REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
20-03-2020	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE
Revitalizing Counterintelligence: A Strategic Approach for Great Power Competition

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Child, Derek J.

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

With a clear understanding of the value of counterintelligence, while also taking into account a U.S. strategic culture that emphasizes transparency and democratic values, the United States can develop a robust counterintelligence apparatus and strategy for its use that will help ensure the United States retains its influence and power within the international system.

15. SUBJECT TERMS
Counterintelligence, Chinese intelligence services, great power competition

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	32	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

Revitalizing Counterintelligence: A Strategic Approach for Great Power Competition

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Derek J. Child

AY 2019-20

Mentor and Oral Defense Committee Member: Richard Hegmann, PhD
Approved: [signature]
Date: 20MAR20

Oral Defense Committee Member: Christopher Hartley
Approved: [signature]
Date: 20 Mar 20

Disclaimer

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Preface

The focus of this paper is counterintelligence and its value as an instrument of national power. I selected this topic based on my observations working for the U.S. Department of Defense and my experience at the Marine Corps Command and Staff College (CSC) during the 2019-2020 academic year. Although the proper label for the current international security environment is up for debate, one truth is unassailable: the United States faces a complex array of national security challenges, including state and non-state actors' pursuit of policies that undermine U.S. strategic interests. However, the United States at times does not fully utilize the immense resources it has in a coherent fashion to combat these threats. For this paper, I chose to highlight counterintelligence because those with experience working in this discipline have a clear understanding of its value to policymakers and warfighters, but know that it is rarely, if ever, considered an instrument of national power. Moreover, there has been no rigorous, public discussion of the role of counterintelligence in supporting the 2018 National Defense Strategy. Therefore, my hope is that this paper's findings will contribute to ongoing discussions about instruments of power and the manner in which the United States can maintain its competitive edge in today's international security environment.

I would like to acknowledge the assistance of Dr. Richard Hegmann, the CIA Chair at Marine Corps University (MCU), who served as my CSC Faculty Advisor for this project. I would also like to thank the military and civilian faculty at CSC for the well-organized and challenging curriculum, which stimulated my academic curiosity and will allow me to make more substantial contributions to the defense of the United States.

Executive Summary

Within the U.S. government, counterintelligence is an underappreciated and underutilized instrument of national power. In the current era of great power competition, this situation undermines U.S. national security because many U.S. adversaries and peer competitors prioritize counterintelligence and integrate it effectively into their strategic decision-making vis-à-vis the United States. Employing counterintelligence more effectively requires a proper understanding of what counterintelligence is and how it can be used in conjunction with other instruments of national power. This paper emphasizes the strategic effects counterintelligence can create in the cognitive domain, and defines counterintelligence as "*a deliberate series of actions taken to shape the perceptions and actions of an adversary's intelligence apparatus in a way favorable to national security, while simultaneously protecting U.S. interests from adversaries' intelligence activities*." Using counterintelligence through these three mutually-supporting elements — deliberation, targeting of an adversary's intelligence service to produce strategic effects, and safeguarding U.S. national security interests — can improve our use of counterintelligence as a tool of statecraft.

In addition to improving the conceptual understanding of counterintelligence, there are a number of actions the United States can take to revitalize its use of counterintelligence. For example, analysis of the ancient Chinese appreciation for counterintelligence principles provides U.S. national security practitioners unique insights into how Beijing is navigating the current era of great power competition. In addition, modifications to the U.S. counterintelligence enterprise, its approach to counterintelligence analysis, its partnership with private industry, and outreach to the American public can help assure the U.S. competitive edge within the international system far into the twenty-first century.

Table of Contents

Page

Introduction

Counterintelligence is often underutilized and misunderstood within the U.S. government, which prevents its strategic application as an instrument of national power. During the low-intensity conflicts in Iraq and Afghanistan that the U.S. military has been involved with during the past two decades, ineffective or insufficient use of counterintelligence resulted in tactical setbacks, but in the current period of great power competition described in the National Defense Strategy, such lapses risk fundamentally harming U.S. national security. In contrast, U.S. adversaries and peer competitors like China consider intelligence and counterintelligence to be integral elements of their national strategies, and key tools for undermining the U.S. position as the dominant world power.

As a means to enhance the understanding and employment of counterintelligence among U.S. policymakers, intelligence practitioners, and the military, this paper will employ both conceptual and practical approaches to argue for the importance of counterintelligence in today's period of great power competition. First, the paper will offer a refined definition of counterintelligence and point out its most relevant aspects to demonstrate how it can be used to strengthen the national security of the United States. Second, it will examine how a peer competitor, China, incorporates counterintelligence into its national strategy based on that country's strategic culture and historical legacy of warfare. Third, it will provide a series of recommendations that will help guide the United States toward more effective counterintelligence at the strategic level. With a clear understanding of the value of counterintelligence, while also taking into account a U.S. strategic culture that emphasizes transparency and democratic values, the United States can develop a robust counterintelligence

apparatus and strategy for its use that will help ensure the United States retains its influence and power within the international system.

Defining Counterintelligence Concepts

Because counterintelligence is so often overlooked or poorly understood, policymakers at times do not appear to fully appreciate its basic tenets and vital role within the national security process. The many competing, often contradictory, explanations of the purpose of counterintelligence furthers confusion.[1] Moreover, most counterintelligence definitions are limited in scope because they focus solely on defensive measures, that is, protecting against the activities of foreign intelligence services. These defensive measures are important but fail to encompass the full scope of counterintelligence.[2] Other definitions, such as that found in Executive Order (E.O.) 12333, are valid but too long and detailed, which can mask the applicability of counterintelligence for strategic decision-making.[i]

This paper defines counterintelligence as "*a deliberate series of actions taken to shape the perceptions and actions of an adversary's intelligence apparatus in a way favorable to national security, while simultaneously protecting U.S. interests from adversaries' intelligence activities*." This definition has better utility in an era of great power competition because it highlights the strategic effects that counterintelligence can produce. Furthermore, this definition emphasizes the effects counterintelligence can create in the cognitive domain. Military theorist Carl von Clausewitz recognized the cognitive domain as the critical aspect of warfare when he wrote that the ultimate aim of warfare is "to compel the other to do our will," and that only by doing so can military force achieve success.[3] Likewise, this cognitive component applies to the

[i] E.O. 12333 defines counterintelligence as "Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."

broader peacetime competition across military, diplomatic, economic, and information arenas. The three mutually-supportive elements that help ensure counterintelligence can achieve victory in the cognitive domain — all of which are included in the definition above — include deliberation; targeting of a specific adversary's intelligence apparatus to achieve a strategic effect; and guarding U.S. national security interests against the intelligence operations of its adversaries. The remainder of this section will examine each of these aspects.

