STRATEGIC COUNTERINTELLIGENCE: AN APPROACH TO ENGAGING SECURITY THREATS TO AMERICAN SECURITY

By:
John Gaitan

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Global Security Studies

Baltimore, Maryland

June 2017

ABSTRACT

The US Intelligence Community has shown a lack of understanding and appreciation of counterintelligence and its capabilities as a strategic tool. Historically, US adversaries have used the famed Double-Cross System to engage in counterintelligence and counter-espionage operations that have effectively neutralized US foreign intelligence operations. This research reviews and answers the question of "Strategic Counterintelligence; What Is It and What Should We Do About it?"[1] Strategic counterintelligence is the analysis of foreign intelligence or security service entity acting on behalf of state or non-state actor. The operational aspect is aimed at exploiting the state or non-state actor's clandestine collection channel to manage the actor's objectives. My deception research revealed that state and non-state actors are still susceptible to deception, and that technology is increasing this vulnerability in the US. Through researched historical examples, it was found that strategic counterintelligence operations are a method of imposing costs on a state or non-state actor, specifically through the controlled release of technology. Lastly, Double-Cross-like operations are viable in cyberspace through the use of decoy and real network systems. The US has the ability to effectively employ strategic counterintelligence operations, deliberately and reactively, against a state or non-state actor, to drive the actor's moves and countermoves.

Thesis Advisor: Dr. Mark Stout

[1] Michelle K. Van Cleave, "Strategic Counterintelligence: What Is It and What Should We Do About It?" *Studies in Intelligence*, 51(2007), accessed April 9, 2016, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/strategic-counterintelligence.html

ACKNOWLEDGEMENTS

I wish to sincerely thank all of my professors at John Hopkins University for the opportunity to research some of the most significant global security topics currently challenging U.S. national security and American allies. In particular, I would like to thank professors Mark Stout, Robert Haffa, and Michael O'Hanlon for sharing their personal thoughts on this topic. I would also like to thank several professional colleagues who listened and provided their critiques and guidance on this topic. Thank you, Dermot O'Reilly, Ryan Dow, Brian Eshenbrenner, Mark Rush, Chris Gore, Joseph Williams, Mike Mumford, Dan Payne, and numerous colleagues at the Air Force Office of Special Investigations, Special Projects. In addition, I would like to call out three friends who challenged me consistently on this topic: Rolf Mowatt-Larssen and Ryan Kovar. This research is dedicated to Tim Peterson and all the nights we spent drawing things up on cocktail napkins, may you rest in peace, a true partner, and thank you for helping me realize I had a knack for this stuff. Special thanks are due to my wife, Karen, who spent many nights listening to me rambling about the topic, who undoubtedly knows more than me.

Table of Contents

Table of Figures

Definitions

**Definitions are specifically within an American context, though some are derived from other academic research.*

Strategic Counterintelligence- Analysis conducted for policy makers of the state, non-state actors, and security and operational intelligence gathering entities. The analysis is completed through the collection of information via human, technical, and disruption activities. The primary means of information collection is through counterintelligence and counter-espionage operations.

Strategic Counterintelligence Operations- Strategic counterintelligence is employed to identify the adversary/competitor's clandestine human, technical, informational networks, and deny access to actual information of value. Through that denial, the goal is to influence the adversary's intelligence collection feeding that adversary's responsible leadership. The influence and management may include the controlled release of manipulated information/data for the purposes of:

- Exploiting the adversary/competitor's view of the US national security goals and objectives.
- Preventing US national security interests from being compromised through clandestine intelligence operations in progress and manage the value of the adversaries' operations.
- Enabling and assisting future clandestine intelligence operations planning and objectives through domestic and external US counter-espionage operations.
- Reducing the potential advantages an adversary can exploit or develop through the active engagement in double-cross-like activities meant to deceive and impose a cost

on the adversary who attempts to illegally subvert or transfer US National Security information, technology, and capabilities.

Counterintelligence (CI)- the art of the identification of foreign agents and officers operating on behalf of an allied or hostile operational intelligence service outside of the US. The objective of the identification could be passive monitoring, recruitment, and compromise, or the disruption of their service's operational objectives.

Counter-Espionage (CE) - the art of identifying foreign agents operating against the state for an allied or adversary intelligence service. The objectives could include passive monitoring, recruitment, and compromising or disrupting their service's operational objectives.[2]

Offensive Counterintelligence Operations- Clandestine activity conducted for military, strategic (for DoD), or national counterintelligence and security purposes against a target having suspected or known affiliations with foreign intelligence entities, international terrorism, or other foreign persons or organizations. The goal is to counter terrorism, espionage, or other clandestine activities that threaten the security of the United States.[3]

Deception- The actions executed to mislead adversary military, state, non-state decision makers as to the initiator of the deception. This may be initiated to protect a state or non-state political, diplomatic, military, and economic capabilities, intentions, and operations.[4]

Hybrid Warfare- incorporates a range of modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts (including indiscriminate violence and coercion), and criminal disorder.[5]

---

[2] Christopher Andrew, *Defend the Realm: The Authorized History of MI5* (New York: Alfred A. Knopf, 2009).
[3] US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Washington, DC: U.S. Departent of State, Joint Publication 1-02, April 12, 2001, As Amended Through April 2010.
[4] United States of America. Department of Defense. Joint Staff. *Joint Publication 3-58: Joint Doctrine for Military Deception.* Compiled by Joint Staff Publication. Washington, DC: Government Printing Office.
[5] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).

Hybrid Challenger- a state or non-state group that employs hybrid warfare.

Target Management- the active manipulation, influence, and handling of the threat through means traditionally associated with deception.

National Security Interests- the foundation for the development of valid national objectives that define US goals or purposes. These national security interests include: preserving the US political identity, framework, and institutions; fostering economic well-being; and bolstering international order supporting the vital interests of the United States and its allies.[6]

Cost Imposition Strategies- focus on eliciting an adversary response that creates a hardship differential favoring the initiating nation.[7]

Left-of-Boom- in terms of strategic counterintelligence, the suggested policy prescription for strategic counterintelligence operations, and places an emphasis on penetration of state or non-state actor intelligence entities before they can initiate clandestine intelligence operations against, manage the actors intelligence entity objectives, and drive their moves/counter-moves.

Cyberspace- first and foremost an informational environment, made up of digitized data that is created, stored, and most importantly, shared.[8]

---

[6] US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Washington, DC: US Department of State, Joint Publication 1-02, April 12, 2001, As Amended through 31 August 2005.
[7] Col. Kenneth P. Ekman, "Applying Cost Imposition Strategies against China," Strategic Studies Quarterly, 9(Spring 2015)
[8] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar, What Everyone Needs to Know* (New York: Oxford University Press, 2014)

CHAPTER 1: INTRODUCTION-*FONS ET ORIGO*

"Although the purpose of counterintelligence is defensive, its methods are essentially offensive"[9]
- Allan Dulles

Introduction of Thesis Concept

This thesis tests the concept of strategic counterintelligence using qualitative research. It focuses on the use of historical cases that articulate how and why counterintelligence (CI) is a strategic tool that has been incorporated in order to serve US national security interests. US national security interests are defined within the context of defense, economic, foreign, and political objectives.

Three of the primary challenges that any researcher faces when it comes to counterintelligence include the lack of literature, the lack of consistent doctrines, and the fact that almost every entity in the US government conducts CI differently. As Sherman Kent once complained in the 1950s, without definitive literature and studies on the practice of CI, "its fundamental theory runs the risk of never reaching full maturity."[10] This warning continues to be echoed by researchers into the present day. American CI literature primarily centers around three principal entities as origins of US CI: James Angleton at the CIA; J. Edgar Hoover and the FBI's interpretation of CI; and the British Counterespionage (CE) history (double-cross system).[11][12][13][14]

---

[9] Allen Dulles, The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World (Guilford, Connecticut: Lyons Press, 2016)
[10] Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence* (September 1955),3.
[11]Holzman, Michael Howard. *James Jesus Angleton, the CIA, and the craft of counterintelligence*. Amherst: University of Massachusetts Press, 2008.
[12] *THE JOURNAL OF INTELLIGENCE HISTORY*, November 2003, 21-49. Accessed January 01, 2016. https://www.cia.gov/library/center-for-the.../JIH-Angleton-Robarge-2003.pdf.
[13] Batvinis, Raymond J. *Origins of fbi counterintelligence*. Lawrence: University Pr Of Kansas, 2009
[14] Andrew, Christopher M. *Defend the realm: the authorized history of MI5*. New York: Vintage Books, 2010.

Without fully understanding the history of CI and CE, there is plenty of room for misinterpretations. In short, in order to understand CI, especially in terms of any strategic relevance, one must understand that it is a blend of disciplines, employed to offset an activity initiated by state or non-state actors. The initiator of the activities could have a number of goals, including theft, sabotage, or inflicting surprise through various designs to minimize the US's military, economic, and political capabilities. CI/CE is protective in nature, but through its protective/preventative operations, it exerts the ability to shift, shape, and influence a state or non-state actor.

The US cannot afford to continue thinking that its economic and military might will always give its adversaries pause. The world is now multi-polar, and violent, non-state actors have adopted a hybrid approach to warfare that challenges US hegemony. New state actors have now engaged the US through multiple media in a manner that directly challenges its ability to project its power in the cyber environment.

The Current and Future Security Environment

With the global security environment becoming more dynamic and unstable, the ongoing evolution of established international relations systems, and the emergence of a multi-polar system, new powers will rise and old forces may fall. The operational aspects highlighted through the historical test cases put forth by this body of research have direct relevance to countering the threats emerging from current and future violent non-state/state actors opposing the US. The current and future threat landscape has given rise to these three trends:

- Violent Non-State Actors (VNSAs) are engaging in offensive and defensive intelligence operations aimed at protecting their networks, illicit finances, and communications.

- VNSAs and Violent State Actors (VSAs) are adopting hybrid warfare as a military strategy. This poses a direct threat to the US and will challenge the US Intelligence Community, which is responsible for providing indications and warnings.
- VSAs that engage in cyber-espionage challenge the US's economic security. As a result, the US needs a cost imposition strategy to ensure its economic security and deter VNSAs and VSAs from engaging in cyber-espionage activities and/or exploit the aggressors' cyber activities.

Accurate and uninfluenced information will be critical to understanding how these new trends and actors will challenge the US and put American interests at risk. Strategic counterintelligence has the potential to deliver an impact by manipulating and imposing a cost to the target, thus remaining faithful to its origins as discovered through the British Double-Cross System. One of the ripple effects of the operational design of the British Double-Cross System was the penetration of the German intelligence clandestine network: the double agents were in receipt of the shopping lists of essential elements of information needed for Nazi military planning. The British managed the double agents and gave them information to assist in Nazi military planning, to the British's benefit.

The literature reviews conducted for each chapter focus on specific case studies that highlight the essence of strategic counterintelligence as understood in this thesis. Through the use of these case studies, which were initiated by various state and non-state actors, we see the success of these operations, ultimately disrupting the target's ability to collect information either overtly or clandestinely. Oftentimes, the evidence from the case studies presents strong indications of ripple effects that compounded and sometimes exposed the targets to other overt or clandestine operational elements in their attempts to engage in espionage against the initiator. Through this text, we will see that the global security

environment is constantly challenging the possibility that a state like the United States will be able to employ a system-based approach relying on whole Intelligence Community discipline approaches to counter state or non-state actors. For this reason, research in this field is all the more critical.

Fons Et Origo **of US Counterintelligence and Counter-Espionage**

"Do not forget that a traitor within our ranks, known to us, can do more harm to the enemy than a loyal man can do good to us."[15]
-Isaac Asimov

In 1937, the British clandestine MI-5 domestic security service employed the Double Cross-System to counter German intelligence services' hidden network of agents. MI-6, the British foreign intelligence service, also played a crucial role in the Double Cross-System, running double agents under its counterintelligence mission. This occurred just as Germany was collecting and preparing for sabotage operations within Britain. The result of these operations helped persuade the Allied chiefs to approve the largest known deception operation in the history of the world.[16] The double-cross system's goal was to manipulate and provide alternative and plausible information to the German military and its leadership, which amplified Allied military plans and ultimately ensured the success of Operation Neptune (D-Day).[17] The most complex, sensitive, and detailed CE operation aimed to essentially blind the Nazi intelligence apparatus, the Abwehr, and prevent Hitler from receiving any information that allowed his military force to have warning of allied activities.

