More CI:
A Grand Theory of Counterintelligence for Intelligence Scholars and Practitioners in the United States

by Lee A. Lukoff

OVERVIEW

Many definitions of counterintelligence and theoretical models which explain how it works have been developed to date. However, a significant gap remains between theory and practice in the field of intelligence studies in general, and in counterintelligence in particular. This piece is intended to provide scholars and practitioners alike with a template that can help bridge the divide between scholars and practitioners who study and practice counterintelligence (CI). The foundations of this theory are premised on lessons learned from the American experience, although the theory could be applied by other practitioners in countries with similar systems of government. In recent years, intelligence studies scholars have been called upon for their expertise due to looming threats regarding issues such as terrorism, WMD proliferation, and transnational crime.[1] Massive CI failures such as the Edward Snowden case and successful penetration of the U.S. election system by the Russian government during the 2016 presidential election are stark reminders that such failures can have grave implications for U.S. national security. It is imperative that CI scholars with fresh ideas share their ideas with practitioners in government. This study seeks to advance a parsimonious theoretical model that can be easily understood by scholars and used by counterintelligence practitioners inside the U.S. Intelligence Community (IC).

This aspiration will be fulfilled in three parts. First, I will provide a brief historical background of the events that shaped contemporary American counterintelligence practices. Second, I will review the existing literature on CI theory. Third, I will showcase a theoretical model of counterintelligence that could be applied by CI practitioners to improve their tradecraft. The theoretical model advanced in this study can be used in future CI studies by both scholars and practitioners. The findings from this study will fill existing gaps in CI literature in two areas. First, it will create a new template that scholars can use to perform post-mortem assessments on previous practices inside the IC. Second, practitioners can use the model to find weaknesses in their own standard operating procedures. The efficient practice of CI is a vital prerequisite to preserving the integrity of the IC. I seek to support this effort by advancing a theoretical model of counterintelligence that both communities can use in future assessments.

A BRIEF HISTORY OF AMERICAN COUNTERINTELLIGENCE

American counterintelligence tradecraft was first implemented during the Revolutionary War. George Washington was well-known for the importance he placed on gathering intelligence and protecting his secrets from the British. The Culper spy ring, which Washington authorized and oversaw as Commander of the Continental Army, was well-versed in CI tradecraft using many tactics still employed by intelligence operatives today. These tactics included coded messages, dead-drops, and the employment of safe-houses. The first official counterintelligence organization was the Committee for Detecting and Defeating Conspiracies. This organization was tasked with identifying British spies and sympathizers operating in New York between 1776 and 1778.[2]

During the Civil War, the Confederates tasked Virginia Governor John Letcher with infiltrating, and procuring intelligence on, Union activities in Washington, DC.[3] President Lincoln tasked Allen Pinkerton's National Detective Agency with stifling Confederate agents in the nation's capital. To root out Confederate sympathizers, Pinkerton hired informants, cultivated double agents, eavesdropped on social conversations, and monitored telegraph lines.[4] Despite its proven value to national security in the early years after the founding of the United States, counterintelligence was not written into law or afforded institutional support from the federal government until 1918 when a joint agreement was signed among the Justice, State, Army, and Navy Departments that authorized the creation of an Office of Intelligence.[5]

The need for an institutionalized Office of Intelligence that could develop a sophisticated counterintelligence strategy was obvious after the United States had been caught flat-footed by continual intelligence failures before World War I. Whether it was successful gun-running operations and raids on southern border towns by Mexican revolutionaries or Germany's efforts to foment political discord in the United States by bombing an ammunition depot in New Jersey,[6] it was clear that America's enemies had successfully penetrated the country and its security institutions.

