 76; and Capt Wyman H. Packard, USN (Ret), *A Century of U.S. Naval Intelligence* (Washington, DC: Department of the Navy, 1996), 15.

[6] Capt Laurence F. Safford, USN (Ret), *A Brief History of Communications Intelligence in the United States* (Fort Meade, MD: National Security Agency: 1952), 6; and Jeffery M. Dorwart, *Conflict of Duty: The U.S. Navy's Intelligence Dilemma, 1919–1945* (Annapolis, MD: Naval Institute Press, 1983). 45.

Starting with the information from those espionage operations, the United States was able to continue to break Japanese codes through World War II. In 1942, after the losses at Pearl Harbor and in the Battle of the Coral Sea, the U.S. Navy was on the defensive in the Pacific. The U.S. Pacific Fleet only had three operational aircraft carriers left, which Japan hoped to draw into an ambush by sending an invasion force to Midway Atoll. The Japanese plan assumed that the U.S. aircraft carrier force would rush north from Hawaii toward Midway.[7]

However, U.S. espionage-enabled codebreaking revealed the Japanese plan and gave the United States an *unexpected time and place advantage*. The U.S. Navy set its own trap for the IJN by massing the entire US. Pacific Fleet to surprise and defeat the Japanese fleet. The IJN never launched another naval offensive in the war, and the industrial capacity of the United States made its defeat inevitable. Ultimately, a U.S. Navy espionage operation launched 22 years earlier set in motion a chain of events that resulted in a critical victory that helped win World War II in the Pacific. Despite repeated tactical losses, the Japanese did not make major changes to their code.

Berlin, Germany, 1931

In 1926, the German military began using a new machine called Enigma to encode its radio communications, and it seemed unbreakable. Originally made for commercial use, the German Defense Ministry cipher office in Berlin controlled the Enigma system. Around 1930,

[7] See Frederick D. Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battle of Coral Sea, Midway, and the Aleutians* (Fort Meade, MD, National Security Agency Center for Cryptologic History, 2017). This provides a detailed historical view from the archives of the National Security Agency of the nature of the signals intelligence effort that led to the U.S. advantage at Midway. See also *Combat Narratives: Battle of Midway, June 3–6, 1942* (Washington, DC: Office of Naval Intelligence, 1943), 5, 55. This provides contemporary background on the battle and hints that the United States was privy to Japanese plans. See also Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York: Simon & Schuster, 2002), 4–5, 13–22.

the director of the office hired Hans Thilo Schmidt, the unemployed brother of an old friend, to serve as his assistant.

Schmidt, a 43-year-old whose flamboyant lifestyle far exceeded his government salary, had routine access to the director's safe, which contained the daily settings and operating instructions for Enigma. Seeking to supplement his salary, in June 1931, Schmidt walked into the French embassy in Berlin. The embassy advised him to write to French intelligence, which he did, and they arranged a meeting across the border in Belgium. Schmidt sold the French an operating manual for the Enigma machine and several months of daily settings.

French intelligence collaborated with British and Polish intelligence to use the material to crack the Enigma code. Fortunately, the Poles, who had a commercial version of the machine, were able to deduce the Enigma's internal wiring, produce a replica, and begin reading German coded messages. In 1938, the Poles gave copies of the Enigma machines to the British and French. Despite many changes, those machines formed the basis of British codebreaking during World War II, with the Allies calling the resulting intelligence "Ultra." German authorities finally arrested Schmidt in 1943, but the Germans never admitted that the Allies had compromised their codes, and they continued to use Enigma until their defeat in 1945.[8]

[8] See David Kahn, "The Ultra Secret," *New York Times*, 29 December 1974. This book review contains the first public revelation of Hans Thilo Schmit's name. This revelation resulted from Kahn's interview with the author of a French-language book written by a World War II-era French signals intelligence officer named Gustave Bertrand, *Enigma ou la plus grande énigme de la guerre 1939–1945*, published in 1973 but unavailable to the author. Bertrand did not name Schmidt but used his cover name, Asché. Kahn later deduced the name through another contact. See also Paul Paillole, *The Spy in Hitler's Inner Circle: Hans-Thilo Schmidt and the Intelligence Network that Decoded Enigma* (Oxford, UK: Casemate, 2016). This is an English translation of a 1985 French-language book written by a French counterintelligence officer who participated in the Schmidt case. While the book is written in a casual style, the facts appear to be genuine and expand on Bertrand's book. See also David Kahn, "Unveiling World War II's Greatest Spy," *Quarterly Journal of Military History* (Autumn 2007): 28–33. Kahn describes the full story of tracking down Schmidt's identity and other sources he unearthed. Oddly, he did not mention Paillole's book. See also Hugh Sebag-Montefiore, *Enigma: The Battle for the Code* (London: Orion, 2000). This book adds to previous information about the Schmidt case

Schmidt's espionage, which led to the breaking of Enigma, gave the Allies an *unexpected time and place advantage* over German forces throughout World War II. This advantage was particularly acute during the Battle of the Atlantic, the yearslong struggle between Allied shipping convoys crossing the Atlantic and Germany's submarine force. After a difficult start, the *time and place advantage* provided by Ultra allowed the Allies to first avoid German submarines and later to sink nearly all of them.[9]

Weapons and Sensors

Espionage that targeted the U.S. Department of the Navy's weapons and sensors was a more common occurrence than espionage-enabled SIGINT, but it was also less damaging and did not alone play a significant role in deciding the outcome of a naval campaign. Two historical examples illustrate the concept.