However, MI-5 and MI-6 were not the only professional service organization engaging in CE operations and deceiving the Nazis. In 1943, the Office of Strategic Services (OSS), the forerunner to the Central Intelligence Agency (CIA), created a CI division, known

[15] Isaac Asimov, *Pebble in the Sky* (New York, Doubleday, 1950), 70.
[16] John Cecil Masterman, *The Double-Cross System in the War of 1939 to 1945* (New Haven: Yale University Press, 1972).
[17] ibid.

as X-2.[1819] The role of X-2 was to learn the art of employing the double-cross system and running the double agent from MI-5 and MI-6. As the initial OSS officers learned from their British colleagues, this technique was successful not merely due to running double agent operations, but also the secret ability of the British to intercept, decrypt, and read the Abwehr's communications.[20] The program was named ULTRA,[21] and was highly classified; dedicated to breaking the German Enigma machine.[22] The ULTRA program would intercept messages and decrypt them so that they could be used to identify Abwehr clandestine agent networks operating within Great Britain and overseas. MI-5's cycle of operations included watching and studying the approaches of the Abwehr agents, who were presented with two options: continuing to spy for the Abwehr while taking direction from the MI-5; or being arrested for espionage.[2324] The result was the blinding of the Abwehr's intelligence apparatus, and as Masterman asserted, "We controlled the whole thing."[25] Masterman was alluding to the control held by British intelligence and security services over all the information that the Abwehr clandestine agents were collecting. The information provided to the agents was a mixture of real and false information. The double-cross system was responsible for providing guidance to the Nazi military and destabilizing the Nazis from within, ultimately leading Nazi leadership to put little to no faith in its intelligence services.[26]

Despite their significance, the value and impact such operations had on the war effort had the potential of derailing ongoing Allied war activities. Due to the crucial nature of this mission, the X-2 became another intelligence service within the OSS intelligence

---

[18] Robert Cowden, "OSS Double-Agent Operations in World War II," *Studies in Intelligence*, 58 (2014)
[19] Dulles, *The Craft of Intelligence*
[20] ibid.
[21] Andrew, *Defend the Realm: The Authorized History of MI5*.
[22] ibid.
[23]ibid.
[24] Cowden, "OSS Double-Agent Operations in World War II," 68
[25] ibid.
[26] Masterman, *The Double-Cross System in the War of 1939 to 1945*.

service, which would have access to all OSS and British intelligence. The British shared the crown jewels with the OSS: as noted in the declassified US government history of counterintelligence Services, "the United States was given the opportunity of acquiring, within a short period of time, extensive counterintelligence records representing the fruits of many decades of counterintelligence experience."[2728] The initial training for the X-2s was provided by MI-5 and MI-6, and included everything from approaching a potential agent, doubling that agent, handling the agent, and the purpose of running the double-cross. As Sir John Masterman, the chief of the British double-cross system, briefed his OSS X-2 colleagues in 1943, the double-cross program's creed included the following:

1. To control the enemy system, or as much of it as we could get our hands on.
2. To catch fresh spies when they appeared.
3. To gain knowledge of the personalities and methods of the German Secret Service.
4. To obtain information about the code and cypher work of the German Service.
5. To get evidence of the enemy plans and intentions through questions asked by them.
6. To influence enemy plans by the answers sent by the enemy.
7. To deceive the enemy about our own plans and intentions.[29]

As the knowledge transfer from the British security and intelligence services amassed, so did the desire for the OSS to initiate its own double-cross like system that would focus on identifying enemy agents operating within Allied territories. A little known case involving one of the first US documented successful recruitments of a controlled agent handler was executed by the OSS X-2's service.[30] Working in conjunction with their British

[27] US Office of Strategic Services, *History of United States Counterintelligence*, Vol. I, 32. (Records of the Office of Strategic Services, Record Group 226, Entry 117, Box 2, National Archives College Park (NACP), 1943), 34.
[28] Cowden, "OSS Double-Agent Operations in World War II"
[29] Masterman, *The Double-Cross System in the War of 1939 to 1945*, 58
[30] Cowden, "OSS Double-Agent Operations in World War II", 68

colleagues, the X-2 identified a Spanish national living in France, who had been reporting to the Abwehr since 1935. Drawing upon the training the X-2 learned from the British, the X-2 officers observed the Spaniard and studied what information he was providing, consulted with military planners to determine how the Spaniard could be used, and then moved in for recruitment. The pitch followed a tried and true method. They knew the Spaniard enjoyed the freedom and life he had, so X-2 officers offered him a deal he couldn't refuse: pass the information X-2 gave him through his wireless radio set, or face prison for treason. The man was arrested and, given the above-mentioned choices, readily agreed to work with X-2. The result of this recruitment identified that the Abwehr was using the Spanish national, whose code name was DRAGOMAN.[31] DRAGOMAN's role was to report to the Abwehr on any ships, commando like units, or other heavy weapons.[32] Once the first successful recruitment occurred, within a few months, the X-2 was able to recruit a few more Abwehr agents operating within France, all of whom were charged with reporting on Allied activities.[33]

This network, now composed of X-2-controlled Abwehr agents, furthered the on-going British double-cross system deception activities in support of Allied military actions.[34] Through the MI-5, MI-6, and X-2 counter-espionage operations, the Abwehr agents were effectively doubled in place, giving direct access to the Abwehr's and Nazi military information needs.

The X-2 was also getting great assistance from their British colleagues' signals intelligence capabilities through the ULTRA program working to transcribe encrypted German intelligence messages. The benefits of ULTRA intercepts for X-2 operations were

[31] ibid. 68-70.
[32] ibid.
[33] ibid, 70-71
[34] ibid. 72

twofold: ULTRA provided leads on the Abwehr agents already in place, which assisted X-2 with targeting; and X-2 was then able to study the potential recruitment and characterize what they were communicating back to Germany. The benefit of this activity ensured that streams of information were provided to the German intelligence service, causing no alarm or suspicion about the agent in place.

This X-2 initiative particularly amplified Allied military operations in France. The results of X-2's France double-cross system operations allowed the allies to control Abwehr intelligence operations. One of the byproducts of the information the Abwehr required included informational questionnaires, which allowed the Allies to have an intimate look and develop a deep understanding of their military strategy and capacities. These operations opened the door to providing both truthful and non-truthful information, and the only way it could be validated was through other information sources. Much like the British operations, upon the recruitment of one Abwehr agent, the rest soon became cooperative informants. Within a matter of time, the network had been identified and was providing Allied-controlled information to the Abwehr.

The DRAGOMAN case highlights the effectiveness of X-2's ability when it came to running double agents, but also demonstrates the effectiveness of deceptive material being reported through clandestine sources. However, as X-2 would learn, along with British security and intelligence services, a deception is only as good as its ability to support and manage the information. This meant the Abwehr had to see physical proof of the information that was passed through the system. Evidence that the false information was true further enhanced the credibility of the British and X-2 controlled agents.[35] This was

[35] ibid., 69

done by providing the Abwehr with manipulated bomb damage assessments of factories, military bases, and Allied logistical movements.[36]

The results of the double-cross system echo the themes of this research project. The system shows that CE operations are effective against adversarial intelligence services and the current security environment the US faces from human, technical and cyber threats are optimal for use to manage them to the US's advantage. Case studies were selected for the study that focused on US operations and adversarial operations. Both US and adversary CE operations had two common objectives: preventing secrets from being compromised and enhancing a secret's capability. Both prevention of the compromise and enhancing the secret's potential involve deception techniques.[37] The secret can be a plan, technology, weapon capability, political interest, or operation; however, the CE operation's effectiveness depends on the knowledge and requirements of the target.[38]

The employment of the double-cross system was so effective because of the deep study and analysis of the Abwehr. This investigation was conducted by British intelligence and security services, and it allowed the MI-5 and MI-6 officers to work quickly and know what information would be passed through their double agents. The information was relevant to the Nazi military strategy, and the deceptive uses of the agents were coordinated with other Allied efforts.[39][40]

Through the placement and access of a double agent, a great wealth of intelligence information was obtained on the target. Such intelligence included tradecraft, clandestine infrastructure, and penetrations within the initiating service, covert communication methods,

---

[36] Masterman, *The Double-Cross System in the War of 1939 to 1945*.
[37] ibid.
[38] ibid.
[39] Andrew, *Defend the Realm*
[40] "Cowden, OSS Double-Agent Operations in World War II"

valuable political information, adversary military capabilities, and military industrial capabilities. As history has shown, this happens to be one of the most effective espionage operations, and it should be run more frequently, particularly with the current threat portfolio that we face in the United States.

Review of Contemporary Counterintelligence and Counter-Espionage Literature

"The purpose is not just to manipulate or frustrate the opponent's intelligence operations, but to capitalize on what he is not doing well or is not doing at all."[41]
-Jennifer E.Sims
vs.
"The real test of successful counterespionage, and that is our task, is locating the spy, ascertaining his contacts and methods of communication-and then closing off his sources of information."[42]
-J.Edgar Hoover

Americans have traditionally focused on CI as an investigation that aims to identify and arrest a spy. This is rooted in the foundations of the Federal Bureau of Investigation Foreign Counterintelligence Program. Unfortunately, the arrest of a spy is not a success, but rather a conclusion of a process emphasizing a failure on the part of the victim's intelligence or security service. The FBI's CI program is defined and focused on four goals:

> Protect the secrets of the U.S. Intelligence Community, using intelligence to focus investigative efforts, and collaborating with out government partners to reduce the risk of espionage and insider threats, Protect the nation's critical assets, like our advanced technologies, and sensitive information in defense, intelligence, economic, financial, public health, and science and technology sectors, Counter the activities of foreign spies, through proactive investigations, the Bureau identifies who they are and stops what they are doing. Keep weapons of mass destruction from falling into the wrong hands, and use intelligence to drive FBI investigative efforts to keep threats from becoming reality. [43]

---

41 Jennifer E. Sims, "Twenty-First-Century Counterintelligence: The Theoretical Basis for Reform," In Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence, eds. Jennifer E. Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2008)

42 Hoover, "Is There a Spy Menace?"

43 "Counterintelligence," FBI, May 03, 2016, accessed September 10, 2017, https://www.fbi.gov/investigate/counterintelligence.

The US Central Intelligence Agency defines CI 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 governments or elements thereof, foreign organizations, or foreign persons or international terrorist activities."[44]

The British foreign and domestic security MI-6 and MI-5 largely view CI and CE as being one and the same, with the point of departure being that CI is conducted by the British foreign intelligence service, while CE is conducted by a security service. The British defines of CI and CE in terms with areas of responsibility. MI-5 operates domestically; it is the security service countering espionage conducted by foreign espionage networks within domestic realm. MI-6 operating in the overseas realm conducts CI because its mission is to collect information outside of its home country. [45]

Strategic counterintelligence operations (SCIOs) are an operational activity, an analytical process, and delivery system that can offset the target's strengths and protect nations' most vital secrets. Through numerous historically documented double-cross-like operations, one of the potential effects of these operations is the uncovering of clandestinely recruited agents who are working on behalf of foreign powers and can then be manipulated. The ultimate goal of CE is to identify and detect a foreign power or group's clandestine intelligence operations, and to control them in order to neutralize any threats.

The scope of this literature review is narrowed to research that attempts to define what, if any, strategic role CI can play. It also examines the efforts, including theory, to define what US CI strategy should be. To explore the origins of this topic, one must first

44 John Ehrman, "Toward a Theory of CI," Central Intelligence Agency, August 24, 2009, accessed September 10, 2017, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/toward-a-theory-of-ci.html.
45 Andrew, *Defend the Realm*

understand what CI is and what it is not. Research provided by Christopher Andrew in *Defend the Realm: The Authorized History of MI-5* (New York: Alfred A. Knopf, 2009), and by Allan Dulles in *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World,* (Guilford, Connecticut: Lyons Press, 2016) serve as the foundations and lineage of the US CI system.[46]

Additionally, four contemporary researchers have also conducted serious research into the topic of CI: Michelle Van Cleave, the former National Counterintelligence Executive (NCIX) director; John Ehrman; Jennifer Sims; and Burton Gerber. Their research, however, was based on pursuing a strategic target with competing state interests, such as military technology or strategy, and fails to even address the issue of non-state threats, much less place them in focus. As seen below, the only researcher who really attempts to define what US strategic counterintelligence should be is Van Cleave.[47] Van Cleave puts forth the argument that strategic counterintelligence is a valuable tool that targets a strategic target through the use of foreign intelligence interests, which is our research and development laboratories, cleared defense contractors, and academic institutions. This is a reversal of sorts, inviting the adversary to dinner of sorts, and feeding the adversary what they wanted to eat per-say.[48]

At the onset of this research, a fundamental question was raised: what is strategic counterintelligence? Several researchers have attempted to answer what the US should be doing in counterintelligence, and a few answers have emerged. These researchers have a common baseline of what American CI is and what it should be: the manner in which the US currently practices CI is flawed; a deep understanding of the adversary requires extensive

[46] Dulles, *The Craft of Intelligence*
[47] Van Cleave, "Strategic Counterintelligence"
[48] ibid

analysis; and that analysis should be used to penetrate the inner circle of a state or non-state intelligence entity and shape what the target knows or does not know.[49505152] Sims and Gerber have taken a multi-opinioned approach from selected researchers in the disciplines of CI and foreign intelligence collection.[53] These researchers agree that counterintelligence is offensive, and the fight against the adversary must be made through expansive global operations.[54] Sims and colleagues propose that counterintelligence should be adapted to the mission or objective that one is attempting to achieve,[55] which some have argued requires the incorporation of additional theory.[56] Their conclusions point to a strong need for solutions.