The foremost principle of effective counterintelligence is that it is deliberate, not reactive. Too often, the United States recognizes the importance of counterintelligence *after* a spy is arrested for working for a foreign intelligence service, *after* a terrorist attack, or *after* a leak of classified information to the media. Certainly, post-mortem damage assessments that lead to revised security measures are helpful in the aftermath of such events. However, the deliberative and anticipatory nature of counterintelligence is what can make it a valuable weapon in the national security toolkit. Deliberation requires planning, the importance of which is exhibited at the highest levels of government when the National Security Council is considering any major policy decision, or when the U.S. military is planning an operation. The Marine Corps Planning Process, for example, is a six-step process that commanders and their staffs use to frame a problem, develop multiple courses of action, and test those courses of action to provide well-developed options for leadership.[4]

Counterintelligence shares many commonalities with military deception, with the primary difference being that its focus is the adversary's intelligence apparatus, rather than foreign military leadership or units. However, the two disciplines overlap because intelligence inputs can influence military decision-making. Military deception exemplifies the deliberative process that should define all counterintelligence operations. Barton Whaley, a military deception

expert, outlines a ten-step planning process required for successful deception. Key elements of this process include understanding the goal of the operation, deciding the desired adversary reactions and perceptions, and determining the channels by which information will be communicated to the enemy, for example human intelligence, signals intelligence, or open-source media.[5] Similar to other national security operations, such as covert action or cyber operations, detailed planning is essential, and effective counterintelligence cannot simply serve as an afterthought for policymakers or warfighters.

RAND researcher Scott Gerwehr describes the counterintelligence planning process as "planning backwards," or alternatively, a reverse of the Observe-Orient-Decide-Act (OODA) Loop decision cycle that U.S. Air Force Colonel John Boyd developed in the 1950s.[6] Similar to reverse engineering, the process begins with the desired end state, such as convincing Hitler that the Allies' D-Day landings would occur at Pas de Calais, rather than Normandy. The next step requires identifying the key branch points that lead to the desired end state. Using the D-Day landing example, this step might involve convincing Germany's military intelligence service, the *Abwehr*, of the Pas de Calais landing. The third step, orientation, is the development of a story the opponent must believe to take the desired actions. Keeping with the D-Day example, this might involve passing material to Germany's human sources, or using electronic or radio communications channels known to be tapped by Germany to portray an Allied troop build-up preparing for Pas de Calais.[ii] Lastly, in the observables stage, there is an identification of the set of observables that would lead to the opponent believing the story. This might entail having an agent-in-place within the German intelligence establishment capable of reporting back to the

[ii] Victor Melendez Jr., a counterintelligence officer working for the U.S. Navy, points out that those conducting deception operations that target an enemy intelligence service will need to recognize when it is appropriate to provide accurate information in addition to false information. Authentic passage material is valuable for shaping the adversary's decision-making and building up credibility so that the passage of false information can have an even greater strategic effect.

Allies how the passage material or disinformation is being received so that the Allies can refine their operations.

The second key element of counterintelligence is that it targets a specific adversary's intelligence apparatus to achieve a desired strategic effect. Its ability to achieve strategic effects means that counterintelligence is an instrument of national power similar to diplomatic, informational, military, and economic measures. Moreover, as Robert Jervis argues, counterintelligence can only achieve its full potential when it is conducted in close coordination with these other instruments of national power.[7] Roy Godson and James Wirtz, academics specializing in counterintelligence and deception, similarly stress the importance of "strategic coherence" when using this important national security tool.[8]

Even so, counterintelligence is not always suitable, acceptable, or feasible, and national security practitioners will need to have keen insights into the situation and the adversary to recognize when it is the appropriate instrument to use. Moreover, the action needs to be suitable, acceptable, and feasible for the larger strategy.[9] Arguably, there is no "one-size-fits-all" counterintelligence approach that works against multiple actors, especially offensive operations like the use of double agents. Each operation must be tailored to the specific enemy as well as to the desired end state. Mirror-imaging U.S. perceptions onto the opponent must be avoided, as well as acknowledgment that just because a counterintelligence operation worked against an enemy in the past, it does not necessarily mean it will work again. Finally, it is important for counterintelligence, as with other instruments of national power, to determine when it should *not* be employed. As Harry Yarger writes in his discussion of strategy, "The strategist must determine if the end justifies the risks of initiating action."[10]

A variety of counterintelligence means are available to shape a foreign intelligence service's perceptions or actions. Typically, these means entail the use of *offensive* counterintelligence operations, which the pseudonymous Christopher Felix describes as seeking to influence the adversary's decision-makers: "luring your opponent into doing voluntarily and by choice what you want them to do."[11] Intelligence and counterintelligence specialists like Mark Lowenthal, John Ehrman, and Paul Redmond have identified various types of operations, including deception, double agents, and disinformation, among others.[12] Prior to the twenty-first century, human intelligence operations were the dominant means of conducting these operations. Now, cyber-, information-, and space-based operations provide additional means to influence the actions of state and non-state intelligence entities. As argued by Victor Melendez Jr. when describing the value of these types of operations for the U.S. Navy, the only limits are the deceivers' own creativity.[13]