Norfolk, Virginia, 1862

During the American Civil War, the use of publicly available information and espionage by both the Union and the Confederacy played a role in a wartime race to build a new type of weapon, armored surface combatants called "ironclads." The U.S. Navy was building the USS *Monitor*, an ironclad from the keel up, while the Confederate States Navy was building the CSS *Virginia*, based on the hull of the partially scuttled USS *Merrimack*. Both sides raced to finish their new weapons

by locating and interviewing Schmidt's daughter.

[9] Cdr Jerry Russell, USN, "Ultra and the Campaign against the U-boats in World War II" (unpublished paper, U.S. Army War College, 30 May 1980).

in anticipation of a Confederate attempt to break the Union's blockade of Hampton Roads.[10]

The Union received information about the construction of *Virginia* from at least four different human sources who either observed or worked aboard the ship. Two made their way to U.S. Navy units blockading Hampton Roads, another was an exchanged prisoner of war, and the fourth sent his information across enemy lines via a courier, Mary Louvestre.[11]

Fort Pulaski, Georgia, 1862

The siege of Fort Pulaski on the Georgia coast near the city of Savannah during the American Civil War offers an example of poor assessment of an adversary's weapons. In 1862, Union forces began a campaign to seize Savannah. The Confederates took control of Fort Pulaski, which both sides thought was impregnable, with its 2.3-meter-thick masonry walls that had been completed only 15 years earlier. However, on an island less than 2 kilometers away, under cover of darkness during a span of four months, the Union secretly landed and positioned 38 artillery pieces, including several newly acquired rifled guns, the latest innovation in artillery at the time. To the surprise of nearly all participants on both sides, the rifled cannon blasted a 9-meter-wide gap in the fort wall within 36 hours, giving the Union a tactical *unex-*

[10] See *Official Records of the Union and Confederate Navies in the War of the Rebellion*, ser. 1, vol. 6, *North Atlantic Blockading Squadron* (Washington, DC: Government Printing Office, 1902), 446, 482, 515, 517, 538, 640. This contains several human intelligence reports regarding the progress of CSS *Virginia*'s construction.

[11] See Gideon Welles, "Gideon Welles Papers: Correspondence, –1878: 1864, August–September 1864," Manuscript Division, Library of Congress, Washington, DC, 103. This contains notes by U.S. Secretary of the Navy Gideon Welles that Mary Louvestre provided important information about the progress of CSS *Virginia* during construction. See also Welles, "Gideon Welles Papers," 37–42. This depicts efforts by Welles to identify and reward Louvestre for providing information about *Virginia* during the war. See also Gideon Welles, letter to Mary Louvestre, 17 August 1872, Vital and Cemetery Records, Esther Murdaugh Wilson Memorial Room, Public Library, Portsmouth, VA. This is a transcription of a letter in which Welles describes Louvestre couriering information circa January 1862 about *Virginia* from a mechanic working on the ship in Norfolk, VA, and the requirement to hasten construction of USS *Monitor*.

pected advantage. The Confederates surrendered a few hours later.[12] Remarkably, Confederate forces had already accidentally contrived a countermeasure to the rifled artillery—earthen walls. In 1861, more than 30 kilometers south of Fort Pulaski, the Confederates had built Fort McAllister from logs and earth, which simply absorbed the shells of rifled runs, giving the Confederates a tactical *unexpected advantage*. For the next two years, Fort McAllister withstood six Union naval bombardments with only minor damage.[13]

North Sea, 1916

A great example of how superior sensors may affect an engagement but not a campaign is the Battle of Jutland between the British Royal Navy and the Imperial German Navy in 1916. The British used SIGINT to achieve an operational *unexpected advantage* by identifying that the German fleet had left port en mass. The British were able to sortie their fleet in response. Additionally, in the opening minutes of the battle, the British used aerial reconnaissance to pinpoint the German fleet and establish their course and speed, giving themselves a tactical *unexpected advantage*.[14] However, while these superior sensors contributed to the British victory at Jutland, they were not critical to the