Van Cleave's Perspective

In 2007, Michelle Van Cleave, the former National Counterintelligence Executive (NCIX) Director, published a piece titled "Strategic Counterintelligence: What Is It and What Should We Do about It?" In this article, Van Cleave argued that strategic counterintelligence is an underdeveloped concept that is even less understood than strategic intelligence.[57] In her view, the "signature purpose of counterintelligence is to confront and engage the adversary."[58] Van Cleave attempted to operationalize the notion of strategic counterintelligence within a large conceptual strategic context, introducing the practice as an instrument of power. A significant aspect of her argument examines on strategic counterintelligence as "the potential for engaging CI collection and operations as tools to

[49] Van Cleave, "Strategic Counterintelligence."
[50] John Ehrman, "Toward a Theory of CI: What are We Talking About When We Talk about Counterintelligence?" Studies in Intelligence, 53(June, 2009).
[51] Sims and Gerber *Transforming U.S. Intelligence*
[52] John Ehrman, "Toward a Theory of CI"
[53] Jennifer E. Sims and Burton Gerber. eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005).
[54] Van Cleave, "Strategic Counterintelligence."
[55] Sims and Gerber *Transforming U.S. Intelligence*
[56] Ehrman, "Toward a Theory of CI"
[57] Van Cleave, "Strategic Counterintelligence."
[58] ibid.

advance national security policy objectives, and, at the strategic level, to go on the offense to degrade hostile external foreign intelligence services and their ability to work against us."[59]

Van Cleave is right: history has shown that such theoretical concepts can be executed. The proof is found in the MI-5 and MI-6's use of the double-cross system in World War Two. Van Cleave reminds policy makers and readers that the US must accept three realities before strategic counterintelligence can be adopted: the threat the US faces from foreign intelligence services is strategic; strategic intelligence threats must be met by a strategic response; and a national level system must exist to integrate and coordinate activities.[60] Van Cleave asserts that the clandestine service must to take the fight to the adversary, meaning that whoever is charged with this mission must engage the adversary offensively in their country and through foreign partners. However, her perspective concerns strategic counterintelligence in support of USIC activities and political activities, which is a very traditional focus that only touches on the protection of US research and development.

Van Cleave's work also indicates why CI is not successful as a whole. From the US domestic perspective, traditional CI is approached in a manner that is case driven,[61] This narrowness of perspective, she argues, reduces the strategic impact that the practice can have on an adversary.[62] In *Counterintelligence and National Strategy*, Van Cleave dives deeper into this approach, reviewing US CI efforts since World War I and stressing the need for a more wide ranging approach employed throughout the US CI system, arguing that the "measures of effectiveness in counterintelligence-and in personal advancement in the profession have

[59] ibid.
[60] ibid.
[61] Van Cleave, "Strategic Counterintelligence."
[62] ibid.

been delimited by individual cases."[63] Van Cleave indicates that CI has been US CI is still very much focused on finding the spy, arresting the spy, and removing the threat through those means. In Van Cleave's eyes, its reluctance to delve into broader, non-governmental institutions is a major reason that the US does not meet the threat that is posed to our national security: "U.S. adversaries do not target an FBI field office, or a CIA station, or a military unit."[64] Our adversaries target banks, laboratories, defense contractors, academic institutions, and the reality is that our CI system is focused on addressing a particular problem and not addressing the whole.

Sims and Colleagues

After 9/11, the US government initiated one of the largest reviews of national security in history, and the 9/11 Commission discovered major vulnerabilities concerning the capacities of law enforcement and the intelligence community. Much of the counter-terrorism focus had been overseas; however, what was lost in all the bureaucratic reforms was the ineffectiveness of the US Domestic and Foreign CI program, which proved to be lacking. American intelligence agencies generated leads from overseas about foreign citizens that were meant to participate in the "plane operation" who ended up entering the US.[65] The indications were visible, but were not understood. No domestic CI service attempted to approach the hijackers, monitor them, or study them. According to Jennifer Sims, "the case of 9/11 reveals what can happen when intelligence and counterintelligence divorce: loss to a weaker enemy".[66] Sims expresses the importance of examining specifically how the US should effectively apply CI in order to capitalize on its strengths to exploit its competitors' weaknesses, and how to persistently exploit their operations to create advantages for US

[63] ibid., 21
[64] ibid., 21
[65] Kean, Thomas H, et al. "The 9/11 Commission Final Report." GPO Access, 4 Feb. 2009.
[66] Sims, "Twenty-first-Century Intelligence", 19.

national security. Ultimately, Sims says the "purpose is not to just manipulate or frustrate the opponent's intelligence operations, but to capitalize on what he is not doing well or is not doing at all."[67]

In *Transforming U.S. Intelligence*,[68] Jennifer Sims and Burton Gerber engaged several experts to write on various topics that are important for the transformation of the USIC. The most emergent theme of this volume is the need to overhaul or reform the USIC to support a new security environment that will be less stable and very dynamic. The researchers emphasize that the US has a dire need for warnings of emerging technology and emerging threats, as well as a new way of countering issues that will challenge elements of US national power. Much like Van Cleave, the researchers have called for a serious look at how the current USIC views the world and how the US can transform its own system.

John Gosler, a resident fellow at Sandia National Laboratories who authored the "Digital Dimension" chapter in the above-cited volume, reviewed the emergence of the cyber threat and how the social culture of the IC has had to evolve.[69] He also examined the proliferation of cyber-attack capabilities that have now found their way into even poorly funded foreign intelligence services and non-state actors, which Hezbollah demonstrated during the 2006 conflict with Israel. Gosler surmised that using technology as a spy or exploiting technology as a weakness can assist elements of US national power, or, more specifically, USIC capabilities to further intelligence collection, which could also be used for counterintelligence purposes.[70]

---

[67] ibid., 20.
[68] Sims and Gerber, ed. *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005).
[69] John Gosler, "The Digital Dimension," in Transforming U.S. Intelligence, edited by Jennifer Sims and Burton Gerber, 96-114. (Washington D.C.: Georgetown University Press, 2005).
[70] ibid.

In June 2015, the Office of Personnel Management reported that its systems had been hacked by an unknown attacker.[71] A month later, FBI Director James Comey confirmed that over 18 million government workers had been affected by the breach.[72] In December of 2015, China then announced the hack was criminal and non-state sponsored, and that the hackers responsible for the attack had been arrested. [73] This incident illustrates how a hybrid challenger can utilize cyber-espionage operations for the purposes of CI. The stolen files provided insight into the personal information of nearly 20 million government workers, including financial data, identities of family members, mental disabilities, health ailments, narcotics usage, and disciplinary information. Such data represents a treasure trove for any intelligence entity aiming to recruit human sources that have access to the information that they need.

Van Cleave and Gosler also emphasized the rise of non-traditional intelligence collection elements and the proliferation of clandestine and technical collection methods. For instance, there is evidence of non-state actors, including criminal, cyber, drug, and terrorist groups, employing counterintelligence apparatuses to monitor their own subsidiaries. These groups have to balance such trade-offs in order to elude detection and avoid compromising their own members. Blake Mobley's dissertation, *Terrorist Group Counterintelligence,* assessed how terrorist groups avoid detection, neutralization, and enhances capabilities. Mobley characterizes the process as an exercise in strategy:

> As in a game of chess, the majority of "moves" in the operational environment enhances some features of an organization's counterintelligence posture while

[71] David Bisson, "The OPM Breach: Timeline of a Hack," *Tripwire*, June 29, 2015. Accessed April 9, 2017, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/

[72] ibid.

[73] Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database", *The Washington* Post, December 2, 2015. Accessed April 9, 2017, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html?utm_term=.d68e3d7e6463

> weakening others.[74]Advanced technologies offer counterintelligence benefits but usher in new technological vulnerabilities. An increased attack tempo earns more popular support for a terrorist group, but also increases the group's operational profile. [Finally], group records enhance counterintelligence analysis, but also leave a paper trail of the organization's most sensitive personnel and activities.[75]

The goal for strategic CI operations should be to study these groups and apply game theory analysis, much like the work carried out by the Double-Cross committee in World War II.[76] Once the strategy is understood, the goal should be to force these non-state actors to make trade-offs that are beneficial to the exploitation or disruption of their activities.

Sims declares that mission-based counterintelligence operations focus on countering an adversary's intelligence service and exploiting its weaknesses.[77] Sims makes many of the same points as Van Cleave, though in Sim's view, such an activity both "targets operations before they take place and weaknesses before they are fixed"[78] and "emphasizes the offensive as it exploits gaps in the opponent's intelligence system in order to set up its own side for winning moves."[79] Sims, like Van Cleave, views CI as an operational activity that produces intelligence that can be analyzed and capitalized upon. The purpose of mission-based CI operations, therefore, is to anticipate the moves of one's adversaries and use one's advantages to counter them.[80] The principal difference between Sims' strategy and previous CI approaches is the emphasis on the acknowledgement of this reality; it is not possible to protect every bit of classified information from an interested FIE, and one has to be willing and expect a loss. Knowing that one uses adversary collection to engage the FIE, degrading

---

[74] Blake W. Mobley, *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection* (New York: Columbia University Press, 2012) 229.
[75] Blake W. Mobley, "Terrorist Group Counterintelligence" (PhD dissertation, Georgetown University, 2008). 347.
[76] Masterman, *The Double-Cross System in the War of 1939 to 1945*.
[77] Sims, "Twenty-first-Century Intelligence".
[78] ibid., 20
[79] ibid.
[80] ibid.

the FIE by providing carefully selected intelligence to the adversary and helping the FIE selectively will open opportunities for offensive operations. [81]

John Ehrman emphasizes that our lack of understanding of CI is due to it being "a neglected area of study", and his major goal is to move the US intelligence community towards a framework and theory of CI.[82] The main foundation of Ehrman's framework is a deep understanding and in-depth analysis of the adversary intelligence apparatus. This requires several different components involving intelligence operations and analysis of those operations that result in successful policy options and effects from the policy that achieve US objectives.[83] The strength of Ehrman's approach is that "it places analysis at the center of counterintelligence work but also makes clear the need for multidisciplinary approach and integrates analytical with operational activities."[84]

By applying both Van Cleave's and Sims' ideas on CI, we reach the conclusion that counterintelligence is analytical, used to enhance the security of operations and protect secrets, but it has the ability to be proactive. This is a break from the approach to traditional USIC strategic intelligence gathering operations. Much of US literature that references the topic of counterintelligence is focused on the traditional CIA approach, which is defensive operation employed to protect tradecraft, operations, and vetting of potential sources. Van Cleave and Sims advocate using the CI's capabilities to enhance intelligence collection and shape adversaries' own collections on US capabilities and intentions. Shaping adversaries' knowledge of US targets involves the use of deceptive information passed back to the adversary intelligence collection service for the purpose of exploiting how the adversary is working against you, such as determining whether they have made penetrations and

[81] ibid., 20-21
[82] Ehrman, "Toward a Theory of CI."
[83] ibid.
[84] ibid.

monitoring intelligence assets for arrest or compromising. This benefits whatever mission or strategy the US is trying to execute.

The results of the double-cross system have highlighted that CE operations also collect valuable intelligence information that can provide actionable information to identify other agent networks, adversary military capabilities, and valuable political information.

Organization of Thesis and Key Findings

Chapter 2 of this study, "Can Violent Non-State Actors be Deceived and Can States Deceive a Violent Non-State Actor Forcing the Target to Act Favorably to the Initiator?" explores whether SCIOs can be used to counter violent non-state actors (VNSA) engaging in hybrid warfare. State actors employing counterespionage operations have proven to be effective at dismantling and disrupting operations initiated by the target from within. Drawing upon cases in other countries that have been engaged in CT operations and used double-cross-like operations focusing on VNSAs demonstrates that deliberate activities can destabilize them from within by deceiving and breeding mistrust between the target members.

The flip side to that coin is that VNSAs can do the same to state actors. The evidence does suggest that violent non-state actors are often very skilled at initiating counterespionage operations and using double agents, as the double agents frequently successfully deceive state intelligence services or entities with information and evidence used to illicit a response from the target that is favorable to the initiator. Specifically, groups like Hezbollah and Al Qaeda have shown a great understanding and appreciation for SCIO like activities. Hezbollah deserves the most attention in this area due to the scale of the deception it employed against Israel.

Both state and non-state actors incorporate great sophistication into their operations, with the use of technology to mask communications, premeditated action, and a deep understanding of their adversaries' desires into their operations. Chapter 3 of the thesis, "Employment of U.S. Controlled Technology Transfer to Aid U.S. Cost Imposition Strategies", poses the following research question: can state-on-state SCIOs be an effective method for delivering cost imposition strategies to an adversary? The discussion on costs will review Russian double-cross like operations initiated against the CIA to influence US defense investments, as well as similar US operations initiated against the KGB to influence USSR defense investments during the Cold War. The examples will articulate how double-cross operations can impose a cost on an adversary, particularly demonstrating that SCIOs can be effective against a state actor. The research reveals that the US previously engaged in clandestine operations to counter Cold War adversaries attempting to acquire US restricted technologies, imposing a great cost upon the USSR. Yet, in turn, the US has also been victim to state adversary CE operations that played a part in the Department of Defense making investments based on deceptive information fed by KGB controlled double-agents.[85]

Chapter 4, titled "Double-Crossing the Computer Network Exploitation (CNE) through the Deception of the Advanced Persistent Threats (APT)", assesses whether or not SCIOs are effective and feasible in cyberspace against APTs. The relevance of this research is how it essentially outlines a framework to initiate SCIO's through a cyber medium. Through the review of current decoy systems, cyber CI practices, and APT behaviors, the results find that the use of decoy systems is proven to work against sophisticated network attackers. However, the APTs today look for specific target material. To affect the APT

[85] Benjamin B. Fischer, "Doubles Troubles: The CIA and Double Agents during the Cold War." *International Journal of Intelligence and CounterIntelligence*29, no. 1 (2015): 48-74. doi:10.1080/08850607.2015.1083313.

and the entity tasking the APT, tactically, decoy systems deceive the APT, while strategically, the target material has to be believable and contain enough feed to continually invite the APT to try again. With the use of other techniques, like using physical double agents, the likelihood of deceiving the actor increases drastically. Additionally, the cyber environment strongly enhances the effectiveness of double cross operations.

Chapter 5, titled *"*Strategic Counterintelligence Defined Through History*",* concludes with a summary of the findings. A predominant theme of the research is that there has not been sufficient exploration of U.S. economic elements in the use of SCIOs and the deliberate transfer of technology to VNSAs and VSAs for the purpose of exploitation and manipulation (except in "Operation Farewell"). The goal is to develop the essential elements needed for offensive and passive intelligence operations aimed at protecting US networks, illicit finances, and communications. Some policy and framework suggestions are also provided, setting the foundation for disruptive innovation (change).