The last component of counterintelligence, protecting the United States against its adversaries' intelligence services — or the comparable security apparatus of non-state actors like terrorists and transnational criminal organizations — is what former National Counterintelligence Executive Michelle Van Cleave refers to as the "shield."[14] It is often the aspect of counterintelligence that receives the most attention within the U.S. national security apparatus and the American public because it is the most easily understood. This aspect of counterintelligence involves ensuring the reliability and integrity of the national security system, including personnel, information systems, facilities, and information.[15]

Analysis is crucial to all aspects of counterintelligence, and it is equally important for informing this defensive side of counterintelligence. According to Ehrman, the study of foreign intelligence entities — an analytical process — is the foundation of counterintelligence because

the United States cannot develop appropriate countermeasures without an accurate understanding of the distinctive behavior and priorities of these entities.[16] Van Cleave agrees, stating that "the first job of counterintelligence is to identify the foreign intelligence activities directed against the United States and its interests," with the intent to inform protective security measures like cyber and personnel security, physical security, and information classification.[17] In addition, Van Cleave notes the unique responsibility counterintelligence analysts have not only to develop expertise in the capabilities of adversaries' intelligence services, but also to identify "anomalies," a type of forensic analysis that can link seemingly disparate patterns of activities to uncover foreign actions that suggest a foreign intelligence entity may have access to sensitive U.S. national security information.[18]

In summary, counterintelligence involves more than just security, law enforcement, or defending against the intelligence actions of our adversaries: it is an instrument of national power that can be incorporated into a broader strategy. Moreover, in warfare, it is one of the most valuable tools for assuring victory because of its focus on defeating the enemy in the cognitive domain by pre-determining an adversary's actions or shaping its perceptions of how the United States will act. Therefore, as with any instrument of national power, its use requires a deliberative planning process that ensures buy-in from relevant members of the national security enterprise. In addition, effective counterintelligence operations should be tailored to a specific adversarial intelligence entity to achieve a desired outcome, which will entail a thorough understanding of the adversary's strategic culture and intelligence capabilities. This end state must align with the actions of the other instruments of national power so as not to be at cross-purposes. Finally, there are some aspects of counterintelligence that are defense-oriented,

specifically the protection of the U.S. national security enterprise against state and non-state intelligence entities that seek to do it harm.

China's Application of Counterintelligence

Armed with a conceptual understanding of what encompasses counterintelligence and how it can be used to further U.S. strategic objectives, it is now useful to analyze the importance that U.S. adversaries attach to intelligence and counterintelligence at the strategic level. This section will examine China's historical legacy of using counterintelligence principles and how this legacy continues to shape Beijing's strategic culture. This analysis can assist the U.S. national security community by deriving lessons learned and identifying some best practices. Even more importantly, insights into Chinese intelligence practices and priorities can highlight U.S. vulnerabilities that can be strengthened and countermeasures that can be developed to retain the U.S. competitive edge in an era of great power competition.

China is the most relevant competitor to study because of its vast military, economic, and intelligence resources, and the high esteem with which it regards counterintelligence. Moreover, it has over two millennia of written and oral history discussing the utility of intelligence and counterintelligence in warfare. Although it is difficult to synthesize over 2,500 years of Chinese warfare, we can distill certain principles that continue to influence modern Chinese security practices and strategy. As Thomas Mahnken argues, most Chinese military leaders and strategic thinkers believe that ancient Chinese values and war-fighting principles remain relevant, and ancient Chinese texts are central to the identity of the Chinese security establishment.[19] One area of consistency that has dominated Chinese national security strategy and practice through the millennia has been an emphasis on deceiving the enemy.

The Chinese emphasis on deception is nested within the cultural concept of *Shih*. This concept has a variety of meanings based on the context within which it is used, but it is most often associated with power, force, or influence.[20] In a military context, a *Shih*-based strategy is one that focuses on the enemy's intent and plans rather than one's own military forces.[21] *Shih* may be endogenous — residing within an army, a commander, a ruler, or the people — or exogenous, found within external conditions like terrain, weaponry, and time.[22] The essence of *Shih* is that it is a dynamic state of power that combines material, human, and natural factors, and a variety of Chinese security theorists and practitioners have made it a foundational aspect of their ideas and actions.[23]

The most well-known and arguably most influential Chinese military theorist focused on deceiving the enemy was Sun Tzu, who is credited with the ubiquitous statement that "all warfare is based on deception."[24] In Sun Tzu's *The Art of War*, written during the Warring States Period (403-221 BCE), he claims that "warfare is the Dao [Way] of deception" and enemies must be "tricked and maneuvered, lured and enticed, frustrated and enervated" to create a strategic imbalance.[25] The chapter in *The Art of War* titled "Employing Spies," widely considered the world's first theoretical discussion of spycraft, addresses the importance of double agents, which Sun Tzu held in high esteem as the most likely to provide accurate and detailed information about an enemy's internal situation because of their placement and access.[26] Regarding *Shih*, Sun Tzu exhorted that it was the key to all military victories because it could break an enemy's resistance without fighting, a clear acknowledgement of the importance of the cognitive realm of warfare.[27] Another important aspect of counterintelligence addressed in *The Art of War* is secrecy, the requirement to protect critical national security information. According to Ralph Sawyer, a U.S. scholar specializing in Chinese warfare, for Sun Tzu, secrecy

not only allowed a military force to hide its intent and act in an unpredictable manner, it also opened up possibilities for conducting disinformation, deception, and other unorthodox operations that could further the state's national security goals.[28]

Sun Tzu offered many additional insights into warfare in his writings, but it was his focus on unorthodox measures like deception and secrecy that gained traction during the Warring States period and throughout the later period of conflict that established the Han Dynasty.[29] According to Sawyer, the application of these measures into military doctrine and practice during this turbulent period was so extensive, that "many unorthodox techniques became virtually orthodox."[30] Sun Tzu's influence was also apparent in the actions and writings of Mao Tse-Tung in the 1900s. Like Sun Tzu, Mao emphasized the importance of using deception to force the enemy to make erroneous judgments and take erroneous actions.[31] In other words, Mao recognized that focusing on the enemy's mind and manipulating it to meet one's own objectives was one of the most salient aspects for success in warfare.