[12] Quincy Gillmore, *Official Report to the United States Engineer Department of the Siege and Reduction of Fort Pulaski, Georgia, February, March, and April 1862* (New York: D. Van Nostrand, 1862); and *Official Records of the Union and Confederate Navies in the War of the Rebellion*, ser. 1, vol. 13, *South Atlantic Blockading Squadron from May 14, 1862 to April 7, 1863* (Washington, DC: Government Printing Office, 1901), 544, 549, 627, 704–5, 720, 727, 732–34.
[13] Charles C. Jones Jr., *Military Lessons Inculcated on the Coast of Georgia during the Confederate War: An Address Delivered before the Confederate Survivors' Association, in Augusta, Georgia, at Its Fifth Annual Meeting, on Memorial Day, April 26, 1883* (Augusta, GA: Chronicle Printing Establishment, 1883).
[14] Julian S. Corbett, *History of the Great War, Based on Official Documents by Direction of the Historical Section of the Committee of Imperial Defence: Naval Operations*, vol. 3, *Spring 1915 to June 1916 (Part 2 of 2)* (London: Longmans Green, 1923), 323, 326, 328, 333. This contains references to British Royal Navy wireless direction finding and radio intercept of German Imperial Navy radio transmissions. It also contains a reference to a seaplane launched for aerial reconnaissance by HMS *Engadine* (1911).

overall German defeat at sea because German submarines (U-boats) remained a threat.

Luzon, Philippines, 1945

A short-lived U.S. intelligence failure to detect a Japanese naval weapon innovation during World War II provides a good example of rapid neutralization of weapons-based surprises through improved tactics. On the night of 9 January 1945 approximately 90 Japanese explosive motor boat (EMB) suicide bombers attacked U.S. Navy amphibious transports off the Lingayen beachhead on the island of Luzon in the Philippines. This was the first attack of its kind, and as the U.S. Navy had no intelligence that these units even existed, the Japanese were given a tactical *unexpected advantage*. At the cost of 45 EMBs lost, the Japanese sank two U.S. landing craft, seriously damaged three landing ships and a transport, and caused lesser damage to seven other transports. Within a few days, the U.S. Navy countered the EMB threat with aggressive daylight motor torpedo (PT) boat patrols that destroyed the EMBs at their bases before they could attack the U.S. fleet. The Japanese managed one more spectacular EMB attack, sinking the submarine chaser USS *PC-1129* south of Manila Bay on 31 January, but within a month of the first attack, the PT boats, assisted by naval aviation, had cleared the area of EMBs.[15]

Indonesia, 1967

In the late 1960s, an incident awoke the DON to the fact that it was not prepared to defeat antiship missiles. In 1967, during the Arab-Israeli Six Day War, three Soviet-designed SS-N-2 Styx antiship missiles fired

[15] Samuel Eliot Morison, *History of United States Naval Operations in World War II*, vol. 12, *The Liberation of the Philippines: Luzon, Mindanao, the Visayas, 1944–45* (Boston, MA: Little, Brown, 1959), 14, 50, 138–40, 189, 191–92, 202, 226. This contains references to several action reports involving Japanese explosive motor boats (EMB). Several EMB attacks also damaged ships off Okinawa in April and May 1945.

from two Egyptian-crewed, Soviet-supplied Komar-class missile craft hit and sank the Israeli destroyer INS *Eilat* (K40) off Port Said, Egypt. The sinking was a turning point in naval warfare.[16]

Far from the scene of action in the Mediterranean, the Central Intelligence Agency (CIA) found an opportunity to obtain information about the Styx and other Soviet weapons in Indonesia. Between 1967 and 1970, the CIA acquired design information for the Styx, which the Soviet Union had sold to Indonesia in the early 1960s. Although control over these weapons was reportedly tight at Soviet bases, a retired CIA officer noted that some of their foreign clients "guarded them with security that was less than absolute."[17]

With knowledge of the Styx designs obtained from Indonesia and the specter of the *Eilat* sinking, the DON embarked on a program to field antiship missile defense systems. The department selected the General Dynamics Phalanx system and installed a prototype aboard the destroyer leader USS *King* (DLG 10) in 1973 for evaluation. Phalanx, also known as the close-in weapon system (CIWS), remains in use today.[18]

[16] See Andrew Hind, "The Cruise Missile Comes of Age," *Naval History Magazine* 22, no. 5 (October 2008). See also Robert M. Clark, "Scientific and Technical Intelligence Analysis," *Studies in Intelligence* (Langley, VA: Central Intelligence Agency, 1975), 41. This provides an overview of the antiship missile issue in 1960. See also "SS-N-2 (STYX) Naval Cruise Missile," Central Intelligence Agency, 30 October 1967. This provides previously classified contemporary background on the sinking of INS *Eliat* and the Styx antiship cruise missile. See also Exchange of memoranda between John A. McCone, director, Central Intelligence Agency, and RAdm Vernon L. Lowrance, USN, director, Naval Intelligence, 1963, Central Intelligence Agency, Langley, VA. Regarding Soviet naval cruise missiles, RAdm Lowrance noted that the only U.S. Navy defense was to destroy the launcher or the missile prior to launch.