CHAPTER 2: CAN VIOLENT NON-STATE ACTORS BE DECEIVED, AND CAN STATES DECEIVE A VIOLENT NON-STATE ACTOR?

"All Warfare Is Based On Deception"[86]
-Sun Tzu

Introduction and Research Question

Can states deceive VNSAs through double-cross like operations? Can VNSAs deceive state actors through double-cross like operations? The evolution of VNSAs has shown existing states the importance these entities place on strategy. Within the context of this research, the use of deception is viewed in a multifaceted manner, and not simply as a theory of "hoodwinking" one's opponent. History has shown that deception occurs regularly and is often times practiced more by US challengers. However, this analysis will focus on states and whether it is possible to deceive a VNSA, and if a VNSA can deceive a state.

Hypotheses:

I offer two hypotheses for investigation in this chapter:

H1 States can deceive VNSAs; and

H2 VNSAs can deceive states.

Review of the Literature

This literature review focuses on two main questions. First, is there evidence of states deceiving VNSAs? Second, do VNSAs deceive states? Literature searches identified the use of CI techniques employed by the British and Saudi states that employed deliberate and reactive double-agent operations to engage a VNSA and provide them with deceptive information for a strategic interest. These interests, on behalf of both states, ranged from

[86] Lionel Giles, trans., *Sun Tzu on the Art of War* (Leicester, UK: Allendale Online Publishing, 2000), 3.

reducing the risk a VNSA posed to the internal security of the state and building better capacity with partners.

MI-5/FRU vs. PIRA

"The trick is to not mind killing, and to expect dying."[87]
Kevin Fullton

MI-5/FRU deceiving PIRA

Reviewing the literature pertinent to CI operations launched against non-state actors, such as the Provisional Irish Republican Army (PIRA), is essential to this research because the US and British also used the PIRA test cases for various military counterinsurgency and irregular warfare studies. The rise of the PIRA was aided both by the local populace and the ineffective strategy employed by the United Kingdom, whose intelligence services were challenged early on in the conflict.[88] However, PIRA's CI focus was on supporting operational intelligence development and operational security measures to mask and hide operations,[89] which was needed because PIRA had to maintain the credibility that it was an effective and powerful organization.[90] CI methods employed by the United Kingdom's Security Service MI-5 against PIRA, as a whole, emphasized recruiting and inserting a mixture of double agents and controlled sources to penetrate PIRA. Those penetrations would identify PIRA members for surveillance, allowing MI-5 (or later FRU) to disrupt and interrogate them.[91] This strategy worked, though it was costly for both services. PIRA challenged MI-5 and other UK intelligence elements in a manner that required a drastically different response than the methods previously used against the organization. For the

[87] As quoted in Matthew Teague, "Double Blind: The Untold Story of How British Intelligence Infiltrated and Undermined the IRA," *The Atlantic* (April 2006).
[88] Mobley, *Terrorism and Counterintelligence*.
[89] Gaetano Joe Ilardi, "Irish Republican Army Counterintelligence," *International Journal of Intelligence and CounterIntelligence*, 23 (2010).
[90] ibid.
[91] Ilardi, "Irish Republican Army Counterintelligence."

intelligence service to be relevant during an insurgency, information had to be timely and relevant to the tactics employed at the time.[92]

When analyzing the British security services operations aimed at PIRA, it became clear that PIRA played the same game against MI-5. It is important to note that PIRA had studied British security service CE operations, so the organization was well aware of the sophisticated CE techniques that MI-5 would take in its attempts to counter PIRA operations.[9394] This was a highly sophisticated and complex CE vs. CE campaign, which involved using deceptive information in an effort on both sides to ferret out informants and enhance military operations. Both PIRA and MI-5 aimed to destabilize and affect each other to establish dominance.[95] Ilardi argued the basics of PIRA's CI analysis of MI-5 and later FRU were formed from CE operations run against MI-5 using PIRA's own developed double.[96] Both MI-5 and PIRA relied on basic human intelligence collection within their areas of interest. PIRA focused on developing sources of information within their controlled territory and areas that were being prepared in forward areas of Great Britain outside their established safe areas. MI-5 did the same thing, working the streets, developing sources of information through various military raids, and police activities. These various sources of information were crucial into forming their respective CE operations, which appeared to focus on the disruption of each other's intelligence gathering and military operations.[97]

British government officials, intelligence historians, and journalists have cited several cases that highlighted the use of CE-like operations with a double-cross system activated with the goal of penetrating PIRA's organization. The known successful penetrations were

---

[92] ibid.
[93] Andrew, *Defend the Realm*.
[94] Ilardi, "Irish Republican Army Counterintelligence."
[95] ibid.
[96] ibid
[97] ibid.

of PIRA's internal security and operational planning apparatus. MI-5, was in the position to direct, manage, and gather operational intelligence that could be used to feed surveillance teams and interrogations.[98] The successful use of operational intelligence helped destabilize the PIRA and fracture its powerful public image. One of the major advantages of these types of CI operations is the means to act at will. Another advantage of these CE operations was that with the penetration, the aggressor eliminated PIRA's ability to "operate clandestinely and maintain at all times the essential element of surprise."[99]

Other early CE operations focused on penetrating PIRA's CI and security apparatus. With that penetration, they learned what PIRA's structure was and how it worked, which allowed for more focused surveillance and enabled MI-5, along with other British services, to identify candidates for recruitment to become double agents from within the organization. With this accomplished, the CE operations next concentrated on penetrating the heart of the organization, which involved both the collection of valuable threat information on target selection and planning and the study of PIRA's military strategy.

Many Irish saw the British as "occupiers",[100] while the PIRA were perceived as the good forces who fought to push out these oppressive forces.[101] Like many paramilitary groups fighting for a cause, PIRA took up efforts within their communities that legitimized its group, calling to young, disenchanted youth and speaking to the poor. PIRA flooded Ireland with money from charities and groups outside the United Kingdom (UK). They urged the youth to fight for a cause, employing TTPs that centered on intimidation, subversion, and terrorist-like behaviors. A response was needed to tackle this issue and provide warning to the British Army. The British needed real-time intelligence that could

[98] ibid.
[99] ibid., 5.
[100] ibid.
[101] ibid.

assist in disrupting assassinations, bombings, and other violent acts. As a result, the British military created a joint CI unit named the Force Research Unit (FRU).

"The FRU recruited and ran agents within PIRA."[102] FRU essentially recruited PIRA members already working within the organization as double agents. The "Program", as it was called, emphasized the recruitment of British military soldiers that had familial ties or who grew up in controlled PIRA areas.[103] The Program not only recruited soldiers to be double agents, but also pursued soldiers who had experience and background in explosives, weapons and intelligence, skills that were badly in need by PIRA. This almost guaranteed the asset direct access to planning and PIRA capabilities. The double agents were providing information ranging from low- grade to high-grade intelligence, which spanned from gossip to imminent attacks on British targets.[104] This program was highly effective for several reasons. First, other penetrations the British security services were running within PIRA's internal security service provided their handlers what PIRA needed and insights on next moves. Second, PIRA needed recruits with experience who could be trusted, and the British security services provided them in the form of soldiers. These former British soldiers were under British control with skills the PIRA needed. Finally, once their double agents were established, the British were able to effectively and surgically destabilize PIRA's leadership and morale.[105]

However, MI-5 and the UK's other intelligence elements were not the only side to engage in CE. PIRA adopted passive and active methods of CE as well. PIRA employed passive methods to vet volunteers prior to PIRA acceptance, and adopted CI as a top

---

102 Teague, "Double Blind."
103 Teague, "Double Blind."
104 Teague, "Double Blind."
105 Gaetano Joe Ilardi, "Irish Republican Army Counterintelligence," International Journal of Intelligence and CounterIntelligence 23, no. 1 (2009): , doi:10.1080/08850600903347152.

priority for the organization. An example of this was how PIRA took a more violent and harsh approach on internal security measures in order to deal with suspected MI-5 informants and collaborators.

PIRA deceiving MI-5/FRU

As Mobley highlighted in *Terrorism and Counterintelligence*, MI-5 and the FRU were not the only organizations that successfully ran aggressive CE operations. PIRA was able to mount successful CE operations aimed at ferreting out double agents working for the FRU. This was done at times by applying the lessons learned from British run operations. PIRA's most successful CE operations were the penetration and compromise of the UK's treasury department, and the West German operation and the retrieval of the Castlereagh Special Branch headquarters files on informants actively supporting UK security service operations. The compromise of UK treasury department workers helped identify government checks sent to citizens who were providing information on PIRA activities in the controlled territory.[106]

The second compromise was decried by British tabloids as "catastrophic a failure of British intelligence as was Kim Philby's defection to Moscow a generation ago."[107] The result of the compromise of joint British and West Germany CI operations was the loss of several direct access cooperating sources that fed information to the UK's security services. Research shows that PIRA kept these records for a period of time prior to releasing them, which, if true, would mean that PIRA's CI staff identified the cooperating sources and either executed or turned the UK's security service operations against them.[108] The "infiltration of the Castlereagh Special Branch headquarters in 2002 netted the IRA computer disks with the

[106] Ilardi, "Irish Republican Army Counterintelligence"; Mobley, *Terrorism and Counterintelligence.*
[107] Duncan Campbell, "Carry on Spying—And Dying?" *New Statesman Society* (October 20, 1989), 12.
[108] Campbell, "Carry on Spying—And Dying?"; Ilardi, "Irish Republican Army Counterintelligence."

names and addresses of more than 250 serving and former Special Branch, the code names of informers, and details of the information they provided to the security services."[109]

Saudi Security and Intelligence Services vs. Al Qaeda Arabian Peninsula

Saudi Arabia Intelligence Double Agent Operation

In 2012, the Saudi external and internal intelligence services, along with the U.S. Central Intelligence Agency (CIA), participated in an operation that enabled one of the first publicly known penetrations of Al-Qaeda. Nevertheless, there is evidence that the Saudi internal and external intelligence services had been performing these types of operations for years.[110] For instance, Saudi internal and external intelligence services disrupted a plot to take down U.S. airliners with a new explosive device that was potentially difficult for U.S. transportation security screeners to detect.[111]

Prior to the Saudi disruption of the operations by the Al-Qaeda Yemen based group, one of the would-be bombers was actually a Saudi intelligence double agent.[112] The goal of the double agent was to penetrate Al-Qaeda in Yemen and convince his handlers of his loyalty in order to gain access to planning activities. However, one ripple occurred, and the double agent was not granted access to the planners, as the Saudi Security services would have thought. Instead the double agent was kept far away from the planning cell and was trained only in detonation of the bomb.[113] Eventually, the agent's Al Qaeda handlers gave him orders to use the new explosive device, which he communicated with his Saudi handlers, and he was instructed to slip away with the device and as much "valuable information" as possible.[114] After this operation, former Director of the CIA Michael

[109] ibid. 20.

Hayden said that "the effect is everyone on the inside is now looking at everybody else on the inside, and you're creating suspicions inside the network."[115]

Evidence of VNSAs Deceiving States

Hezbollah vs. Israel

Carl Anthony Wege has provided a historical review of the organizational structure of Hezbollah and its CI operational successes after the 2006 conflict with Israel. Hezbollah's intelligence and counterintelligence roots are found within the Iranian Pasadran and Quds forces.[116] Wege specifically emphasized that non-state actors that receive state assistance (Iran was providing aid to Hezbollah) are truly a force with which to be reckoned. Groups like Hezbollah have received funding, training, and weapons from Iran since the inception of the group, as confirmed in the Middle East Institute article, "Hezbollah Deputy Leader Expresses Gratitude in Iran and Syria".[117]

Hezbollah has a very extensive history of running CI and CE operations, detecting spies, and manipulating state intelligence security services. Wege's brief historical overview of Hezbollah CI operations began in the late 1980s, when the organization identified several Lebanese nationals who were employees of the Lebanese Cyprus ferry lines and providing

---

[110] Max Fisher, "What We Can Learn from Saudi Intelligence," *The Atlantic* (November 1, 2010). Accessed April 10, 2015, https://www.theatlantic.com/international/archive/2010/11/what-we-can-learn-from-saudi-intelligence/65518/

[111] Scott Shane and Eric Schmitt, "Qaeda Plot to Attack Plane Foiled, U.S. Officials Say," *The New York Times* (May 7, 2012). Accessed on February 10, 2016, http://www.nytimes.com/2012/05/08/world/middleeast/us-says-terrorist-plot-to-attack-plane-foiled.html

[112] Todd Eastham, "Yemen Underwear Bomber Was 'Saudi Double Agent,'" *The Independent* (May 9, 2012).

[113] Ellen Knickmeyer and Siobhan Gorman, "Al Qaeda Double Agent Had Western Roots," *The Wall Street Journal* (May 10, 2012). Accessed April 10, 2017, https://www.wsj.com/articles/SB10001424052702304203604577396572887391582

[114] Ken Dilanian and Brian Bennett, "Al Qaeda Bomb Plot Was Foiled by a Double Agent," *Los Angeles Times* (May 9, 2012). Accessed June 15, 2014, http://articles.latimes.com/2012/may/09/world/la-fg-bomb-plot-20120509

[115] Knickmeyer and Gorman, "Al Qaeda Double Agent Had Western Roots."