Although Sun Tzu receives most of the credit from the West for his conceptual understanding of deception and application of *Shih*, several other Chinese theorists and ancient military narratives advocated a *Shih*-based approach that continues to shape modern Chinese national security thinking. For example, the *Tradition of Tso* (circa 770-403 BCE) emphasized the importance of intelligence in warfare, notably referring to the importance of operations that deceived adversaries and denied them certain information.[32] The book *Thirty-Six Stratagems*, which originated in oral and written Chinese history nearly 2,000 years ago, describes the use of deception as an enabler for other instruments of power.[33]

These ancient Chinese military histories and teachings contributed to the development of a strategic culture that, today, emphasizes deception and other intelligence operations to further

national security interests. For example, *The Science of Military Strategy*, a foundational contemporary document, considers stratagem, loosely defined as a type of strategic cleverness emphasizing deception, to be one of the six primary focus areas of military science.[34] China's contemporary intelligence apparatus has multiple civilian and military entities responsible for conducting intelligence and counterintelligence operations in support of strategic objectives, and these organizations and their leaders are deeply interwoven.[35] One of these agencies is the Ministry of State Security (MSS), which combines functions similar to those of the CIA and FBI and has officers both overseas and inside China for counterintelligence purposes. The Ministry of Public Security is a national police force that mirrors the MSS structure and it also contributes to counterintelligence operations. Within the military, intelligence and counterintelligence functions reside within the People's Liberation Army (PLA) General Staff Department, the General Political Department, and the PLA Navy and Air Force.[36] According to China expert Peter Mattis, the intelligence efforts of these various entities are thoughtful, deliberate, well-informed, and are tied closely to national strategic objectives.[37]

In sum, China has a long-established affinity for using the main principles of counterintelligence, and this strategic culture allows Beijing to incorporate counterintelligence into a broader strategy. As it has done throughout its history, the Chinese national security enterprise continues to promulgate strategies that combine a target-based approach with an emphasis on achieving victory in the cognitive domain. An example is a document released in 2003 titled "Political Work Guidelines of the People's Liberation Army." The document describes a three-pronged warfare strategy applied by China that focuses heavily on psychological and informational elements.[38] As former U.S. military intelligence analyst Nicholas Eftimiades attests, Chinese policymakers have a keen appreciation for the proper

application of intelligence and counterintelligence activities in support of the state. As such, China's intelligence apparatus "is inextricably linked to the foreign policy decision-making process…economic development and political control."[39] Xuezhi Guo, an expert on China's internal security apparatus, concurs that Beijing views its intelligence operations as "indispensable" to furthering China's industrialization and modernization efforts, while also serving as the shield that keeps the Chinese Communist Party in power, an acknowledgement of the important defensive aspects of counterintelligence.[40] A comprehensive *Shih*-based strategy, which incorporates deception and other means to manipulate the actions of the United States and its allies, provides an overarching foundation for China's current objectives of excluding the United States from the Pacific region and ultimately ending U.S. hegemony over the international system.[41]

Toward an Improved U.S. Counterintelligence Framework

What are the main differences between China's approach to counterintelligence to that of the United States, and more importantly, what are the implications for U.S. national security? U.S. strategic documents, especially those directly tied to how the United States will achieve its national security objectives, attach little, if any, importance to manipulating the activities of the enemy. As a result, the United States approaches counterintelligence in a haphazard manner, making it difficult for U.S. national security practitioners to integrate counterintelligence operations into a coherent strategy. Certainly, the inherent differences between the authoritarian People's Republic of China and the liberal, democratic United States are major factors for the different perspectives on employing deception and other aspects of counterintelligence.[42] However, there are ways for the United States to strengthen its counterintelligence capabilities without compromising its democratic principles.

Based on the conceptual foundation of counterintelligence outlined in the first part of this paper, combined with an understanding of how U.S. adversaries use counterintelligence to advance their interests, it is possible to propose a new counterintelligence framework appropriate for the United States. A full-scale "Revolution in Counterintelligence Affairs" probably is not necessary because the United States already has the majority of the agencies, systems, personnel, and financial resources it needs to address many of its counterintelligence deficiencies. However, a fresh approach to counterintelligence is required to compete with our adversaries in the current era of great power competition, and to protect the American way of life and core national security interests. This paper offers eight recommendations to improve the manner in which the U.S. government understands and employs counterintelligence to achieve its strategic interests. These recommendations emphasize a realistic approach that would require only minimal investments in additional personnel and resources.

First, ***individuals responsible for making decisions regarding the core national security interests of the United States are likely to have greater success if they understand what counterintelligence is (and is not) so that they can recognize its utility as an instrument of national power***. Frederick Wettering has observed a multitude of factors explaining why counterintelligence is not prominent when important national security decisions are being made in the United States. These factors include the American public's suspicions of a too-powerful federal government; the reaction to the abuses of the CIA and FBI outlined in the Church and Pike Committee Reports of the 1970s; the uncooperative nature of bureaucracies; a cultural aversion to informing, informers, and secrecy; and a general perception of counterintelligence as a second-class profession.[43] The first section of this paper sought to balance these negatives by providing a common understanding of counterintelligence that highlights its most salient aspects

and benefits for strategic decision-making. Without understanding the basic premises of counterintelligence, it is difficult, if not impossible, to use it to obtain strategic effects.