[17] John McBeth, "How a CIA Operation in Indonesia Turned the Vietnam War," *Asia Times*, 27 March 2021.

[18] See Robert H. Stoner, "R2D2 with Attitude: The Story of the Phalanx Close-in Weapons," NavWeaps, 30 October 2009. See also "MK 15: Phalanx Close-in Weapon System (CIWS)," Navy.mil, 20 September 2021. This notes the first installation of the Phalanx system in 1980.

Shore Establishment Observation

Passive observation of fleet concentration areas can provide critical order of battle information. As an enemy can nearly always overtly or covertly observe one's ports and airfields, that advantage should *be expected*, and military leaders should always assume it. However, three historical examples demonstrate that naval leaders do not always focus on their adversary's observation advantage over shore establishments.

Inchon, South Korea, 1950

The first example features a U.S. naval intelligence mission at Inchon, South Korea, in 1950, the first year of the Korean War. One U.S. Navy officer accompanied by a team of South Korean naval personnel spent two weeks reconnoitering the approaches to Inchon in advance of a campaign-winning amphibious assault launched in September.[19] The North Koreans failed to assume that their shore establishment at Inchon was under observation and take the appropriate measures to detect the approach of the amphibious task force, which gave the U.S. amphibious task force commander an *unexpected advantage*. The Inchon landing and the eventual liberation of the South Korean capital of Seoul doomed North Korea's attempt to seize the entire Korean peninsula, though it did not result in a complete victory for South Korea and its United Nations allies.[20]

Falkland Islands, 1982

In 1982, the United Kingdom and Argentina fought over ownership of the Falkland Islands, a British overseas territory some 650 kilometers

[19] Cdr Eugene F. Clark, USN, *The Secrets of Inchon* (New York: G. P. Putnam's Sons, 2002).
[20] Lynn Montross and Capt Nicholas A. Canzona, USMC, *U.S. Marine Operations in Korea, 1950–1953*, vol. 2, *The Inchon-Seoul Operation* (Washington, DC: Historical Branch, G-3, Headquarters Marine Corps, 1955), 296–97; and LtCol Pat Meid, USMCR, and Maj James M. Yingling, USMC, *U.S. Marine Operations in Korea, 1950–1953*, vol. 5, *Operations in West Korea* (Washington, DC: Historical Division, Headquarters Marine Corps, 1972), 478.

off the coast of Argentina in the South Atlantic. After an Argentinian invasion of the islands, a British amphibious task force recaptured them in a grueling campaign. To warn of Argentinian air attacks, British special forces reportedly established observation posts at Argentinian mainland and island military ports and airfields to provide a steady stream of intelligence that gave the British amphibious task force commander an *unexpected advantage*.[21] While the Argentinian military took measures to prevent sabotage, they failed to neutralize British observation of their shore establishments.

Aden, Yemen, 2000

A more recent example of failure to assume that an adversary has an *unexpected advantage* at a shore establishment was the al-Qaeda attack on the guided missile destroyer USS *Cole* (DDG 67). On 12 October 2000, *Cole* was conducting a brief stop for fuel (BSF) at Aden, Yemen. U.S. Navy ships had begun making BSFs in Aden in January 1999, and *Cole* was the 28th such combatant to conduct a BSF there.[22] Unbeknownst to the DON, within a few months of the start of BSF operations in Aden, al-Qaeda began planning for a suicide waterborne improvised explosive device (SWBIED) attack on a U.S. Navy ship there. During the next year, an al-Qaeda cell built a SWBIED, prepared observation points in the city, and attempted one unsuccessful but unobserved attack against USS *The Sullivans* (DDG 68) on 3 January 2000. Through its secret preparations, the al-Qaeda cell in Aden achieved an *unexpected advantage* over the DON. Compounding the situation was that, despite intelligence suggesting a high threat

[21] "The British Army and the Falklands War," National Army Museum, accessed 29 May 2021; Don Sellar, "Captive Commandos 'Alive' in Argentina, Condition Unknown," *Vancouver Sun*, 22 June 1982; and Derek Oakley, *The Falklands Military Machine* (Staplehurst, UK: Spellmount, 2002) 141.

[22] "Opening Remarks of General Tommy R. Franks, Commander in Chief, U.S. Central Command, before the United States Senate Armed Services Committee," Federation of American Scientists, 25 October 2000.

from a terrorist attack, *Cole* was not fully protected from attack.[23] The al-Qaeda cell successfully employed their SWBIED against *Cole*, killing 17 sailors and nearly sinking the ship.[24]

Observation of Aden Harbor in 1999–2000 resulted in a tactical defeat but did not change the course of the U.S. campaigns against al-Qaeda. Conversely, U.S. observation of Inchon Harbor in 1950 and British observation of Argentinian airbases in 1982 facilitated significant naval campaign victories. This history suggests that minor shore establishments are not critical for campaigns because the adversary force can rebuild or relocate the capabilities provided there. However, observation of major military concentration areas can be critical for the success of naval campaigns, as demonstrated by the Yoshikawa case in chapter 2.