[116] Carl Anthony Wege, "Hizballah's Counterintelligence Apparatus," *International Journal of Intelligence and CounterIntelligence*, 25 (2012).

[117] Alex Vatanka, "Hezbollah Deputy Leader Expresses Gratitude to Iran and Syria," *Middle East Institute*, January 27, 2017. Accessed January 30, 2017, http://www.mei.edu/content/is/hezbollah-deputy-leader-expresses-gratitude-iran-and-syria

information on passengers and cargo to the CIA.[118] An additional gain for Hezbollah was acquiring the knowledge that the CIA was actively developing and recruiting sources of information using the ferry lanes. Just as Hezbollah was smuggling equipment and information into the region, the CIA was doing the same. Another major Hezbollah CI victory occurred in 1994, when the group prevented the CIA-engineered kidnapping of a senior Hezbollah officer who ran its foreign operations branch.[119][120] Hezbollah identified the compromised Amal agent who was assisting the CIA and exploited that nexus to prevent the kidnapping.[121] Essentially, Hezbollah had turned the CIA's prized asset into its weakest link.

Hezbollah's use of CE against the Israeli security services went on display from 1997 through 2000. In 1997, Hezbollah manipulated IDF double agents by providing them with deceptive information that led to the death of elite Israeli naval commandos.[122] One of Hezbollah's most sophisticated CI operations occurred three years later: the reversing of an Israeli Mossad false flag operation that had been launched at Hezbollah.[123] Rather than resulting in a success for Mossad, Hezbollah lured the Mossad officer to Lebanon, where he was arrested.[124]

Well before the summer of 2006, Hezbollah had initiated efforts to disrupt and blind the Israeli intelligence network in Lebanon. During the 2006 IDF vs. Hezbollah conflict, unbeknownst to Israel security services, Hezbollah CI officers compromised IDF Lt. Col Omar al-Heib, who provided detailed "surveillance data on IDF military installations to

[118] Wege, "Hizballah's Counterintelligence Apparatus." 773.
[119] ibid.
[120] ibid.
[121] ibid.
[122] ibid.
[123] Wege, "Hizballah's Counterintelligence Apparatus."
[124] ibid.

Hizballah in return for narcotics."[125] Wege's review of Hezbollah's CI use paints a picture of the sophistication, growth, and desire for more offensive-based activities that emerged to enhance the organization's military capabilities and operations against Israel.

This case study particularly highlighted a non-state sponsored group's use of multiple modes of deception to mask the employment of advanced weapons systems, combining them with irregular tactics to inflict lethal consequences on an adversary. The significance of Hezbollah's strategy is a warning to many countries that rely on hard power. Hezbollah, a non-state actor, had the ability to run effective CE operations against Israel, which has one of the most feared intelligence and security services in the world.[126] The human sources did not completely destroy the Israel Defense Forces (IDF) or Israel, but they helped paint a picture that deceived the IDF.

Hezbollah had initiated the deception campaign years before.[127] However, the other unique aspect of this war was the calculated planning and deliberate employment of a deception campaign by its leadership. The group approached a military conflict with Israel in a manner similar to the application of game theory.[128] It was clear that the IDF reacted the way in which Hezbollah expected. As a result, Hezbollah could then engage the IDF's heavy armor and soldiers lethally, causing the IDF to take pause. In the 2006 case, the group also showed reliance on outside influences like Iran, which provided Hezbollah with the advanced weapons, advanced signals, intelligence equipment, and essential Israeli strategic intelligence vulnerabilities that allowed Hezbollah to use missiles to exploit the IDF, causing a number of civilian casualties within Israel. However, the IDF could also exploit

---

[125] ibid., 776; Amir Kulick, "Hezbollah vs. the IDF: The Operational Dimension," *Strategic Assessment*, Jaffee Center for Strategic Studies, Tel Aviv University, 9 (November 2006).
[126] Kulick, "Hezbollah vs. the IDF."
[127] Acosta, "The Makara of Hezbollah."
[128] ibid.; Kulick, "Hezbollah vs. the IDF."

Hezbollah's reliance on Iran to become Hezbollah's greatest weakness, particularly if a dedicated strategic counterintelligence campaign was launched by the IDF. Thus, this campaign would not only have to focus on Hezbollah, but on Iran as well. A closer review of the deception is needed to showcase the effectiveness of the VNSA's ability deceive a hard power reliant state actor.

The Deception Dimension

Hezbollah's use of deception is of great note. Hezbollah's overall military strategy shocked many western militaries because of its sophistication, deliberateness, and ability to inflict surprise upon the IDF, which is one of the most capable militaries in the Middle East. The initiator of deception (Hezbollah) upon the target (IDF) was a deliberate campaign designed to effectively blind the IDF's military and civilian intelligence apparatus. Hezbollah's use of deception was prevalent in four areas:

Act	Level of Warfare	Description
Fake Bunkers	Tactical	Hezbollah built fake bunkers to confuse Israeli Intelligence about the actual location of their bunkers.
Electronic Warfare Bluff	Tactical/Operational	Hezbollah bluffed about being able to listen into Israeli security frequency hopping radios.
The Media	Operational	Hezbollah used the media as its tool to conceal its use of civilian areas to launch rockets.
Hijacking the Internet	Tactical/Operational	Hezbollah "hid" on the internet service providers in the US to maintain its capability to broadcast via broadband.

Figure 1. Hezbollah's use of deception.[129]

Hezbollah's hybrid military strategy sent a message to Israel and others that Hezbollah could humiliate the IDF. Within the opening hours of the war, the IDF launched a brutal air

[129] Acosta, "The Makara of Hezbollah."

campaign into the south of Lebanon. The "five key Israeli objectives for the war" included:[130]

- Destroy the Iranian Western Command before Iran could "go nuclear";
- Restore the credibility of Israeli deterrence after the unilateral withdrawal from Lebanon in 2000 and Gaza in 2005, and counter the image that Israel was weak and forced to leave;
- Force Lebanon to become and act as an accountable state, and end the status of Hezbollah as state within a state;
- Damage or cripple Hezbollah, with the understanding that it could not be destroyed as a military force and would continue to be a major political actor in Lebanon;
- Bring the two captured Israeli soldiers back alive without major trades in prisoners held by Israel.

Within hours of the war's initiation, the IDF Navy created a blockade on Lebanese ports with the hope of cutting off illegal weapon shipments. The IDF air campaign began with a series of hard-hitting attacks, targeting missile locations and infrastructure and hitting "54 long range rocket and missile launch sites in 39 minutes on the first day of the conflict." [131] However, the IDF and the Israel populace were still coming under siege from Hezbollah "Katyusha rockets on Israel's northern towns and villages daily",[132] while in the first three days of the attack, IDF's air assault appeared to do little to no damage to Hezbollah's rocket barrages.[133]

[130] ibid. 38
[131] ibid., 39
[132] ibid., 39
[133] Acosta, "The Makara of Hezbollah."

Blinding the IDF through Denial Operations

Years before the 2006 offensive, Hezbollah aimed to deny Israel the use of sensors. In this case, the sensors were Israeli run human intelligence networks that had been targeted and exploited years in advance.[134] Hezbollah developed a counterintelligence capability through the use of signals intelligence collection to produce actionable information that allowed its security apparatus to identify Israeli-run human intelligence networks. Hezbollah would then approach the suspected spies working for Israel and, similar to the British DC Operation, would either double them or arrest them.[135] Hezbollah did not end double agent operations there, however, but identified other Israel intelligence networks that were reporting on Hezbollah weapons cache locations and other sites, again using the double agent concept to "turn" these new agents to deliver inaccurate information. As Perry and Crooke state, "Hezbollah effectively closed down Israel's human intelligence capability", [136] and the results were highly damaging to IDF's overall fighting strategy in 2006.

Bunkers-

Shortly after the Israeli withdrawal from Southern Lebanon, Hezbollah began to lay the foundations to use deception to inflict strategic surprise upon the IDF. This included test cases and other mechanisms to practice deception. From the year 2000 onwards, Hezbollah implemented an "elaborate construction effort of display fortification along the Blue Line with the intent of deceiving information gathering assets such as Israel unmanned aerial vehicles, United Nation (UN) monitors, and Lebanese spying for Israel."[137] Following

---

[134] Mark Perry and Alistair Crooke, "How Hezbollah Defeated Israel, Part 1: Winning the Intelligence War," *Asia Times* (October 12, 2006). Accessed April 9, 2016, http://www.atimes.com/atimes/Middle_East/HJ12Ak01.html

[135] Richard Schultz and Roy Godson, "Intelligence Dominance: A Better Way Forward in Iraq," *The Weekly Standard* (July 31, 2006). Accessed April 9, 2017, http://www.weeklystandard.com/intelligence-dominance/article/13606

[136] Perry and Crooke, "How Hezbollah Defeated Israel, Part 1."

[137] Acosta, "The Makara of Hezbollah." 43

these deceptive measures, Hezbollah targeted Israeli intelligence sensors (UAVs, UN monitors, spies), and deliberately provided observables to the overt and clandestine Israel intelligence sensors, informing them that these were the Hezbollah bunkers. During the 2006 conflict, it became known that those bunkers were decoys. During the construction time frame of the dummy bunkers, Hezbollah was building the real bunkers to be used for a conflict with the IDF elsewhere. Tunnels and fiber were laid; creating a communications network that could prevent disruption by IDF electronic countermeasures.[138] The results of this deliberate deception targeting Israel's intelligence sensors conditioned the IDF to believe they knew the location of Hezbollah's bunkers early on in the campaign, allowing Hezbollah to operate elsewhere with little threat of an IDF attack. The results gave Hezbollah the tactical breathing space to effectively engage IDF ground forces.[139]

Electronic Warfare-

Hezbollah essentially planted information through counterintelligence operations (and executed through electronic communications) that would be received by IDF signals intelligence systems. The information Hezbollah planted suggested that they were somehow able to decrypt IDF secure communications. IDF military analysts concluded that this must have been one of the reasons as to why IDF efforts in the south of Lebanon had been going so poorly.[140] Analysis after the fact proved that Hezbollah (with the assistance of Iran) had not actually hacked or cracked the encryption.[141] What Hezbollah really did was create doubt within the IDF about its communications, and through timing and the use of the media, enhance the planted information, further allowing the lie to form into a reality. The

[138]ibid.
[139] ibid.
[140] ibid.
[141] ibid., 47

operational implications caused the IDF to take a tactical pause and "rethink their communications network in the wake of Hezbollah's alleged EW capabilities."[142]

The Media-

Hezbollah had propaganda material ready to provide the media outlets before the conflict began as well as during the war. Hezbollah messaged the content in a manner that misled the media and Israeli society, specifically targeting journalists with the facts and stories they wanted printed.[143]

Hijacking the Internet-

Hezbollah also displayed its cyber prowess during the 2006 conflict, deliberately employing an offensive cyber campaign, which, while not as strong as a state-sponsored campaign was nonetheless highly significant. In order to balance the IDF's computer network operations, Hezbollah built extensions off US based network routers that would be used in the event that Israel tried to deny Hezbollah's communications infrastructure. Hezbollah identified a series of websites primarily located in the US that were vulnerable to Hezbollah cyber tools and hijacked them.[144] These websites served as tunnels for covert communications, though the overall application failed due to the efforts of informal, non-state sponsored networked groups such as the Society for Internet Research, who were able to track Hezbollah's activities and report them to the US government.[145]

The use of deception in the 2006 Hezbollah and IDF conflict is of great importance, particularly in the context of the employment of SCIOs. During this type of warfare, information has become a critical element to either support a hybrid military strategy or

[142] ibid.
[143] ibid.
[144] ibid.
[145] ibid., 59

counter a military strategy employed to defeat hybrid challengers. Information for targeting, propaganda use, and defense decision-making has to be protected from manipulation and deception from a hybrid challenger.

David Acosta has proposed that "Hezbollah and Israel serve as the perfect backdrop to examine the effects of deception in current asymmetric conflicts."[146] The comparison Acosta chose is the contemporary David vs. Goliath battle, in which David is represented by Hezbollah and Goliath is Israel. David balanced Goliath's clear hard power advantage through the use of deception, which inflicted military and technical surprise upon the IDF, reducing the advantage the IDF had in several military areas, and making the battle an even fight. Acosta cites the work of Marvin Kalb, who wrote *The Israel-Hezbollah War of 2006: The Median as a Weapon in Asymmetrical Conflict*, in which he expressed the conclusion that Hezbollah won in the area of "information and news propaganda".[147] Both authors have attributed Hezbollah's success to the use of *makara*, which is the Arabic word for deception. The variable that helps non-state actors like Hezbollah is the openness of democracies such as Israel. Israel, as described by both authors, is a relatively open society that is at times very critical of its own political, defensive and national leadership, with contention among diverse opinions sometimes hampering the process of decision-making and disrupting the momentum of offensive actions. Hezbollah's closed society and ability to control the news flow and propaganda bombarding its supporters is one of its greatest strengths, because it helps the organization remain resilient in the face of the hard Israeli military approach to the Hezbollah issue.