To meet the newfound demand for counterintelligence, the War Department (precursor to the Department of Defense) established a separate Counterintelligence Branch on April 17, 1939. During this time, counterintelligence was perceived as being a military responsibility rather than a police function.[7] The specific tasks of the newly created Counterintelligence Branch included:

> (1) Plans and regulations for both national and military censorship
> (2) Plans and regulations for counterespionage and passport control
> (3) Domestic intelligence information
> (4) Safeguarding of military information
> (5) Plans and regulations for espionage[8]

In order to accomplish the lofty goals of the Counterintelligence Branch, other stakeholders within the federal government were brought in to shed light on threats that the military was unable to uncover or incapable of uncovering.

During World War II, the Special Intelligence Service (SIS) was created. The SIS was an interagency effort that included personnel from the State Department, War Department, Federal Bureau of Investigation (FBI), and other smaller agencies that gathered economic and political intelligence on potential threats to U.S. national security interests.[9]

COUNTERINTELLIGENCE IN THE OFFICE OF STRATEGIC SERVICES

The Office of Strategic Services was responsible for intelligence collection and analysis during World War II. Agency personnel would then report their findings to the Joint Chiefs of Staff and the President. The OSS was also tasked with counterintelligence responsibilities. Within the OSS, the Counterintelligence Division had the following responsibilities:

> (1) To collect from every authorized source appropriate intelligence concerning espionage activities of the enemy.
> (2) To take such action with respect thereto as may be appropriate, and to evaluate and disseminate such intelligence within OSS as may be necessary, and to exchange such information with other agencies as may be appropriate.[10]

During World War II, counterespionage became a core component of the organizational mission of the OSS. The Counterespionage Branch, also known as X-2, collected intelligence on subversives, prepared actionable intelligence products for counterintelligence personnel, performed security for OSS operatives, and shared forums to share CI reports with other agencies within the federal government.[11]

COUNTERINTELLIGENCE AND THE CIA

In 1947 the National Security Act created the Central Intelligence Agency (CIA). The Agency was responsible for conducting intelligence-gathering and counterintelligence activities overseas. The FBI was given purview over domestic counterintelligence within the continental United States and the CIA was in charge of CI overseas.[12] The Venona program became the primary body responsible for CI activities inside the CIA. It was predominantly a program that relied on volunteers.[13] Its results were mixed. On one hand, it helped identify and capture spies like Rudolf Abel. Abel was a valued Soviet agent operating a ring inside the United States who was later exchanged in a prisoner swap for downed U-2 pilot Francis Gary Powers. On the other hand, the greatest CI successes during the 1950s came not from the Venona program but from Soviet walk-ins and agents-in-place inside the Soviet Union (i.e., moles).[14]

COUNTERINTELLIGENCE ABUSES IN THE 1960S AND 1970S

During the late 1950s, domestic criticism of American counterintelligence programs came under closer scrutiny by civil liberties advocates. The left-wing Campaign for Political Rights was founded to monitor the malfeasance of CIA and FBI operatives who were slowly and steadily taking a more active role in surveilling left-wing antiwar activists on college campuses across the United States.[15] The CI programs run by the CIA and FBI were a response to violent riots in the mid-1960s that broke out on college campuses across the United States in reaction to the assassination of Martin Luther King and the ongoing Vietnam War.[16] In theory, the purpose of the investigations was to expose and neutralize communist sympathizers who were fomenting the riots.[17] In practice, counterintelligence programs, such as COINTELPRO, were politically motivated counterespionage programs designed to stamp out widespread anti-government dissent among college students critical of the draft and U.S. intervention in Vietnam.[18] To add insult to injury, these programs failed to uncover any direct link between the actions of the protesters and the Soviet Union.

The findings of the Church Committee laid bare the nefarious actions of CIA counterintelligence head James Angleton during the 1960s and early 1970s. Angleton was widely condemned for carrying out an obsessive mole hunt using illegal spying methods on U.S. citizens.