[23] *Command Investigation into the Actions of USS Cole (DDG 67) in Preparing for and Undertaking a Brief Stop for Fuel at Bandar at Tawahi (Aden Harbor) Aden, Yemen on or about 12 October 2000* (Washington, DC: U.S. Navy, 2000).

[24] "United States v. Jamal Ahmed Mohammed, Ali Al-Badawi, and Fahd Al-Quso," United States District Court, Southern District of New York, 2003.

Select Annotated Bibliography and Suggested Further Reading

The following 46 books and articles provide some basic background on intelligence and espionage more specifically. Several focus on the history of U.S. naval counterintelligence. Many, but not all, touch on naval espionage cases that impacted warfighting from the American Revolutionary War through the Cold War. Also included are several illustrative books about British intelligence operations during World War II in both Europe and Asia.

Allen, Thomas B. *George Washington, Spymaster: How the Americans Outspied the British and Won the Revolutionary War*. Washington, DC: National Geographic, 2004. A handy and readable account of the first U.S. intelligence operations during the American Revolutionary War. It includes an account of a campaign-altering naval counterintelligence operation in 1780 that diverted a British naval strike on a French fleet that had just arrived in Rhode Island. That counterintelligence operation set the stage for the eventual British capitulation at Yorktown the following year.

Andrew, Christopher. *The Defence of the Realm: The Authorized History of MI5*. London: Penguin, 2009. An extensive history of British counterintelligence that mentions the Harry F. Houghton case but fails to connect it to U.S. Navy ballistic missile submarines and Soviet espionage at Holy Loch, Scotland, in the early 1960s.

Andrew, Christopher, and Vasili Mitrokhin. *The Mitrokhin Archive: The KGB in Europe and the West*. London: Penguin, 1999. An au-

thoritative history of Soviet Committee for State Security (KGB) intelligence operations based on notes smuggled out of the KGB's archives. The book covers the 1967 John A. Walker Jr. case and the Houghton Royal Navy case in the 1960s. Andrew notes, "The most important Cold War agent recruited in Washington before Aldrich Ames walked in in 1985 was probably Chief Warrant Officer John Anthony Walker, a communications watch officer on the staff of the Commander of Submarine Forces in the Atlantic (COMSUBLANT) in Norfolk, Virginia."

Barker, Rodney. *Dancing with the Devil*. New York: Simon & Schuster, 1996. An account of the Clayton J. Lonetree espionage case and subsequent investigation. Published prior to Lonetree's release.

Bayly, Christopher, and Tim Harper. *Forgotten Armies: The Fall of British Asia*. Cambridge, MA: Belknap Press, an imprint of Harvard University Press, 2005. "Prologue, Part I: Escaping Colonialism" provides an overview of the haphazard and belated British response to pre-World War II Japanese espionage operations in Malaya (present-day Malaysia and Singapore). As in the United States, the British suspected that members of the Japanese expatriate community in their Asian colonies were cooperating with Japanese intelligence. Unlike the United States, the British were occasionally correct, which fed a degree of espionage hysteria as the war approached.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. New York: Touchstone, 2002. A thorough history of codebreaking and signals intelligence during World War II. Describes the Han Thilo Schmidt espionage-enable signals intelligence case on pp. 101–3.

Carlson, Elliot. *Joe Rochefort's War: The Odyssey of the Codebreaker Who Outwitted Yamamoto at Midway*. Annapolis, MD: Naval Institute Press, 2011. An excellent study of the U.S. intelligence failure at Pearl Harbor, HI, and intelligence success at the Battle

of Midway. The descriptions of Japan as an irrational actor and the failure of Rochefort and the rest of the U.S. intelligence community to understand Japanese motivations for war are particularly noteworthy.

Clark, Cdr Eugene F., USN. *The Secrets of Inchon: The Untold Story of the Most Daring Covert Mission of the Korean War*. New York: Putnam, 2002. A first-person account of U.S. Navy espionage operations in the archipelago outside the port city of Inchon, South Korea, in the prelude to the amphibious assault in 1950.

Dobbs, Michael. *Saboteurs: The Nazi Raid on America*. New York: Alfred A. Knopf, 2004. Tells the story of Nazi Germany's futile attempt to rebuild its espionage network in the United States after the Duquesne Spy Ring was neutralized by the Federal Bureau of Investigation (FBI) in 1941.