---

[146] David Acosta, "The Makara of Hezbollah: Deception in the 2006 Summer War" (Ph.D. diss., Naval Postgraduate School, 2007). 2

[147] Marvin Kalb and Carol Saivetz, "The Israel-Hezbollah War of 2006: The Median As A Weapon in Asymmetrical Conflict," *The International Journal of Press/Politics*, 12 (July 2007). 44

What these authors mean is that every hard power attack launched by the IDF opens up the IDF more to Hezbollah's influence, and risks manipulation of the IDF's intended mission. The authors also highlighted that Hezbollah's information collection operations took place through the use of offensive counterintelligence operations, or CE. These operations led to the collection of valuable foreign intelligence on the IDF that was used in turn to collect more information and enhance Hezbollah's deception campaigns to neutralize IDF military tactics. It is clear that this was the result of IDF's significant hard power capability.[148] Acosta's research cites specific examples of Hezbollah's employment of deception tactics through information sources such as human assets, news media outlets, and social media posts, arguing that all assisted in "significantly offset[ing] many of Israel's hard power advantages."[149] Acosta's research offers a new model for information flow to the hierarchy, which gives insight to how Hezbollah's use of deception masked their tactics, objectives, and reduced IDF's ability to provide warning.

In actuality, IDF's intelligence apparatus had no indications or warning that Hezbollah was planning such a grand operation. Part of the challenge that Hezbollah continues to pose to the IDF is in its ability to employ conventional warfare-like tactics, employing high tech and low tech weapons effectively while using highly skilled irregular tactics, coordinated operations, and sophisticated communications to strike with precision. As Hoffman has assessed, Hezbollah "withstood the attack and fought back. It did not wage a guerilla war either… it was not a regular army but was not a guerilla in the traditional sense either. It was something in between. This is the new model". [150]

[148] Acosta, "The Makara of Hezbollah."
[149] ibid., 2-3
[150] Hoffman, Conflict in the 21st Century.

Al-Qaeda vs. CIA

In the 1990s, Al-Qaeda was a little known terrorist group primarily based out of the country of Sudan. Its international and popular support grew over the Muslim world. Al-Qaeda operated largely under the radar of the US intelligence community, mostly because of its ability to conduct counterintelligence activities and feed that collected information to enhance their operational security of their cells. When former CIA director George Tenet discussed Al Qaeda's operational capabilities before the 9/11 Commission, he noted that "based on what we know today, the investigation of the 9/11 attacks has revealed no major slip in the conspirator's operational security."[151] In his study, "The 9/11 Attacks-A Study of Al Qaeda use of Intelligence and Counterintelligence", Gaetano J. Ilardi attributed great significance to this statement "because it conceded that the hijackers did not reveal their intentions, but also because subsequent investigation, even with the benefit of hindsight, was unable to detect significant lapses in the conspirator's counterintelligence tradecraft."[152] Ilardi's piece is interesting because rather than highlighting Al Qaeda's strategies of surprise, he simply reminded the reader that Al Qaeda trod a very deliberate path in taking the fight to the US.[153] In other words, the US had dismissed Al Qaeda, not appreciating the threat, and the value of surprise cannot even be assessed because Al Qaeda told the US very publically that it would be attacking the homeland. Ilardi has also noted how Al Qaeda cell formed its plan by studying operational realities and developing knowledge of US security and law enforcement capabilities, and that much of its operational plan was continually adjusted,

---

[151] George Tenet, "Unclassified Version of Director of Central Intelligence George J. Tenet's Testimony Before the Joint Inquiry into Terrorist Attacks Against the United States," *DCI Testimony Before the Joint Inquiry into Terrorist Attacks Against the United States* (June 18, 2002). Accessed January 15, 2016, https://www.cia.gov/news-information/speeches-testimony/2002/dci_testimony_06182002.html.
[152] Gaetano J. Ilardi, "The 9/11 Attacks-A Study of Al Qaeda use of Intelligence and Counterintelligence," *Studies in Conflict and Terrorism,* 32 (March 2009). Doi: http://dx.doi.org/10.1080/10576100802670803.
[153] ibid.

even on the day of the execution of the operation.[154] This could be a potential area to exploit in the future.

Through his research, Ilardi articulated Al Qaeda's use of deception and which is similar to Russia's intertwining of deception and OFCO, also known as *maskirovka*.[155][156] "In fact, this deception proved so effective precisely because it was based on the hijacker's keen knowledge of their adversaries' own perceptions and preconceived ideas."[157] Al Qaeda's security measures were developed in order to cover all actions before the hijackers ever appeared on American soil. The use of non-alarming personalities did not trigger reactions from the US security and law enforcement services, as the selected hijackers were rational and able to live the double lives needed to achieve their group's objectives. Non-state actor's intelligence and counterintelligence practices seem to be their greatest strength because those actions form a security umbrella. Once that has been compromised, the rest of the operational activities can be manipulated and even disrupted.

Double agents have become a valuable tool for VNSAs, including Al Qaeda. One example is the story of Humam Khalil al-Balawi, the subject of Joby Warrick's book, *The Triple Agent: The Al-Qaeda Mole Who Infiltrated the CIA*. This story begins in the country of Jordan in 2009. The CIA and many intelligence services in the Gulf region had been inundated with the desire to penetrate Al Qaeda,[158] Jordan's internal security service, known as the Mukhabarat, shares a very close relationship with the CIA, often working hand in

---

[154] ibid.
[155] Gaetano Joe Ilardi, "Al-Qaedas Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control," International Journal of Intelligence and CounterIntelligence 22, no. 2 (2009): 247-250, doi:10.1080/08850600802698226.
[156] Joergen Oerstroem Moeller, "Maskirovka: Russia's Masterful Use of Deception in Ukraine," The Huffington Post, April 23, 2014, , accessed May & june, 2016, http://www.huffingtonpost.com/joergen-oerstroem-moeller/maskirovka-russias-master_b_5199545.html.
[157] Ilardi, "The 9/11 Attacks."
[158] Joby Warrick, "CIA: Systematic Failures Led to Suicide Attack," *The Waashington Post* (October 20, 2010). Accessed April 9, 2017, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/19/AR2010101907514.html

hand, [159] and the Mukhabarat alerted the CIA of a blogger critical of Western policies whom they had been monitoring online. Investigative reporting by Evan Kohlman later uncovered an online profile that actually belonged to Al-Balawi, who had been chatting on various online forums linked to Al Qaeda.[160] Al-Balawi would not take up issues with the West in these discussions, but rather often challenged Jordanians themselves.[161] Through some means, it was determined that Al-Balawi had access to Al Qaeda, and during interrogations, the Jordanians attempted to sway him and convince him to use his access to Al Qaeda to assist the Mukhabarat, providing them with key information on members and leaders, and sharing knowledge of operational plans. The Mukhabarat was working to turn Balawi into a double agent.

Mukhabarat officers suggested that Balawi travel to Pakistan to offer his medical services to Al Qaeda.[162] From that point, Balawi made his way into Afghanistan, linking up with Al-Qaeda.[163] Balawi re-contacted the Mukhabarat to inform them that Al Qaeda's members had introduced him to the number two in command, Ayman al-Zawahiri, and sent videos of himself treating a senior aide to Osama Bin Laden. [164] Mukhabarat and the CIA thought they had finally acquired a source within Al Qaeda. However, it appears that all Balawi was trying to do was increase his bond with the terrorist group while simultaneously working to improve his credibility with the CIA and Mukhabarat. [165]

---

[159] ibid.
[160] Robert Windrem and Richard Engel, "Al-Qaida Double Agent Killed CIA Officers," *NBC News* (January 04, 2014). Accessed January 12, 2016, http://www.nbcnews.com/id/34687312/ns/world_news-south_and_central_asia/#.WPxA8FN94o8. Fdjf
[161] ibid.
[162] ibid.
[163] Bruce Reidel, "Khost CIA Attack: Lessons One Year Later," *The Daily Beast* (December 29, 2010). Accessed April 9, 2015, http://www.thedailybeast.com/articles/2010/12/29/khost-cia-attack-lessons-one-year-later.html
[164] ibid.
[165] ibid.

Sometime in December 2009, Al Qaeda planned to lure the Mukhabarat officers to a meeting location, where Balawai would detonate himself. Sharing the videos and passing accurate information were setting the stage for a re-contact meeting with his CIA and Mukhabarat handlers. According to a later review of the case conducted by Bruce Reidel, videos and literature released by Al-Qaeda showed Balawi with an Al-Qaeda leader discussing plans to blow up the CIA forward operating base in Khost, Afghanistan.[166] Other videos appeared to be debriefings conducted by Al-Qaeda members of Balawi, during which Balawi detailed how he dangled himself in front of the Mukhabarat, gaining access to Mukhabarat headquarters and described meetings with his handlers, revealing his initial objective of kidnapping a Mukhabarat officer.[167] Balawi himself provided his Al-Qaeda handlers the tactics, techniques, and procedures of the Mukhabarat.[168] During the interview with Balawi, he exploited previous Jordanian Mukhabarat intelligence operations run against Al-Qaeda and other extremist groups. Unbeknownst to the CIA Al-Balawi was already a double agent.

The CIA arranged for Balawi to come to Khost, Afghanistan, where he could be debriefed securely. However, Balawi was never debriefed. On 30 December 2009 Al-Balawi took the lives of nine CIA intelligence officers, including a Mukhabarat officer. Post-event analysis determined three things: Balawi was a triple agent who took direction and orders from Al-Qaeda; no formal counterintelligence vetting was ever carried out on Balawi; and Al

---

[166] ibid.
[167] Bill Roggio, "CIA Agents Killed in Suicide Attack 'A Gift from Allah'," *Long War Journal* (March 1, 2010), Accessed April 9, 2017, http://www.longwarjournal.org/archives/2010/03/cia_agents_killed_in.php
[168] Bill Roggio, "Transcript of Interview with Jordanian Suicide Bomber Khurasani," *FDD's Long War Journal* (March 1, 2010). Accessed April 9, 2015, http://www.longwarjournal.org/archives/2010/03/transcript_of_interview_with_j.php

Qaeda seemed to have run a sophisticated operation that was designed to bait two highly experienced intelligence services.[169]

Analysis of Data

Material evidence has been presented to support conclusions 1 (C) and 2 (C): both entities can be deceived. However, the selected test cases focused on the discipline of CI collection, which was used to mount effective CE operations that were used on behalf of the respective intelligence and security services. CE operations can have an impact upon a state intelligence service as well as non-state intelligence entities. It is also clear that costs were leveled upon the target of the initiator. Essentially, MI-5/FRU teams were successful at infiltrating PIRA and destabilizing the organization from within. The British security services were able to "infiltrate the IRA, spreading deceit and rumors of deceit",[170] which was a very effective strategy. Another important point is that the use of operational security was paramount to avoid detection by the other side, especially during the information-gathering phase. What evidence is missing, whether because it does not exist or has not been found, is the deliberate compromise of an operation for the purpose of denying the target the ability to gain access to the true intentions of the initiators activity. That is clear use of deception operations designed to actively deny the target access to information of value.

Finally, the initiator defines what "deception" means not contemporary academically accepted definitions, and one can argue that PIRA's use of false information resulted in the British being deceived into acting on something false, creating tactical opportunities for PIRA. Hezbollah used deceptive information to identify Israelis intelligence sources and to

[169] Steven J. Garber, "Intelligence in Public Literature," Central Intelligence Agency, November 09, 2011, , accessed August 10, 2014, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-3/the-triple-agent-the-al-qaeda-mole-who-infiltrated-the-cia.html.
[170] Teague, "Double Blind"

enhance Hezbollah military operation to create tactical victories and strategically message to others regionally that David (Hezbollah) was able to hurt Goliath (Israel).

MI5/FRU vs. PIRA

It is important to note the effectiveness of CE operations that the British intelligence and security services operated against PIRA. Through placing double agents with skills needed by PIRA, the British were able to gain direct access to planning and information on the execution of attacks. As a result, British intelligence and security services could increase the credibility of the double agents by placing them into positions that allowed the use of techniques to destabilize PIRA from within.

One of Britain's most effective double agents was codenamed StakeKnife,[171] and his role inside the IRA was to manage the CE investigations unit,[172] with the primary task being to identify British intelligence and security service informants operating within PIRA.[173] StakeKnife's value was enhanced by his ability to remove any threat to his access afforded by his position and alert the British intelligence and security services to the threats they were facing.[174] Stakeknife was also able to provide access to the most intimate secrets of PIRA personnel, which no doubt aided British intelligence and security services in recruiting other PIRA members

Saudi Arabia vs. Al-Qaeda

It appears that the Saudi Arabian security services operated much like the MI-5 activities launched against PIRA. CE TTPs worked on penetrating and deceiving Al-Qaeda. The Saudi government deceived the VSNA Al-Qaeda gave a new weapon to a Saudi

---

[171] Liam Clark, "Freddie Scappaticci Was Our Most Valuable Spy in the IRA during the Troubles: British Army Chief," *Belfast Telegraph* (April 20, 2012). Accessed April 8, 2017, http://www.belfasttelegraph.co.uk/news/northern-ireland/freddie-scappaticci-was-our-most-valuable-spy-in-ira-during-the-troubles-british-army-chief-28739868.html

[172] ibid.

[173] ibid.

[174] Mobley, *Terrorism and Counterintelligence.*

"double", who in turn compromised Al-Qaeda's sophisticated weapons development and next phase of operations. This ultimately led to a paranoid atmosphere within the Al-Qaeda ranks.

Hezbollah vs. Israel

Hezbollah's use of CI and CE operations married with established deception practices (camouflage, blinding, cover) directly challenged Israel politically, militarily, and diplomatically. Hezbollah showed great skill and integration of its intelligence, counterintelligence, and military units to match up its capabilities to Israel's military capabilities early on in the 2006 conflict. Whether or not the concept of hybrid warfare is accepted within the US military, the use of deception, double agent operations, married with VNSA's sophisticated strategy and high-tech weapons have proved to be a direct challenge to any military. The other dimension that needs to be fully evaluated is the use of Iranian military and intelligence units leading up to the 2006 conflict and how much intelligence was transferred to the Iranians from Hezbollah post 2006 conflict.