In the wake of the Watergate scandal, many committees involved in counterintelligence activities, such as the Justice Department's Internal Security Division and even the House of Representatives Committee on Internal Security, were disbanded.[19] The findings of the Church Committee laid bare the nefarious actions of CIA counterintelligence head James Angleton during the 1960s and early 1970s. Angleton was widely condemned for carrying out an obsessive mole hunt using illegal spying methods on U.S. citizens. Thereafter, intelligence reform and renewed Congressional oversight of covert action and counterintelligence practices became a key priority for American lawmakers. This permanently altered both the legal mechanisms and bureaucratic structures within the agencies that practiced counterintelligence. It also spawned efforts to improve Congressional oversight of agency abuses in these areas through the creation of the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI).

THE YEARS OF FAILURE: COUNTERINTELLIGENCE IN THE 1980s AND 1990s

Some former counterintelligence officers such as William R. Johnson have noted that the Church Committee had the effect of dampening U.S. efforts to improve its CI capabilities.[20] Counterintelligence became less of a priority for the IC after it was revealed that both CIA and FBI had employed domestic surveillance methods for political purposes. In 1981 President Ronald Reagan signed Executive Order 12333, which redefined counterintelligence in the United States.[21] In 1985 a slew of CI failures during "The Year of the Spy" brought to light the failures of the IC in its practice of counterintelligence. Edward Lee Howard, Ronald Pelton, Jonathan Pollard, Sharon Scranage, and Larry Wu-Tai Chin were harbingers of worse things to come less than a decade later when it was revealed that CIA counterintelligence officer Aldrich Ames had spied for the Soviets for nine years, outing the identities of all of the most prominent American assets inside the Soviet Union. Ames was able to remain in place as a Soviet mole partly because CI officers in both the CIA and the FBI were unable to cooperate in a joint investigation after he was identified as a security risk.[22]

The Ames case was the impetus behind the Aspen-Brown Commission, which made recommendations to fix America's counterintelligence programs. Shortly thereafter, President Bill Clinton signed an executive order creating a National Counterintelligence Policy Board (NACIPB) and the National Counterintelligence Center (NACIC). The NACIPB reports to the National Security Council (NSC) on policy issues confronting counterintelligence practitioners in the field. The NACIC is a forum for counterintelligence officers from disparate agencies to collaborate on joint initiatives that require interagency coordination. [Editor's Note: After 9/11, the NACIC evolved into the Office of the National Counterintelligence Executive, or ONCIX, under the newly designated Director of National Intelligence. That senior CI executive now directs the National Counterintelligence and Security Center, or NCSC.]

RENEWED INTEREST IN COUNTERINTELLIGENCE IN THE POST- 9/11 ERA

U.S. policymakers were caught flat-footed on September 11, 2001, when al-Qaeda leader Osama Bin Laden orchestrated the largest attack on American soil since Pearl Harbor. Since then, policymakers have pressed the IC to improve its counterterrorism policies and practices.[23] A need for capable counterintelligence operations to root out terrorist "sleeper cells" operating discreetly through shell organizations in the United States became a newfound priority for the newly reorganized IC. Financial resources for counterintelligence grew in the wake of 9/11 as new agencies such as the Department of Homeland Security were created to meet the demand for national security. Despite increased spending on intelligence by Congress after 9/11, major CI failures have continued to occur. The recent cases of Edward Snowden, Chelsea Manning, and Jerry Chun Shing Lee have shown that CI weaknesses remain a constant threat inside the U.S. Intelligence Community.

A PAUCITY OF EXISTING COUNTERINTELLIGENCE THEORIES

Counterintelligence practitioners could greatly benefit from using academic studies to improve their operational practices. Unfortunately, few theories exist upon which to draw. There are three primary reasons why CI theory has not taken off in the discipline of intelligence studies. First, scholars have yet to conceptualize counterintelligence appropriately as a political phenomenon. John Ehrman famously noted in the June 2009 issue of *Studies in Intelligence* that counterintelligence lacked a theoretical foundation within the discipline of intelligence studies and that overly broad conceptualizations of the nature of CI inhibited theory development.[24] Second, counterintelligence has often been confused with security.[25] Lastly, existing theories have focused on individual cases and micro-level explanations. Miron Varouhakis has noted that CI theorists have focused on micro-level variables and case studies and have not yet accounted for external influences in their assessments.[26] Without solid theoretical foundations, CI practitioners and scholars have been deprived of a thorough understanding of the practice of counterintelligence. Such circumstances are detrimental to its study in the academy and its practical implementation inside the Intelligence Community.