Dorwart, Jeffery M. *Conflict of Duty: The U.S. Navy's Intelligence Dilemma, 1919–1945*. Annapolis, MD: Naval Institute Press, 1983. A detailed history of ONI organization and operations before and during World War II. This account focuses on the extralegal activities of ONI at the time and the excesses that occurred. It includes information about both the John S. Farnsworth and Harry T. Thompson cases.

———. *The Office of Naval Intelligence: The Birth of America's First Intelligence Agency, 1865–1918*. Annapolis, MD: Naval Institute Press, 1979. A detailed history of the establishment of the Office of Naval Intelligence (ONI) and the expansion of its remit to include domestic intelligence and counterintelligence. It details ONI's amateurish and bigoted targeting process employed during World War I.

Drabkin, Ron, Ken Kusunoki, and Bradley W. Hart. "Agents, Attachés, and Intelligence Failures: The Imperial Japanese Navy's Efforts to Establish Espionage Networks in the United States before Pearl Harbor." *Intelligence and National Security* 38, no. 3 (2022): 390–

406. https://doi.org/10.1080/02684527.2022.2123935. A broad account of Japanese espionage against the United States prior to World War II. It includes the Frederick J. Rutland, Farnsworth and Thompson cases and suggests that the Japanese effort was largely a failure despite poor U.S. security. The article provides some unique insights but does not discuss Japanese espionage in Hawaii in depth.

Earley, Pete. *Family of Spies: Inside the John Walker Spy Ring*. New York: Bantam Books, 1988. A thorough account by a journalist of the Walker espionage case. The account barely mentions naval counterintelligence but heavily faults the FBI for failing to act quickly on the allegations made by Walker's wife.

Espionage. Washington, DC: Naval Investigative Service, 1989. An official public relations publication that advertises 1980s-era espionage cases and double agent operations in the U.S. Navy. Provides good background on how espionage investigations and operations were conducted.

Espionage and Other Compromises of National Security Case Summaries from 1975 to 2008. Monterey, CA: Defense Personnel Security Research Center, 2009. Provides a broad overview of individual late Cold War and post-Cold War U.S. defense-related espionage cases, which are organized alphabetically, by year of initiation, and by victim organization. Includes some cases not included in this study.

Everest-Phillips, Max. "The Pre-War Fear of Japanese Espionage: Its Impact and Legacy." *Journal of Contemporary History* 42, no. 2 (April 2007): 243–65. https://doi.org/10.1177/0022009407075546. A thoughtful article that notes, "The history of espionage is often a history of ignorance, xenophobia, racial prejudice, and stereotyping." The author makes that case when discussing Japanese espionage against the United States and the United Kingdom in the 1930s.

Farago, Ladislas. *The Game of Foxes: The Untold Story of German Espionage in the United States and Great Britain during World War II*. New York: David McKay, 1971. A popularized account of German *Abwehr* operations during World War II, allegedly based on records captured after the German surrender. Panned by a professional intelligence officer familiar with those records as "unremittingly sensationalized." To be avoided.

Headley, John W. *Confederate Operations in Canada and New York*. Washington, DC: Neale Publishing, 1906. Describes Confederate intelligence operations in Canada and New York during the American Civil War.

Hembry, Boris. *Malayan Spymaster: Memoirs of a Rubber Planter, Bandit Fighter and Spy*. Singapore: Monsoon Books, 2011. A first-person account of British reconnaissance operations in South and Southeast Asia during World War II. It provides revealing detail of the British Secret Intelligence Service's rush to organize effective espionage operations in areas occupied by the Japanese.

Hubbard, Douglass H., Jr., *Special Agent, Vietnam: A Naval Intelligence Memoir*. Washington, DC: Potomac Books, 2006. A first-person account of Naval Investigative Service (NIS) activities in Vietnam. While it is a detailed account, it is remarkable for the lack of espionage investigations described. It is unclear if this was the result of the author's omission or a lack of naval espionage cases in Vietnam.

Huchthausen, Peter A., and Alexandre Sheldon-Duplaix. *Hide and Seek: The Untold Story of Cold War Naval Espionage*. Hoboken, NJ: John Wiley & Sons, 2009. A broad account of U.S. naval intelligence activities during the Cold War. Discusses the Walker case in chapter 12.

Keegan, John. *Intelligence in War: Knowledge of the Enemy from Napoleon to al-Qaeda*. New York: Vintage Books, 2002. A series of

seven case studies ranging from the Napoleonic Wars to the 1982 Falklands War, which show both the utility and limits of intelligence information in wartime.

Kessler, Ronald. *The Spy in the Russian Club: How Glenn Souther Stole America's Nuclear War Plans and Escaped to Moscow*. New York: Charles Scribner Sons, 1990. A good journalistic account of the Glenn Michael Souther espionage case. The author is critical of the counterintelligence response to the case.