AQ Deceiving CIA and Using CIA to Kill AQ Selected Targets

The evidence provided through the review of literature makes it very clear that a VNSA did deceive two state professional intelligence services. If the transcripts of Balawi are to be believed, then Al Qaeda proved it could penetrate and deceive state intelligence services. One aspect of research that has yet to be explored is whether or not Balawi provided actionable intelligence to his Jordanian or CIA handlers while he was in Afghanistan or Pakistan. If so, this is important because it would reveal that Al Qaeda was willing to deliberately feed truthful sensitive information, infrastructure, and insights to the organization that would entice intelligence and security services targeting Al Qaeda. The intent of providing the CIA with this information would have been to increase the credibility

of Balawi. This would show that the Al Qaeda operations are not short-term, but rather more enduring and designed with specific objectives in mind. The other piece of analysis that is lacking is what information the CIA already knew before this case came along. This is extremely relevant when trying to detect deceptive information being passed to the CIA from Al Qaeda double agents. According to news reports, unnamed intelligence sources claimed that during Balawi's directed travel to Pakistan and Afghanistan, he provided "information that led to the drone-launched missile strikes."[175] If the Al Qaeda transcripts from Balawi are true, then was the information the US and Jordan acted upon genuine? As stated previously, Al-Qaeda deceived two professional intelligence services. If Balawi provided information on the drone strikes, should we now question which strikes were targeted and neutralized? The major lesson from the Balawi case is alarming for two reasons. First, the case received little to no vetting and the CIA did not appear to have been concerned that Al Qaeda was able to run this sophisticated of an operation. Secondly, Al Qaeda was able to deliberately launch an offensive CI operation, undermining the internal security practices of the Jordanian and American intelligence and security services. Al Qaeda had studied the playbook of the Jordanian security service and engaged in a deliberate offensive CI operation effectively feeding false information; that action was taken upon by the CIA, and neutralized CIA operations in that portion of Afghanistan.

Conclusion

The analysis of the test cases determined that CE operations are effective when initiated by a state or a non-state actor, and that when coupled with other techniques that can enhance a deceptive message, CE operations are very effective at enhancing the surprise

[175] Jim Maceda, Richard Engel and Robert Windrem, "Source: CIA Bomber's Intel Led to Successes," *NBC News.com*, (January 6, 2010). Accessed April 9, 2015, http://www.nbcnews.com/id/34705029/ns/world_news-south_and_central_asia/t/source-cia-bombers-intel-led-successes/#.WOwYlIgrLIU

and lethal capacity of the initiator, which was clear in all cases. Additionally, the analysis found that VNSAs employing CE operations in conjunction with a deception campaign should be the most worrisome to states. However, operational securities during the initial stages of the operation are crucial, because if detected by the target's intelligence or security service, it will gain ability to manipulate and turn the operation against you quite easily. Israel and IDF's history has shown that nation's ability to engage in multi-modes of warfare as well. Taking military strategy out of the analysis, the 2006 test case shows the effectiveness of CE operations launched to blind the target's intelligence service and render the leadership of the target service or entity without effective information to counter the action.

The second point of note is that VNSAs have the ability to run highly developed operations even against sophisticated state actors. State intelligence services have particularly had a history targeting the US for CE operations. When effective, these operations impose a cost on the actor being deceived; however, the deception is employed within the context of the information, which conceals who is actually is managing the asset feeding the information. In the case of Al-Qaeda, its operation was so valuable because Balawi's ability to penetrate both major security services showed the susceptibility the CIA had to double-agents, especially those who came with information of value to US national leadership. The Balawi case also was a blow to the morale and credibility of the CIA and Jordanian intelligence services, and enabled Al-Qaeda to enhance its own CI and CE programs through compromising these state actors. This also has become a template for other VNSA's on how to launch operations against sophisticated state intelligence and security services.

In closing, deception works. Both sides can be deceived. However, one of the most effective ways to provide indications and warning of attack is to have an asset on the inside. In addition, a common means of detecting deception is to launch a deception of your own.[176] CE is a valuable tool when countering an adversary deception operation, especially when the initiator of the deception recruits double agents with critical skills, and when the initiating service or entity enhances the credibility of the double agent through other modes of deception. [177][178] CE operations initiated internally or externally must meet areas of weakness, and to effectively engage a VNSA in deception, it is important to identify what the VNSA needs and what it is lacking. However, these operations take time and must be deliberate.

[176] Barton Whaley and Susan Stratton Aykroyd. *Turnabout and Deception: Crafting the Double-Cross and the Theory of Outs.* (Annapolis, MD: Naval Institute Press, 2016).
[177] Fischer, "Doubles Troubles"
[178] Masterman. *The Double-Cross System*

CHAPTER 3: EMPLOYMENT OF U.S. CONTROLLED TECHNOLOGY TRANSFER TO AIDE U.S. COST IMPOSITION STRATEGIES

"Any intelligent fool can make things bigger and more complex. It takes a touch of genius-and a lot of courage-to move in the opposite directions."
-Ernest Schumacher[179]

Research Question

Can the controlled release of US national security-based research and development assist in the implementation of cost imposition strategies against potential challengers?

Hypothesis

1 (A) SCIOs designed to support US cost imposition strategies levied against an adversary are a potential vehicle to impose costs. 1 (B) SCIOs designed to support US cost imposition strategies are effective only in the area of denial, no evidence exists in open source research to indicate its utility.

Introduction

This research explores the potential relationship between strategic counterintelligence and US cost imposition strategies, specifically looking at employing SCIOs as a way to deliver a cost to an adversary. The purpose would be to minimize the risk to US national security investments, simultaneously reducing the risk to illegal or clandestine technological transfer by providing the adversary through a controlled setting, eliciting a response that favorable to the US. Drawing on other academic research and historical cases shows that during the Cold War, the US utilized CE operations to deliver real but tampered equipment to the USSR's science and technology directorates'.[180] During the Cold War the US National Security Council (NSC) assumed that the KGB would somehow obtain access to its secrets through various human sources. NSC members relied on the KGB's skills and

[179] Ernst F. Schumacher, "Small is Beautiful," *The Radical Humanist*, 37 (August 1973). 22
[180] Sergei Kostin, Eric Raynaud, Catherine Cauvin-Higgins, and Richard V. Allen. *Farewell: the greatest spy story of the twentieth century* (Las Vegas: Amazon Crossing, 2011).

provided the KGB through double agents and controlled operations with material and data they required for Soviet economic means.[181] This operation serves as material proof and a template for future operations on how to manage countries like China, Russia, and Iran who engage in economic espionage activities, which aims to engage in illegal technology transfer.

The US is the most highly targeted nation in research and development (R&D), as its corporations maintain a technological edge in many areas. The US government develops the design and manufacturing of future capabilities that drive our economic interests' strategic capabilities, and in some cases impact the global economy. Preserving the edge and amplifying current and future US capabilities should be a major priority.

In the 1980s, the Soviet Union depended heavily on the theft of US defense technology and manufacturing secrets, and the Pentagon estimated that over 70% of all Soviet research and development were reliant on US technology and research.[182] Due to the KGB's exercising their capabilities within the US they had several other successes. The Soviets were able to clone the B-1B bomber aircraft and Airborne Warning and Control System.[183]

The DSS "2015 Targeting U.S. Technologies Report" provided a summary of the reporting and analysis of CDC reporting on suspicious events and attempts by foreign governments to gain access to US sensitive and classified technologies. To highlight the need for a strategic component of CI and explain why the foreign intelligence entities threat is strategic in nature, DSS provided a five year review of technologies that are highly sought after by entities in East Asia and the Pacific, which showed that for five years, entities in East Asia and the Pacific aggressively sought US technology in electronics, command and

---

[181] ibid
[182] Andrew, *Defend The Realm*.
[183] Christopher M. Andrew and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 2001). 218-223

control communications, software, aeronautical systems, and marine systems.[184] These technology areas cost $74.9 billion per year, according to the DoD's 2014 "Program Acquisition Cost By Weapon System",[185] and this figure excludes the $11.5 billion used for funding research and development programs, which are primarily executed by CDCs and US academic institutions.

When we discuss CI issues within the domestic framework, the focus is on law enforcement investigations that usually target a person engaging in illegal activity. However, CI practiced within the definition of a SCIO aims to reverse the illegal US technology transfer to state or non-state actors through commercial, clandestine, and cyber espionage. This a change from traditional neutralization approaches that US law enforcement chooses, like prosecution.

This chapter will show that SCIOs can also be useful in US cost-imposition strategies. The literature review is structured to examine the current US literature on cost-imposition strategy, Russia's reflexive control, and determine if any CE cases that would meet the definition put forth for SCIOs that prove the research conclusions. The importance and inclusion of reflexive control is to highlight the adversary thought in this area. The Russian perspective is designed to use SCIO-like activities to undermine US national security through messaging to a target and getting the target to act in a favorable way to the initiator. US SCIOs are worthy of exploration as the counter to reflexive control and serve as a means to deliver costs to an adversary like Russia.

[184] ibid.
[185] ibid.

Literature Review

"In Peace as well as War a carefully cultivated double agent system is the safest and surest weapon of counterespionage, and the most easily adaptable to changing conditions, changing problems, and even changing enemies."
-J.C. Masterman[186]

Thomas G. Mahnken wrote that "the competitive strategies approach focuses on the peacetime use of latent military power-that is, the development, acquisition, deployment, and exercising of forces-to shape a competitor's choices in ways that favor our objectives."[187] Mahnken proposed five concepts that can be applied to an actor the US desires to impose a cots upon. His particular focus was China, and managing their areas of growth that challenge the US's ability to project power. [188]

- First, the approach is employed against a strategic state actor that has its own objectives and ability to formulate its own strategy.
- Second, both actors have interactions between the competing establishments. Each actor makes limited decisions based on their competitor.
- Third, the competitive strategies approach acknowledges that the choices competitors have open to them are constrained. (limitations in capability and resources).
- Fourth, the competitive approach acknowledges that interactions may play out over the course of years or decades.
- Finally, the competitive strategies approach assumes sufficient under-standing of the competitor to be able to formulate and implement a long-

[186] Masterman, *Double-Cross System*.37
[187] Thomas G. Mahnken, "Cost-Imposing Strategies: A Brief Primer," (Washington, DC: Center for New American Security, November 2014).
[188] ibid.

> term…….Effective competitive strategies are predicated on an understanding of a competitor's decision making process and doctrine.

One form of competitive strategies is a cost-imposition strategy. Two contemporary researchers on cost imposition strategies are Colonel Kenneth Ekman, author of *Winning the Peace through Cost Imposition* and "Applying Cost Imposition Strategies Against China", and Dr. Thomas Mahnken, who published a primer ahead of his book titled *Competitive Strategies for the 21st Century: Theory, History, and Practice*. Both authors define cost imposition strategies as the deliberate programming, planning, budgeting, and equipping process of US military forces that will force the competitor to make trade-offs to balance against US military forces.

As defined by Ekman, "cost imposition strategies focus on eliciting an adversary response that creates a hardship differential favoring the initiating nation".[189] Mahnken, along with Bradford Lee's[190] research, seeks to convince an adversary that the costs of continued competition or conflict are prohibitively high and that accommodation is a more attractive option."[191]

Mahnken and Ekman both note that cost imposition strategies are not just American tools: other states apply them to the US as well. A close comparison in terms of eliciting your adversary's response is the Russian military application of reflexive control. Reflexive control is more focused on the application side of the actual conflict, but its operation involves a significant and detailed planning process.[192] Reflexive control seeks to impose a hard cost on the adversary by enticing the target to attack a particular way by using various

---

[189] Ekman, "Applying Cost Imposition Strategies against China." 26
[190] Mahnken, "Cost-Imposing Strategies: A Brief Primer."8
[191] Mahnken, "Cost-Imposing Strategies: A Brief Primer."8-9
[192] Timothy Thomas, "Russias Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* 17, no. 2 (2004): 237-56. Doi: 10.1080/13518040490450529. Snegovaya, Maria. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Russia Report 1, Institute for the Study of War. (Washington DC: Institute for the Study of War, 2015).

techniques relying on human intelligence and information operations.[193] When the target reacts, the initiator of reflexive control actually knows how the target will react, and the applier of reflexive control can inflict such damage to break the will of the target.[194]

Noting the use of such strategies among non-state actors, Mahnken particularly cites the examples of Al Qaeda and the effects of cyber-espionage. In Mahnken's view, when Al Qaeda implemented their attacks against the US in 2001, the group may have not calculated for the security costs associated with the attack and impact to the US security and transportation, in effect causing significant challenges for Al Qaeda exploiting the US transportation means for future attacks.[195] Cyber-espionage can be argued as one of the largest costs to the US government and economy, and with every breach and compromise comes at even greater cost. According to Mahnken, cyber-based attacks on government networks "that have triggered the development and deployment of increasing layers of security have yielded considerable costs, to include that of developing and fielding cyber security capabilities as well as the efficiency losses associated with such security measures."[196]

Cost-imposition strategies first surfaced in the 1970s within the US government, specifically the Department of Defense (DoD).[197] The US was facing budget shortfalls, domestic economic challenges, and the persistent threat of a capable communist competitor. An example of the cost imposition strategy the US pursued, as identified by Ekman and Mahnken, is the research, development, and fielding of the US Air Force's stealth fighter and bomber programs. With the release of these aircraft, the Soviets would be forced to

---

[193] ibid
[194] Ionita, Craisor Constantin. "Potential National Measures To Counter Hybrid Warfare." *Romanian Military Thinking*, February 2015, 17-27.
[195] Mahnken, Thomas G. *Competitive strategies for the 21st century: theory, history, and practice*. Stanford, CA: Stanford Security Studies, 2012.
[196] ibid.
[197] Ekman, "Applying Cost Imposition Strategies against China"; Mahnken, "Cost-Imposing Strategies: A Brief Primer"

develop a whole new set of countermeasures to defend their airspace, harden strategic targets, and expend clandestine intelligence sources who would attempt to collect information on the secretive programs that would benefit Soviet weapon and countermeasure programs. The use of cost-imposition strategies dates back to "Athens and Sparta in the third century."[198] It is a state option that was formulated within an overall strategy.