ABSENT THEORY?

Without an array of counterintelligence studies to draw on for advice, CI policy may be implemented by practitioners unaware of scholarly research that may improve their standard operating procedures. For example, a CI analyst may be intimately familiar with assessing polygraph examination answers. However, he or she may be unaware that other factors, such as personality type (which cannot be measured in a polygraph test), may be more consequential when predicting whether a test subject is a security threat due to findings in a recent study. Hypothetically, the existence of a CI theory that accounts for this variable would alleviate the blind spot. Absent such circumstances, important aspects of the practice of counterintelligence may be downplayed to the detriment of the IC and the national security interests of the United States. Identifying the core components of counterintelligence, and developing a parsimonious theory explaining its practice, can help both scholars and practitioners in the United States improve their overall understanding of an area of intelligence tradecraft that is vital to preserving the integrity of the IC. It is my intention to advance a theory of counterintelligence that can meet this challenge.

BACK TO BASICS: WHAT IS COUNTERINTELLIGENCE?

As previously mentioned, CI scholars have yet to agree on a universal definition of the term. Academic definitions of counterintelligence have identified its dual offensive and defensive nature. These terms are often interchangeably used with the terms “active” and “passive.” Existing academic definitions of counterintelligence have also identified both its behavioral and organizational nature. These definitions have been largely premised on the notion that a more succinct definition of counterintelligence is preferable to a broader one.

Loch Johnson argues that “counterintelligence is made up of two matching halves: security and counter-espionage.”[27] He defines security as being defensive in nature and counterespionage as being offensive. John Ehrman argues that “counterintelligence is the study of the organization and behavior of the intelligence services of foreign states and entities and the application of the resulting knowledge.”[28] William Johnson defines counterintelligence as an activity that is “aimed against intelligence, against active, hostile intelligence, against enemy spies. And it is itself active, not passive.”[29] Harry Prunckun uses a truncated version of Johnson’s definition of counterintelligence. He argues that counterintelligence ought to be described as “an activity aimed at protecting an agency’s intelligence program against an opposition’s intelligence service.”[30] Stan Taylor states that counterintelligence is designed for the protection of state secrets and to inoculate one’s own intelligence operations from penetration and disruption by hostile nations or groups.[31]

The U.S. government has also issued disparate definitions of counterintelligence. The federal government’s has been broader and more extensive than those used in academic circles. For example, the National Security Act of 1947 described counterintelligence as:

> Information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities.[32]

This definition was slightly modified when President Reagan signed Executive Order 12333. EO 12333 defined counterintelligence as:

> Information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted

> for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.[33]

In 1993 the CIA conceptualized counterintelligence as constituting "knowledge (information about counterintelligence), activity (counterintelligence measures) and organization (personnel tasked to conduct operations)."[34]

Since CI is an understudied area within the field of intelligence studies, the development of a new grand theory of counterintelligence will provide scholars with a theoretical framework to build upon in future studies. It will also create a foundation for CI scholars to test the empirical validity of their hypotheses in the future.

The differences between the academic and governmental definitions of counterintelligence are stark. Academics have been far more interested in classifying behavior whereas practitioners have been focused on identifying behavior. This fact can be chalked up to the fact that practitioners are far more concerned about the political and legal ramifications which a broad conceptualization of the term may imply. What is needed is a middle ground between the two camps that can bridge the divide between CI theory and practice. To accomplish this objective, I will identify the behavioral aspects of counterintelligence within a framework that encompasses the full scope of CI practices.