Kotani, Ken. *Japanese Intelligence in World War II*. London: Osprey, 2009. A unique view of Japan's intelligence organization. The account relies heavily on British records and includes information about the Rutland case. Kotani also advances a theory, which he credits to the British counterintelligence and security agency MI5, that during the 1930s, Japanese intelligence shifted from technology to strategic intelligence as war loomed.

Landau, Henry. *The Enemy within: The Inside Story of German Sabotage in America*. New York: Van Rees Press, 1937. An exaggerated account of German intelligence activities in the United States prior to its entry into World War I but still useful for understanding the general situation at the time. The author was a former British intelligence officer employed as an investigator for a post-World War I international commission that investigated German wartime sabotage.

Leab, Daniel J. "The Red Menace and Justice in the Pacific Northwest: The 1946 Trial of the Soviet Naval Lieutenant Nikolai Gregorevitch Redin." *Pacific Northwest Quarterly* 87, no. 2 (Spring 1996): 82–93. An account of the trial of a Soviet Navy officer who allegedly attempted to collect information about the U.S. Navy destroyer tender USS *Yellowstone* (AD 27). Redin was acquitted and returned to the Soviet Union. The case points out how easily an espionage prosecution can be frustrated without strong evidence backed by extensive investigation and surveillance.

Lord, Walter. *Lonely Vigil: Coastwatchers of the Solomons*. Annapolis, MD: Naval Institute Press, 1977. An extensive account of the Royal Australian Navy's observational espionage network in Melanesia during World War II.

Lysenko, Vladil. *A Crime against the World: Memoirs of a Russian Sea Captain*. Translated by Michael Glenny. London: Victor Gollancz, 1983. Chapter 16, "Warlike Uses of the Soviet Merchant Fleet," describes how Soviet merchant ships were liable for mobilization and used for intelligence collection during the Cold War.

Macintyre, Ben. *Double Cross: The True Story of the D-Day Spies*. New York: Crown, 2012. A thorough and readable account of the deception operations conducted against Germany during World War II. The book describes how signals intelligence, human intelligence, and double agents were woven together to deceive German intelligence. Just prior to World War II, ONI attempted, but failed, to double Thompson, Bernard J. O. Kuehn, and one of the Drummond brothers back against Japanese intelligence precluding a similar deception operation in the Pacific Theater.

———. *Operation Mincemeat: How a Dead Man and a Bizarre Plan Fooled the Nazis and Assured an Allied Victory*. New York: Crown, 2010. An entertaining account of a successful British deception operation conducted in advance of Operation Husky, the Allied landings on Sicily in 1943. The book describes how thorough British counterintelligence efforts in a neutral country, fused with an inventive deception operation, successfully deceived German intelligence. Made into a film by the same name in 2021.

Mattis, Peter, and Matthew Brazil. *Chinese Communist Espionage: An Intelligence Primer*. Annapolis, MD: Naval Institute Press, 2019. A thorough analysis of intelligence as practiced under the Chinese Communist Party that points out both the strong and weak points of the system. It includes summaries of the Chi Mak and Gregg W. Bergersen cases. Most significantly, the book notes

the importance of computer-based espionage to Chinese intelligence, noting, "Computer network exploitation changed everything for Chinese intelligence."

Mortimer, Gavin. *Double Death: The True Story of Pryce Lewis, the Civil War's Most Daring Spy*. New York: Walker, 2010. An entertaining account of espionage and counterintelligence operations during the American Civil War.

Olive, Ronald J. *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice*. Annapolis, MD: Naval Institute Press, 2006. A comprehensive account of the Jonathan J. Pollard espionage investigation written by the NIS special agent who led it.

Packard, Capt Wyman H., USN. *A Century of U.S. Naval Intelligence*. Washington, DC: Departmewnt of the Navy, 1996. Chapters 21 and 22 provide a thorough overview, from official records, of the organization of U.S. naval counterintelligence from its inception in 1917 until 1973.

Pincher, Chapman. *Treachery: Betrayals, Blunders, and Cover-Ups: Six Decades of Espionage against America and Great Britain*. New York: Random House, 2009. Written by a longtime critic of the British security services, Chapters 61 and 65 provide an overview of two British Royal Navy espionage cases during the Cold War. One, the Houghton case, was tertiarily related to Soviet intelligence monitoring of the U.S. ballistic submarine base in Holy Loch, but that connection is not made in the book.

Popov, Dusko. *Spy/Counterspy: The Autobiography of Dusko Popov*. Greenwich, CT: Fawcett Crest, 1975. A first-person account of a British double-agent operation conducted during World War II against the German *Abwehr*. Provides fascinating insight into double agentry and is highly critical of the FBI's approach to counterintelligence at the time.

Prados, John. "The U.S. Navy's Biggest Betrayal." *Naval History* 24, no. 3 (June 2010). An informative summary of the basic facts of the Walker case.