Second, in order to strengthen the effectiveness of counterintelligence, ***the United States should continually reassess its vulnerabilities and shortfalls*** in this area. Recognizing the shortfalls of U.S. counterintelligence is not new, and there is typically ample discussion in the aftermath of spy scandals or leaks of sensitive information. In 2005, the Silberman-Robb presidential commission determined that "U.S counterintelligence efforts have remained fractured, myopic, and only marginally effective."[44] Similar declarations of U.S. counterintelligence ineffectiveness appeared in prior decades. This paper argues that only the official recognition of counterintelligence as an instrument of national power and the formalization of its role in the policymaking process will allow it to achieve true success. Furthermore, reviews of U.S. counterintelligence operations and their shortfalls should not occur only after the arrest of a spy in the United States or a damaging intelligence leak. Congressional oversight must continue to play a significant role in overseeing the activities of the counterintelligence community and ensuring it is organized and resourced in a way to achieve success. Moreover, the National Counterintelligence and Security Center (NCSC), which The Counterintelligence Enhancement Act of 2002 established under the Office of the Director of National Intelligence, must find new and innovative ways to remain effective and relevant. Despite its creation eighteen years ago, the NCSC remains a mostly toothless organization. The NCSC need not be a mere administrative bureaucracy, and it should have an active role in strengthening the counterintelligence community — to include collection, operations, analysis, and investigations — and advocating for counterintelligence's role in the development and promulgation of U.S. national security strategy.

Third, ***the U.S. national security enterprise must maintain an up-to-date and thorough understanding of adversaries' intelligence capabilities, priorities, and intent***. One way to improve this understanding is by reinvigorating the counterintelligence analysis profession. As mentioned previously, analysis is a crucial counterintelligence activity because it informs not only policymakers, but also the other three components of the counterintelligence taxonomy: investigations, collection, and operations. However, as noted by Ehrman, U.S. policymakers have a tendency to ignore the unique contributions that counterintelligence analysts can bring to a problem set, such as understanding the outsized influence that intelligence services have in authoritarian states compared to other government entities.[45] Therefore, analysts have less motivation to pursue careers in counterintelligence, opting instead for what they perceive are more important accounts, such as regional, counterterrorism, counterproliferation, political-military, or economics analysis. One way to address this situation would be national-level guidance to raise the analytical priority of counterintelligence issues within the Intelligence Community. This could happen by modifying counterintelligence's ranking within the National Intelligence Priorities Framework. Another option would be the creation of a strategic, interagency counterintelligence center modeled after the National Counterterrorism Center. Analysts from across the Intelligence Community could serve there on a rotational basis and provide strategic-level production focused on specific foreign intelligence services, trends, and risks to U.S. national security interests. Additionally, in the event of another scenario similar to *Wikileaks* or the Edward Snowden revelations, damage assessment task forces could be stood up "in-house," with only minimal, additional support required from the rest of the Intelligence Community. The CIA's stand-up of the Mission Center for Counterintelligence in 2015 demonstrates the importance of unifying counterintelligence capabilities, but an interagency

Center that brings together analysts from CIA, DOD, and elsewhere would be even more effective in addressing modern security challenges.

Fourth, and closely related to the aforementioned analytical recommendation, ***the impact of counterintelligence analysis would improve with a more clearly delineated policymaker customer set***. As academic Jennifer Sims correctly points out, "the intelligence process begins and ends with the decision maker who needs its support. Successful performance requires a locus in the government for deciding who needs to be getting intelligence on threats and opportunities…Without getting this right, an intelligence system is doomed to fail, since it can be neither relevant nor timely."[46] Unlike other analytical disciplines throughout the Intelligence Community, there is no clearly defined set of counterintelligence customers who drive production or issue analytical requirements. For example, it is easy for CIA political analysts working on Iran to figure out who their customers are within the White House, the Pentagon, and State Department because there are clear-cut policymaker positions and offices dealing with those issues. No such clarity exists for a counterintelligence analyst, making initiative production difficult, and tasked production almost non-existent. This lack of clarity can create a perception that there is little appetite for counterintelligence analysis among policymakers, which further impedes analysts from pursuing counterintelligence careers. Within DOD, one possible solution would be the creation of an Assistant Secretary of Defense-level position responsible for counterintelligence. The creation of such a position would ensure that all relevant analysis on counterintelligence trends or concerns is routed properly and incorporated into strategic decision-making within the Pentagon. If such a position proved successful, equivalent positions could then be established elsewhere, such as at the National Security Council and the State Department.

Fifth, as a means to inculcate a counterintelligence mindset among policymakers and warfighters, ***counterintelligence should be incorporated into the curricula of professional military education (PME) and similar higher-level education for other national security professionals***. Currently, there is a lack of study on counterintelligence and deception in U.S. PME. When deception is mentioned, for example during war planning exercises, it is generally an afterthought and there is little rigor applied to deceiving hypothetical enemy forces, let alone an actual adversary. There is ample space within the curricula of the various services' PME to incorporate historical case studies of successful counterintelligence operations to demonstrate the discipline's strategic utility. Moreover, planners with previous experience contributing to the counterintelligence portions of U.S. war plans should be brought in to share lessons learned. To achieve the most beneficial results, counterintelligence should be addressed during the portion of the curriculum that discusses operations in the information environment because of the linkages with achieving victory in the cognitive domain. If the U.S. military truly considers information to be a war-fighting function, then it should be apparent that the manipulation of information provided to an adversary's intelligence service should be a critical learning requirement for future planners and senior commanders.