A THEORY OF COUNTERINTELLIGENCE FOR SCHOLARS AND PRACTITIONERS

The theoretical framework of counterintelligence described in this study can be used by both scholars and practitioners alike. For scholars, the development of a new theory of counterintelligence will help to expand the paucity of existing theories on the subject. Since CI is an understudied area within the field of intelligence studies, the development of a new grand theory of counterintelligence will provide scholars with a theoretical framework to build upon in future studies. It will also create a foundation for CI scholars to test the empirical validity of their hypotheses in the future.

For CI practitioners, a grand theory of counterintelligence will create a coherent roadmap explaining the nature of the system in which they operate daily. The development of such a new grand theory will simplify the tactical and strategic realities of an often complicated trade. This will benefit all practitioners regardless of their position in the CI hierarchy inside the IC. It will allow practitioners to see the importance of their efforts in the broader context of the counterintelligence system of which they are a part. In an ideal world, a better understanding of the CI system among all practitioners would incentivize collaboration with other stakeholders in the IC such as policymakers and analysts. Helping CI practitioners recognize the importance of implementing the policy guidelines and procedures crafted by their colleagues in the analytical community would work toward breaking down the institutional and cultural barriers that inhibit collaboration between the two communities. A close working relationship between CI operators and analysts would also increase the overall effectiveness of the practice of counterintelligence.

For policymakers tasked with identifying flaws in existing CI systems, a grand theory of counterintelligence would aid their efforts to improve the systems they are responsible for managing. By helping CI analysts break down the barriers that stymie collaboration between policymakers and practitioners, analysts will learn first-hand whether their policies are viable, pragmatic, and capable of operational success.

The grand theory of counterintelligence imparted in this study is described in four parts: the mapping phase, the observing phase, the reporting phase, and the ending phase. Each phase is vital to the overall success of CI tradecraft. Failures in one realm can negate successes in others. Each phase showcases the importance of a specific area of CI tradecraft. The theoretical framework advanced in this study showcases the disastrous effects that failures in each phase of counterintelligence can have on the implementation of effective CI policy. Most importantly, the theory articulated in this study is designed to serve as a blueprint for future studies and assessments by scholars and practitioners of CI.

The Mapping Phase

The mapping phase is carried out by policymakers in the IC. The purpose of the mapping phase is to identify both strategic and counterintelligence targets. Strategic CI threats include enemy states and individuals capable of recruitment in rival intelligence services. Insider threats include U.S. intelligence personnel and political institutions. For any country, it is a necessity to track intelligence officers who may become potential security threats. It is also important to monitor institutions and institutional assets of the IC vulnerable to infiltration. For example, it is important for CI officers to protect safe-houses from being bugged and classified document repositories from being ransacked. Today, cybersecurity and defense are taking on newfound importance as foreign governments and non-state actors seek to exploit weaknesses and vulnerabilities inside the federal government's information technology systems.

The Observing Phase

The observing phase involves counterintelligence officers monitoring the activities of strategic and insider threats that have been identified as security risks. Strategic threats may include a geopolitical adversary's intelligence services, vulnerable computing systems (possessing sensitive materials that can be exploited), or personnel ripe for recruitment or blackmail. During the Cold War, both the United States and the Soviet Union successfully infiltrated each other's intelligence services by identifying the vulnerabilities of their opponents. The Soviets cultivated lucrative relationships with walk-ins such as Aldrich Ames and Robert Hanssen which allowed them to gain access to troves of documents from inside the CIA and FBI. Similarly, CIA personnel maintained longstanding relationships with individuals such as KGB officer Vitaly Yurchenko and GRU Major General Dmitri Polyakov, which yielded similar results.

Insider threats often include vulnerable infrastructure within the U.S. Intelligence Community targeted by outside actors for infiltration. Activities carried out by counterintelligence personnel during the observing phase may include audio and visual surveillance of compromised personnel, behavior monitoring, polygraph examinations, and cyber-defense adjustments. These tactics are designed to prevent security breaches before they occur and can also stop threats from causing further damage if they are discovered amid an ongoing operation. Such practices are a prerequisite to ensuring that the insider threats identified by CI officers in the mapping phase are addressed and accounted for.