Riehle, Kevin P. *Russian Intelligence: A Case-based Study of Russian Services and Missions Past and Present*. Bethesda, MD: National Intelligence Press, 2021. An excellent nuts-and-bolts overview of intelligence operations in general as well as Soviet/Russian intelligence tactics, techniques, and procedures.

Rose, Alexander. *Washington's Spies: The Story of America's First Spy Ring*. New York: Bantam, 2007. A very readable and thorough account of the espionage networks operated by the Continental Army against the British Army during the American Revolutionary War.

Ruder, Stephen C. "A Confederate Intelligence Coup Won the Siege of Charleston Harbor." *Civil War Quarterly* 5, no. 1 (Early Spring 2015): 70–77. An account of campaign-altering espionage that thwarted the joint U.S. Army-Navy effort to seize Charleston, South Carolina, during the American Civil War. One aspect of this espionage resulted in the defeat of a U.S. Marine Corps assault on Confederate-held Fort Sumter in 1863.

———. "Espionage Double Cross in Singapore." *WWII History* 16, no. 4 (June 2017): 20–23. An account of a 1934 Japanese intelligence operation targeting the British Royal Navy and Royal Air Forces bases in Singapore. The case ended in a Singapore Special Branch double-agent operation and the suicide of the main operative.

Sebag-Montefiore, Hugh. *Enigma: The Battle for the Code*. Hoboken, NJ: John Wiley & Sons, 2000. An account of the effort to break and continue reading German encryption during World War II. The book opens with an extensive account of the Hans Thilo Schmidt espionage case.

Shennan, Margaret. *Our Man in Malaya*. Singapore: Monsoon Books, 2014. An account of the British scramble to improvise intelli-

gence operations in South and Southeast Asia during World War II. Focuses on the Special Operations Executive.

Smith, Michael. *Station X: The Codebreakers of Bletchley Park*. London: Channel 4 Books, 1998. Chapter 2 mentions the Hans Thilo Schmidt espionage case.

Stoll, Cliff. *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. New York: Pocket Books, 1990. An entertaining first-person story of the first computer espionage case in U.S. history. In 1986, Stoll tracked down the Hanover Hackers, a group of East German hackers working on behalf of the Soviet KGB. Stoll's work inspired much of what forms cyber espionage investigative techniques today. Also made into a documentary film starring Stoll as himself, *The KGB, the Computer and Me*, in 1990.

Suvorov, Viktor. *Inside Soviet Military Intelligence*. New York: Macmillan, 1984. A thorough overview of Soviet Military Intelligence (GRU) during the Cold War by a defector. Chapters 2–6 describe espionage by GRU officers under diplomatic cover. Chapter 7 discusses intelligence operations carried out from within the Soviet Union. Chapter 10 may be of particular interest to U.S. naval counterintelligence as it describes Soviet fleet intelligence.

Young, Desmond. *Rutland of Jutland*. London: Cassell, 1963. An account of the Rutland espionage case. While the book provides excellent background about Rutland, the author minimalizes his espionage for the Japanese. The book was published 40 years before the British Security Service released its files on Rutland.

Zacharias, Ellis M. *Secret Missions: The Story of an Intelligence Officer*. Annapolis, MD: Naval Institute Press, 1946. A firsthand account by a naval officer assigned to counterintelligence duties as a district intelligence officer in the 11th Naval District, headquartered at San Diego, CA, from 1938 to 1940. Chapters 17 and 20 note three prewar cases briefed in this work. The author had firsthand

involvement with the 1937 Hafis Salich case, as he was Salich's commanding officer when the espionage was discovered.

Zimmerman, Maj John L., USMCR. *The Guadalcanal Campaign*. Washington, DC: Historical Division, Headquarters Marine Corps, 1949. An extensive account of the largely naval Guadalcanal campaign. It credits the observational espionage of Coastwatchers with providing potentially campaign-altering intelligence before and during the campaign. It quotes the official Marine Corps final report on the campaign: "The invaluable service of the Solomon Islands coastwatching system . . . cannot be too highly commended."

Index

About the Author

Stephen C. Ruder has worked in the U.S. defense intelligence community for nearly 40 years as a Marine Corps signals intelligence and electronic warfare officer and a civilian analyst with the Naval Criminal Investigative Service. A student of naval espionage history, he has previously published three popular history magazine articles covering espionage and counterespionage cases from the American Civil War, World War I, and pre-World War II eras. He graduated from Virginia Tech in 1983 with a degree in history and, having completed the Marine Corps Platoon Leaders Class, was commissioned as an officer in the Marine Corps. He served as a company commander with the 2d Radio Battalion with deployments to Honduras and Panama before transitioning to the Marine Corps Reserve. He joined the Naval Investigative Service in 1989 as a counterespionage and counterterrorism analyst, serving in a variety of roles in the United States, Central America, Europe, and Asia for the next 35 years and receiving five national individual or team counterintelligence awards.