Sixth, in recognition of the critical counterintelligence threat that states like China pose to the United States, ***there should be stronger collaboration between the U.S. government and private industry***. As with other instruments of national power, counterintelligence's effectiveness depends in large part on coordination with other elements of the government. Increasingly, because of adversaries' emphasis on the cyber and informational domains to penetrate and manipulate U.S. national security interests, a strong counterintelligence strategy also requires collaboration with private industry. Darren Tromblay has suggested the creation of

a counterintelligence "hub" to work with private industry.[47] Realizing that counterintelligence is unlikely to receive considerable new financial resources in the near future, the creation of a new entity probably is not feasible. However, new units within the Department of Homeland Security, the FBI, and the NCSC could be stood up with the mission of strengthening relations with private industry and educating those workforces on the threats posed by hostile intelligence services. For example, the U.S. counterintelligence community should explain to private companies how China uses its intelligence apparatus to steal U.S. intellectual property, which costs the U.S. economy an estimated $225 billion to $600 billion annually.[48] Conversely, private industry has a wealth of knowledge to share with the Intelligence Community on topics with counterintelligence implications, such as artificial intelligence, quantum computing, and other technological developments. The latest U.S. *National Counterintelligence Strategy*, released in February 2020, emphasizes the importance of working with private industry by mentioning the topic within each of its five priorities: protecting critical infrastructure, reducing threats to key U.S. supply chains, countering the exploitation of the U.S. economy, defending American democracy against foreign influence, and countering foreign intelligence cyber and technical operations.[49]

Seventh, ***national security policymakers and warfighters should prioritize the proactive elements of counterintelligence rather than the reactive elements***. The definition of counterintelligence used in this paper highlights the importance of this proactive approach when describing the deliberate nature of counterintelligence. James Gosler, in discussing the role of counterintelligence in combating the sophisticated array of technical intelligence threats facing the United States, concludes that the U.S. counterintelligence culture is too timid, and that the United States is too focused on the investigative pillar of counterintelligence, that is, reacting to

threats rather than preempting them or prompting them to occur in a way that aligns with U.S. interests.[50] This is not to suggest that the creation of security countermeasures or investigations of known or suspected spies are not important. Rather, this recommendation is about changing a mindset: focusing on the offensive capabilities of our counterintelligence assets to achieve greater strategic effect.

Finally, ***the United States needs to develop a counterintelligence strategy and architecture that conforms to American ideals, norms, and principles***. Paradoxically, this will require more transparency and openness with the American public regarding the threat posed by hostile intelligence services, despite secrecy being essential for the success of counterintelligence operations. When conducting counterintelligence operations and investigations, the U.S. Intelligence Community will almost always be at a tactical disadvantage compared to authoritarian regimes like China because the intelligence services of those countries are not bound by the same regulations, procedures, and oversight inherent to the U.S. system. Nevertheless, this tactical disadvantage can be turned into an operational and strategic advantage if the situation can be conveyed with candor and consistency to the American public. Whether it is via Intelligence Community leaders' Annual Threat Testimony to Congress, or in national security and defense strategies published by the White House and the Pentagon, the American people need constant reminders from national leaders regarding the pervasive threats that hostile intelligence services pose to U.S. national interests and the American way of life, and how these hostile entities seek to exploit our own freedoms and transparency to do us harm. Unfortunately, the only time that most Americans hear about counterintelligence is when an espionage case is mentioned in the media. The U.S. government should lean forward to publicize or declassify some of its recent counterintelligence successes to demonstrate the strategic value and necessity

of this intelligence discipline. Even though such revelations may provide hostile intelligence services with information about U.S. tactics, techniques, and procedures, the gains of getting buy-in from the American public should outweigh the risks. As Sims suggests, the "[American] public is not likely to oppose the more aggressive collection and even the proactive deception" that operating in the current international environment requires "so long as the rationale for operations remains tightly aligned with America's strategic purpose and appropriate oversight is in place."[51] Sims further emphasizes the pragmatism of Americans, noting, "secrecy and deceit can be tolerable when they are welded to a tolerable enterprise."[52] As the post-9/11 environment has demonstrated, Americans are willing to make exceptions for intelligence when there are obvious threats to national security. If Americans are convinced that successful counterintelligence operations can counter adversaries intent on undermining core American interests and create opportunities to bolster the U.S. geostrategic position, then they will most likely support changes that make counterintelligence a more consistent instrument of national power.

Conclusion

According to B.H. Liddell Hart, "While fighting is a physical act, its direction is a mental process. The better your strategy, the easier you will gain the upper hand, and the less it will cost you."[53] Although he was writing about strategy in general, his observation serves as a critical reminder that, as in war, maintaining the strategic edge in today's international security environment will require the United States to maintain its advantage in the cognitive battlespace. As discussed in this paper, the proper employment of counterintelligence as an instrument of national power is one manner in which the United States can do so. For the United States to remain ahead of its adversaries, it needs to accomplish three tasks that only counterintelligence

can provide: know what the adversary's intelligence services are doing and intend to do, manipulate those actions in a manner beneficial to U.S. interests, and keep vital national security information out of the enemy's hands. These actions not only strengthen U.S. national security on their own merit, but they also enhance the effects of the other U.S. instruments of national power.

The creation of a strategic culture within the U.S. national security enterprise that recognizes the importance of counterintelligence as an instrument of national power will not be a simple task. For one, it will require a new strategic mindset in which the United States is continually on the offensive to seek victory in the cognitive domain. Moreover, successful counterintelligence operations require such high levels of sophistication, ingenuity, creativity, and risk-taking that it will be a challenge to convince the American public and national security leaders of its necessity during a time when the United States is not engaged in overt combat with a peer or near-peer adversary.[54] However, this paper argues that there is no better time than now to develop U.S. expertise in this discipline and take actions against current, or potential future, adversaries. State actors like Russia and China are already doing so, and in the case of China, its security services have been honing their tradecraft for more than two thousand years. If the United States continues to accept a counterintelligence enterprise that is only "marginally effective," our adversaries will continue to exploit one of our few national security vulnerabilities and undermine our dominant position within the international system. If, however, the United States recognizes the value of counterintelligence and incorporates it into its strategic decision-making, our competitive edge can be assured far into the twenty-first century.

[1] John Ehrman, "What Are We Talking About When We Talk About Counterintelligence?" in *Intelligence: Volume III: Counterintelligence: Shield for National Security Intelligence,* ed. Loch K. Johnson (London: Routledge, 2011), 6-7.