The Reporting Phase

The reporting phase occurs when counterintelligence officers provide reports of their activities to bureaucratic stakeholders in the IC. These may include agencies such as the National Counterintelligence and Security Center, the National Security Council, or the HPSCI and SSCI within the legislative branch. Depending on the sensitivity of the CI breach, the media and the American public may be informed as well. By reporting their findings to actors both inside and outside the IC, counterintelligence officials can give policymakers and interested stakeholders (such as intelligence scholars) the information they need to carry out post-mortem assessments of CI failures. Such practices will not only increase government transparency but will also allow for voices from outside the government to add their own insights and recommendations to government officials in the IC.

The Ending Phase

In the ending phase, policymakers use the assessments provided by CI practitioners and government officials to make either domestic or international policy decisions. Domestic policy decisions may include calls for additional intelligence oversight hearings or a law enforcement response such as an arrest or issuance of criminal charges against an alleged perpetrator. An international response may include the implementation of targeted economic sanctions against a foreign government deemed responsible for orchestrating an espionage operation. Other tools available to policymakers may include diplomatic admonishment or even a reprisal attack such as a drone strike or a targeted assassination.

If a foreign ally is caught spying, as occurred when Israel used Jonathan Pollard to spy on the United States, policymakers may feel that quiet diplomacy and enhanced defensive measures are best suited to address the breach that occurred.

Depending on the severity of the security breach, the policy implications of a harsh reprisal may have adverse political consequences at both the domestic and international levels. For example, mass arrests of alleged infiltrators perceived as potential security threats may spark a political backlash among the broader public as occurred at the peak of the McCarthy era in the 1950s.

At the international level, policymakers may be reluctant to spark a tit-for-tat fight against a powerful foreign adversary that carried out a successful espionage operation. A disproportionate response could spark international criticism from an otherwise sympathetic international community. For example, a military strike or even a state-sanctioned execution may potentially lead to an even harsher response by the same enemy in the future. If a foreign ally is caught spying, as occurred when Israel used Jonathan Pollard to spy on the United States, policymakers may feel that quiet diplomacy and enhanced defensive measures are best suited to address the breach that occurred. In some situations, a non-response may be preferable, especially if raising public attention to the subject of counterintelligence could lead our adversaries to threaten increasing their own defensive capabilities.

CONCLUSION

To date, there have been relatively few theories of counterintelligence articulated by intelligence studies scholars. Despite being largely overlooked by the academic community, flawless counterintelligence tradecraft is vital for the U.S. Intelligence Community to maintain. The theoretical model developed in this study can serve as a departure point for use by both scholars and practitioners of counterintelligence in the United States. Scholars may use this model to perform post-mortem assessments of the CI practices of governments that have been open and transparent with implementation of their CI policies in the past. Practitioners inside the IC can use the model described in this study to audit existing practices and procedures and to identify potential flaws in existing systems. Such audits would better inform decision-makers and hasten bureaucratic reforms vital to ensuring the success of counterintelligence tradecraft inside the Intelligence Community.

NOTES

[1] Scott, L. and R.G. Hughes (2006). "Intelligence, crises and security: Lessons from history?" *Intelligence & National Security* 21(5): p. 657.

[2] Rafalko, F.J. (2004). *Counterintelligence Reader: American Revolution to World War II*. Washington, DC: National Counterintelligence Center (2004). Volume 1, Chapter 1, p. 2.

[3] Central Intelligence Agency (2018). Intelligence and the Civil War. Washington, DC: Office of Public Affairs, 2018. https://www.cia.gov/library/publications/intelligence-history/civil-war/Intel_in_the_CW1.pdf, p. 11.

[4] Rafalko. *Counterintelligence Reader.* Volume 1, Chapter 2, p. 7.

[5] Rafalko. *Counterintelligence Reader.* Volume 1, Chapter 3, p. 4.