[2] Darren E. Tromblay, "Counterintelligence Needs Reboot for 21st Century," *The Hill*, October 31, 2017, https://thehill.com/opinion/national-security/358075-counterintelligence-needs-reboot-for-21st-century.

[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 75.

[4] Headquarters US Marine Corps, *Marine Corps Planning Process*, MCWP 5-10 (Washington, D.C.: Headquarters U.S. Marine Corps, May 2, 2016).

[5] Barton Whaley, *Practise to Deceive: Learning Curves of Military Deception Planners* (Annapolis, MD: Naval Institute Press, 2016), 180-182.

[6] Robert M. Clark and William L. Mitchell, *Deception: Counterdeception and Counterintelligence* (Los Angeles, CA: CQ Press, 2019), 37-38.

[7] Robert Jervis, "Intelligence, Counterintelligence, Perception, and Deception," in *Intelligence: Volume III: Counterintelligence: Shield for National Security Intelligence,* ed. Loch K. Johnson (London: Routledge, 2011), 34.

[8] Roy Godson and James J. Wirtz, "Strategic Denial and Deception," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, eds. Roy Godson and James J. Wirtz (Washington, D.C.: National Strategy Information Center, 2002), 3.

[9] Harry Yarger, *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle, PA: Strategic Studies Institute, 2006), 68.

[10] Yarger, 67.

[11] Christopher Felix, *A Short Course in the Secret War* (Lanham, MD: Madison Books, 2001), 128.

[12] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (United Kingdom: CQ Press, 2012), 222.

[13] Victor M. Melendez Jr., "Counterintelligence: An Asymmetric Warfighting Tool for the U.S. Navy," in *International Journal of Intelligence and Counterintelligence*, 32:4, 2019, 750.

[14] Michelle Van Cleave, *Counterintelligence and National Strategy* (Washington, D.C.: National Defense University Press, 2007), 3.

[15] National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America," in *21st Century Counterintelligence*, ed. John Deady (New York: Nova Science, 2009), 6-7.

[16] Ehrman, 5.

[17] Van Cleave, 6.

[18] *Ibid*.

[19] Thomas G. Mahnken, *Security and Stratagem: Understanding Chinese Strategic Culture* (Australia: Lowy Institute for International Policy, 2011), 3.

[20] William H. Mott IV and Jae Chang Kim, *The Philosophy of Chinese Military Culture: Shih vs. Li* (New York, NY: Palgrave Macmillan, 2006), 15.

[21] Mott IV and Jae Chang Kim, 12.

[22] Mott IV and Jae Chang Kim, 15-16.

[23] Mott IV and Jae Chang Kim, 18.

[24] M. R. D. Foot, "Conditions Making for Success and Failure of Denial and Deception: Democratic Regimes," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, eds. Roy Godson and James J. Wirtz (Washington, D.C.: National Strategy Information Center, 2002), 95.

[25] Ralph D. Sawyer, "Subversive Information: The Historical Thrust of Chinese Intelligence," in *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*, eds Philip H.J. Davies and Kristian Gustafson (Washington, D.C.: Georgetown University Press, 2013), 30-31.

[26] Ralph D. Sawyer, "Subversive Information: The Historical Thrust of Chinese Intelligence," in *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*, eds Philip H.J. Davies and Kristian Gustafson (Washington, D.C.: Georgetown University Press, 2013), 36.

[27] Mott IV and Jae Chang Kim, 15.

[28] Ralph D. Sawyer, *The Tao of Deception: Unorthodox Warfare in Historic and Modern China* (New York: Basic Books, 2007), 387.

[29] Ralph D. Sawyer, *The Tao of Deception: Unorthodox Warfare in Historic and Modern China* (New York: Basic Books, 2007), 69.

[30] Ralph D. Sawyer, *The Tao of Deception: Unorthodox Warfare in Historic and Modern China* (New York: Basic Books, 2007), 97-98.

[31] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 55.

[32] Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), 4.

[33] Clark and Mitchell, 14.

[34] Mahnken, 24.

[35] Xuezhi Guo, *China's Security State: Philosophy, Evolution, and Politics* (Cambridge: Cambridge University Press, 2012), 445.

[36] Peter Mattis, "A Guide to Chinese Intelligence Operations," *War on the Rocks*, August 18, 2015 https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/.

[37] *Ibid*.

[38] Sergio Miracola, "Chinese Hybrid Warfare," *Instituto Per Gli Sudi di Politica Internazionale (ISPI)* December 21, 2018 https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853.

[39] Eftimiades, 4.

[40] Guo, 441-445.

[41] Ralph D. Sawyer, *The Tao of Deception: Unorthodox Warfare in Historic and Modern China* (New York: Basic Books, 2007), 390-391.

[42] Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* (Washington, D.C.: National Strategy Information Center, 1995), 249.

[43] Frederick L. Wettering, "Counterintelligence: The Broken Triad," in *Intelligence: Volume III: Counterintelligence: Shield for National Security Intelligence*, ed. Loch K. Johnson (London: Routledge, 2011), 225 and 248.

[44] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, D.C.: Government Printing Office, 2005), 490.

[45] Ehrman, 15.

[46] Jennifer Sims, "Understanding Ourselves," in *Transforming U.S. Intelligence*, eds. Jennifer Sims and Berton Gerber (Washington, D.C.: Georgetown University Press, 2005), 41.

[47] Tromblay.

[48] The Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (The National Bureau of Asian Research, 2017), 1.

[49] National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States of America 2020-2022* January 7, 2020.

[50] James R. Gosler, "Counterintelligence: Too Narrowly Practiced," in *Vaults, Mirrors and Masks: Rediscovering U.S. Counterintelligence,* eds. Jennifer Sims and Burton Gerber (Washington, D.C.: Georgetown University Press, 2009), 193.

[51] Jennifer Sims, "Understanding Ourselves," in *Transforming U.S. Intelligence*, eds. Jennifer Sims and Berton Gerber (Washington, D.C.: Georgetown University Press, 2005), 54.

[52] Jennifer Sims, "Understanding Ourselves," in *Transforming U.S. Intelligence,* eds. Jennifer Sims and Berton Gerber (Washington, D.C.: Georgetown University Press, 2005), 34.

[53] B.H. Liddell Hart, *The Strategy of Indirect Approach* (London: Faber and Faber Limited, 1967), 207.

[54] Foot, 127.

Bibliography

Bozeman, Adda B. *Strategic Intelligence & Statecraft*. McLean, VA: Brassey's (US), Inc., 1992.

Clark Robert M. and William Mitchell. *Deception: Counterdeception and Counterintelligence*. Los Angeles, CA: CQ Press, 2019.

Clausewitz, Carl von. *On War*. Ed. and trans. Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*. Washington, D.C.: Government Printing Office, 2005.

Commission on the Theft of American Intellectual Property. *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*. The National Bureau of Asian Research, 2017.

Davies, Philip H. J. and Kristian C. Gustafson, eds. *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*. Washington, D.C.: Georgetown University Press, 2013.

Deady, John M., ed. *21st Century Counterintelligence*. New York: Nova Science, 2009.

Eftimiades, Nicholas. *Chinese Intelligence Operations*. Annapolis, MD: Naval Institute Press, 1994.

Ehrman, John. "Toward a Theory of Counterintelligence: What are We Talking About When We Talk About Counterintelligence?" In *Studies in Intelligence*, 53, no. 2 (2009).

Felix, Christopher. *A Short Course in the Secret War*. 4th edition. Lanham, MD: Madison Books, 2001.

Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*. Washington, D.C.: National Strategy Information Center, 1995.

Godson, Roy and James Wirtz, eds. *Strategic Denial and Deception: The Twenty-First Century Challenge*. Washington, D.C.: National Strategy Information Center, 2002.

Golovin, Andreas H., ed. *Fundamental Elements of the Counterintelligence Discipline*. New York: Nova Science Publishers, 2009.

Guo, Xuezhi. *China's Security State: Philosophy, Evolution, and Politics*. Cambridge: Cambridge University Press, 2012.

Headquarters US Marine Corps. *Marine Corps Planning Process*. MCWP 5-10. Washington, D.C.: Headquarters US Marine Corps, May 2, 2016.

Holt, Pat M. *Secret Intelligence and Public Policy: A Dilemma of Democracy*. Washington, D.C.: Congressional Quarterly Inc., 1995.

Liddell Hart, B.H. *The Strategy of Indirect Approach*. London: Faber and Faber Limited, 1967.

Johnson, Loch K., ed. *Critical Concepts in Military, Strategic & Security Studies: Volume III: Counterintelligence: Shield for National Security Intelligence*. London: Routledge, 2011.

Johnson, Loch K. *National Security Intelligence*. 2nd ed. United Kingdom: Polity Press, 2017.

Johnson, William R. *Thwarting Enemies at Home and Abroad: How to be a Counterintelligence Officer*. Washington, D.C.: Georgetown University Press, 2009.

Lahneman, William J. *Keeping U.S. Intelligence Effective*. Lanham, MD: The Scarecrow Press, Inc., 2011.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy.* 7th ed. United Kingdom: CQ Press, 2017.

Mahnken, Thomas G. *Secrecy and Stratagem: Understanding Chinese Strategic Culture*. Australia: Lowy Institute for International Policy, 2011.

Mattis, Peter L. "Assessing Western Perspectives on Chinese Intelligence." In *International Journal of Intelligence and Counterintelligence*, 25, no 4, (2012).

Mattis, Peter L. "Li Kenong and the Practice of Chinese Intelligence." In *International Journal of Intelligence and Counterintelligence*, 28, no. 3 (2015).

Melendez Jr., Victor M. "Counterintelligence: An Asymmetric Warfighting Tool for the U.S. Navy." In *International Journal of Intelligence and Counterintelligence*, 32, no. 4 (2019).

Mott IV, William H. and Jae Chang Kim. *The Philosophy of Chinese Military Culture: Shih vs. Li*. New York, NY: Palgrave Macmillan, 2006.

The Office of the Director of National Intelligence. *National Intelligence Strategy of the United States of America*. Washington, D.C., 2019.

Prunckun, Hank. *Counterintelligence Theory and Practice*. Lanham, MD: Rowman & Littlefield Publishers, 2012.

Sawyer, Ralph. *The Tao of Deception: Unorthodox Warfare in Historic and Modern China*. New York: Basic Books, 2007.

Sims, Jennifer and Burton Gerber, eds. *Transforming U.S. Intelligence*. Washington, D.C.: Georgetown University Press, 2005.

Sims, Jennifer and Burton Gerber, eds. *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*. Washington, D.C.: Georgetown University Press, 2009.

Stolberg, Alan. "Crafting National Interests in the 21st Century." In *U.S. Army War College Guide to National Security Issues: Volume II: National Security Policy and Strategy*. Ed. J. Boone Bartholomees, Jr. Carlisle, PA: U.S. Army War College, 2012.

Sun Tzu. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Van Cleave, Michelle. *Counterintelligence and National Strategy*. Washington, D.C.: National Defense University Press, 2007.

Varouhakis, Miron. "An Institutional-Level Theoretical Approach to Counterintelligence." In *International Journal of Intelligence and Counterintelligence*. 24, no. 3 (2011).

Whaley, Barton. *Practise to Deceive: Learning Curves of Military Deception Planners*. Annapolis, MD: Naval Institute Press, 2016.

The White House. *The National Security Strategy of the United States of America*. Washington, DC, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf/.

Yarger, Harry. *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. Carlisle, PA: Strategic Studies Institute, 2006.