[6] Neiberg, M. (2013). "World War I Intrigue: German Spies in New York!" 2018, from http://www.historynet.com/world-war-i-intrigue-german-spies-in-new-york.htm.

[7] Ibid.

[8] Rafalko. *Counterintelligence Reader.* Volume 1, Chapter 4, p. 17.

[9] Rafalko. *Counterintelligence Reader.* Volume 2, Chapter 1, p. 2.

[10] Rafalko. *Counterintelligence Reader.* Volume 2. Chapter 3, p. 9.

[11] Ibid.

[12] Wannall, W.R. (2002). Undermining Counterintelligence Capability. Great Britain: Intel Publishing Group, Inc.: p. 322.

[13] Parrish, M.E. (2001). "Venona: Soviet Espionage and the American Response." *Diplomatic History* (1): p. 13.

[14] Ibid.

[15] Wannall. *Undermining Counterintelligence Capability*, p. 324.

[16] Rafalko. *Counterintelligence Reader*, Volume 3, Chapter 2, p.118.

[17] Ibid., p. 119.

[18] Ibid.

[19] Wannall. *Undermining Counterintelligence Capability*, p. 325.

[20] Johnson, W.R. (2009). *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*. Washington, DC: Georgetown University Press, p. 2.

[21] Rafalko. *Counterintelligence Reader*, Volume 3, Chapter 3, p. 217.

[22] (1997). *A review if the FBI's performance in uncovering the espionage activities of Aldrich Hazen Ames*, Washington, DC: U.S. Department of Justice, Office of the Inspector General: 1997, p. 5.

[23] Shelton, C. (2013). *Applying Counterintelligence Tradecraft to Defeat Terrorist Threats*, Great Britain: Taylor & Francis.

[24] Varouhakis, M. (2011). *An Institution-Level Theoretical Approach for Counterintelligence.* Great Britain: Taylor & Francis**:** p. 494.

[25] Rafalko. *Counterintelligence Reader*, Volume 3, Chapter 3, p. 240.

[26] Ibid., p. 499.

[27] Johnson, L.K. (2015). *Essentials of Strategic Intelligence*, Santa Barbara, CA: Praeger, an imprint of ABC-CLIO, LLC, (2015), p. xv.

[28] Ehrman, J. (2009). "Toward a Theory of CI: What Are We Talking About When We Talk About Counterintelligence?" Washington, DC: Center for the Study of Intelligence. *Studies in Intelligence*, Vol. 53, No. 2.

[29] Johnson, W.R. *Thwarting Enemies at Home and Abroad*, p. 2.

[30] Prunckun, H.W. (2012). *Counterintelligence Theory and Practice*. Lanham, MD: Rowman & Littlefield Publishers, p. 38.

[31] Johnson, L.K. *Essentials of Strategic Intelligence.* Stan A. Taylor, Chapter 14: "Definitions and Theories of Counterintelligence," p. 285.

[32] The National Security Act of 1947. (1947) Public Law 253, 80th Congress; Chapter 343, 1st Session; S. 758. Washington, DC, https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf.

[33] Rafalko, *Counterintelligence Reader,* Volume 3, Chapter 3, p. 217.

[34] Central Intelligence Agency. (1993) Counterintelligence for National Security. CIA Historical Review Program. Washington, DC, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm#5-security-

Lee A. Lukoff is a PhD candidate (all but dissertation) in Political Science and International Affairs at the University of Georgia, where he is writing his dissertation on U.S.-Israeli relations during the Reagan administration. He holds master's degrees from Boston College (Political Science) and George Mason University (Public Policy). His research interests include subjects in the areas of international relations, American foreign policy, intelligence studies, and political psychology. Lee has taught nine courses on topics such as International Conflict, Global Issues, U.S.-Israeli Relations, and American Public Policy. He currently serves as an Adjunct Instructor for the University of Georgia's Washington Semester Program and lectures part-time in the Department of Government at American University.