Cost-imposition within the US security context focuses primarily on fiscal, security and political realities. Ekman and Mahnken's research reveals that cost imposition is a deliberate strategy that works best as a preliminary defense framework, rather than during times of active conflict, and that it is based on fiscal realities, meaning that a government must have the resources to invest in developing the programs designed to trigger the adversary countermeasures.[199] These US defense investments will elicit a response from the adversary. One of the main principals' areas where SCIO's can be married up with is in the area of Denial, which is one of the principal elements of cost imposition, "denial, cost-imposition, attacking the enemy's strategy, and attacking the enemy's political system."[200]

The desired objective of this employment strategy is to deter one's adversary from initiating attacks. In short, a denial operation looks to "make it hard for the adversary to translate its operational means into political ends that it desires."[201] It may involve transforming defense investments into new technologies that would force an adversary to either organically research and develop a countermeasure or steal it. The denial operation

[198] ibid.
[199] Ekman, "Applying Cost Imposition Strategies against China", Mahnken, "Cost-Imposing Strategies: A Brief Primer"
[200] Lee, "Strategic Interaction: Theory and History for Practitioners."
[201] ibid, 32

may be focused on containing one's adversaries' abilities to organically research and develop a technology, or preventing the theft of that technology elsewhere.

The other portion of the strategy is "attacking the enemy's strategy", which incorporates two modes of operation: reactive and proactive, both of which serve the purpose of manipulating the interaction with one's adversary, forcing it to destabilize its strategy on its own through the modes of operation employed by the initiator.[202] As defined by Bradford Lee, proactive approaches involve "inducing strategically self-defeating behavior on the enemy side is on those non-Western enemies of the United States use more readily than leaders who emerge from American strategic culture and educational institutions."[203] In other words, through its interaction with the adversary, the initiator attempts to get the target to engage in some type of self-defeating behavior.

From a national security perspective, the United States is failing to recognize that it is entering an era of total warfare because it continues to view targets with conventional lenses. In other words, it has been fighting on a 1950s model against state actors such as Russia, China, and Iran. The current situation is that the United States is also facing violent non-state actors that are used as proxies, which assists state actors in skirting internationally, accepted laws or norms.

CE Operations Imposing Costs on Initiators

During the Cold War, several cases highlighted the use of coordinated double-cross-like system operations that influenced the target to recruit potential sources of information, engage in national decisions leading to false investments, and paint a picture of the operation initiator that was not advantageous to the target of the operation.

[202] ibid, 37
[203] ibid, 37

The Farewell Operation is probably one of the most daring and innovative CE operations in history. "Farewell", a Soviet engineer also known as Col. Vladimir I. Vetrov, was working within KGB's Directorate T,[204] which was responsible for the supervision and evaluation of technical intelligence collected by Line X,[205] the clandestine collection program set up "to obtain technical and scientific knowledge from the West."[206]

Vetrov offered his services to the DST, the French security service, which mainly specialized in counterintelligence rather than foreign intelligence.[207] Some researchers have assessed that Vetrov chose the DST because he was concerned for his safety and he had intimate knowledge of penetrations within western intelligence services.[208] The KGB and the Soviet Union did not really consider France an enemy, as the country had recently elected a socialist prime minister.[209] Vetrov ultimately found that a counterintelligence service was much more difficult to penetrate than anticipated.[210]

Unbeknownst to the DST and "Farewell", President Ronald Reagan, who had taken office only a year earlier, and his national security team strongly aspired to win the Cold War. Reagan and his staff did not believe the Soviet economic system was working as efficiently as the Soviets thought, and they were right. Coming into the Reagan administration, were several national security advisors focused on exerting "economic pressure" on the Soviet system.[211] The policy based on that hypothesis was to develop a strategy to "take advantage

---

[204] Sergei Kostin and Eric Raynaud, *Farewell: The Greatest Spy Story of the Twentieth Century*, trans. Catherine Cauvin-Higgins (Las Vegas: Amazon Crossing, 2011)
[205] Gus W. Weiss, "The Farewell Dossier: Duping the Soviets," *Studies in Intelligence* (CIA, 1986).
[206] ibid.
[207] Kostin and Raynaud, *Farewell: The Greatest Spy Story of the Twentieth Century*.
[208] ibid.
[209] ibid.
[210] ibid.
[211] Weiss, "The Farewell Dossier: Duping the Soviets."

of the USSR's low productivity, its lag in technology, oppressive defense burden, and inefficient economic structure."[212]

In late 1981, Dr. Gus W. Weiss, who served as Special Assistant to the Defense and as the Director of International Economics for the National Security Council, was briefed about the Farewell case. Dr. Weiss carried on some research that began under the Carter administration, the purpose of which was to assess the Soviets' interest in acquiring US technologies illegally.[213] The briefing or Farewell couldn't have come at a better time. French President Mitterand briefed President Ronald Reagan on a source of information that was placed within the KGB's Line T, who evaluated the intelligence gathered from Line X. This source of information provided volumes of data, which detailed gaps in Soviet technological knowledge and capability, identified more than 200 Line X KGB officers and 100 leads to recruited KGB sources, and demonstrated how a large majority of Soviet R&D relied on the West.[214] "Farewell" had confirmed the suspicions of many on the National Security Council that Soviet R&D and its national defense was benefiting from illegal technology transfer through Line X officers' clandestine collection program.[215] The primary areas of Line X intelligence collection were in the areas of "radar, computers, machine tools, and semiconductors."[216] The assessment was that Line X was asked to collect certain information on key technologies and had "fulfilled two-thirds to three-fourths of its collection requirements."[217] The conclusion of the assessment was that through the French DST, the CIA now had the "shopping list of still-needed technology, and with the list American intelligence might be able to control for its purposes at least part of Line X's

[212] ibid.
[213] ibid.
[214] ibid.; Kostin and Raynaud, Farewell: The Greatest Spy Story of the Twentieth Century.
[215] Weiss, "The Farewell Dossier: Duping the Soviets."
[216] ibid.
[217] ibid.

collection, that is, turn the tables on the KGB and conduct economic warfare of our own."[218]

Weiss's new playbook utilized the analysis of the Farewell material "to feed or play back the products sought by Line X",[219] but instead of KGB sources, it would come from US human sources (doubles), providing Line X with "improved" designs of technologies they still needed. The technologies would be genuine, pass inspection, and when integrated into Soviet R&D, the article would fail. Based on the dynamics and behaviors at the time, the risk of compromise existed. However, Weiss felt that "if some double agent told the KGB the Americans were alert to Line X and were interfering with their collection by subverting, if not sabotaging, the effort I believed the United States could not lose." Due to their extreme paranoia, it was assessed that the KGB would more than likely "reject everything Line X collected."[220] The conclusion: it would be a win for the US and a significant loss for the USSR, posing a significant cost to the latter.

The CIA, Department of Defense, and FBI set up a task force to do what was theorized. They evaluated foreign companies, licenses, and people, and introduced the improved products, designs, and material to Line X sources through doubles. The result of this operation severely impacted the USSR, as "contrived computer chips found their way into Soviet military equipment, flawed turbines were installed on a gas pipeline, and defective plans affected the output of chemical plants."[221] The DOD planted misleading information on "stealth aircraft, space defense, and tactical aircraft."[222] Upon the decision of the closing down of the operations the USIC was not selfish, they accordingly alerted their allies, who

---

[218] ibid.
[219] ibid.
[220] ibid.
[221] ibid.
[222] Peter Schweizer, *Victory: The Reagan Administration's Secret Strategy that Hastened the Collapse of the Soviet Union* (New York: Atlantic Monthly Press 1995)

expelled over 200 Line X collection officers globally, leading to the collapse of the clandestine collection program.[223]

Analysis of SCIO's, Cost Imposition, and the Effect on the Target

"*Why not help the Soviets with their shopping? Now that we know what they want, we can help them get it.*"[224] – Gus Weiss

Having the knowledge of a country's shopping list of technologies needed to become more economically competitive in today's global market place would be any secret worth protecting, buying, and exploiting to any country. Some factors that were critical to the success of this operation include:

- The Soviet's technological areas of weakness were the US's strengths, namely computers and microelectronics, an area in which, according to the former science and technology chief Roald Sagdeev, the USSR trailed the US by 15 years before the initiation of the CE activity feeding the Soviets technology through controlled operations.[225]
- The target of the SCIO primarily relied on its foreign intelligence and security service to illegally acquire US technologies that ranged from unclassified to top-secret materials.[226] They utilized tradecraft associated with a foreign intelligence and security service operating within the US. Through the initiation of a few US based CE activities; the US was able to exploit the KGB's Line X clandestine network.[227]

---

223 Weiss, "The Farewell Dossier."
224 Thomas C. Reed and George Bush, At the Abyss: An Insiders History of the Cold War (New York: Presidio Press/Ballantine Books, 2004), 267-268.
225 Weiss, "The Farewell Dossier."
226 William Safire, "The Farewell Dossier," The New York Times (February 01, 2004). Accessed January 24, 2016, http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?mcubz=3.
227 Weiss, "The Farewell Dossier."

- Just one CE operation ran off of information provided by Farewell, which allowed the KGB to steal software from a Canadian company that had a Trojan horse embedded in the code, and would cost the Soviets over 8 billion a year in 1980 dollars.[228]
- Over 70% of Soviet defense research was derived from the illegal technology transfer from US defense contractors to the Soviets through Line X operations.[229]

Conclusion

SCIOs are highly effective at imposing a cost against the targeted adversary. This was proven and demonstrated by numerous Cuban, East German, and Russian operations launched at the United States. However, the most compelling case for SCIOs is demonstrated by the review of "Operation Farewell", a program that proved to be extremely costly to the Russians politically, economically, and affecting their defense investments. Farewell's revelations "exposed the abject failure of the Communist system to match rapid Western advances in electronic micro-technology."[230] As described in previous research, a task force was set up within the US to take advantage of this strategic technological weakness, and a large and complex US CE operation was initiated to continue to allow the illegal acquisitions by Line X officers to collect "advanced" and "manipulated" technology.[231] This, in turn, led to the collapse of the Soviets' clandestine technology collection program. In short, the United States' ability to both engage and implement cost imposition strategies in denial operations and attack its adversaries strategically acted as a catalyst, leading to the collapse of the Soviet economic and defense structure. The "Farewell" revelations helped

---

228 Safire, "The Farewell Dossier."
229 Andrew and Mitrokhin. *The sword and the shield*
230 John Lichfield, "How the Cold War Was Wom…By the French," *The Independent* (September 16, 2009). Accessed April 11, 2016, http://www.independent.co.uk/news/world/politics/how-the-cold-war-was-won-by-the-french-1788720.html
231 Weiss, "The Farewell Dossier"; Lichfield, "How the Cold War Was Wom…By the French."

to point out critical gaps in the main adversary's capabilities. This research also provided a strong argument for Mahnken and Ekman cost imposition strategies, especially when the adversaries we face today practice a form of reflexive control. In terms of a potential US strategy, cost imposition is the US's answer to counter reflexive control, and SCIO's are the delivery mechanism to message to the adversary through the use of specially packaged information or material to entice the adversary to make a move that is advantageous to the US. Taking advantage of an adversary's weakness is a key element in warfare.

To fully evaluate if the hypothesis stands true, however, further research needs to be conducted to determine whether or not a US SCIO-like system can survive in today's ever-evolving security environment. Namely, can a double-cross like system survive today in a cyber environment that appears to be a major challenge to the US, particularly considering the manner it is intertwined with the civilian communication structure?

CHAPTER 4: IS THE DOUBLE-CROSS SYSTEM WITHIN THE A VIABLE COST IMPOSTION STRATEGY COUNTERING CYBER ESPIONAGE?

"*Pretend inferiority and encourage his arrogance"*[232]

-Sun Tzu

Question: Are SCIOs possible in cyber-space, and is it technically feasible to reverse computer network exploitations (CNE)? Are SCIOs a viable option to increasing the cost and risk of states, organizations, and groups who attempt to exploit stolen US Government data? Can this be achieved with existing capabilities and techniques?

Hypothesis: A cyber SCIO using a contemporary network environment would be no different from what the British employed during World War II. The computer and network are the new wireless radio set and selected transmission system for already recruited double agents or agents waiting for adversarial recruitment and employment. SCIOs are a viable option to increasing the costs and risk of states, organizations, and groups who exploit US government data. They are technically feasible based on tested and approved research. Historical research leads to a conclusion that SCIOs in cyberspace, integrated with physical agents, will effectively increase the believability of the data provided from both channels of clandestine communication, thus providing opportunities to elicit a response favorable to the initiator. However, the scalability and capacity to conduct large-scale SCIOs cannot be fully evaluated at this time.

[232] (Tzu)

Introduction to Focus

The true cost of cyberespionage remains elusive-costs measured in terms of economic deprivation and loss of technical military dominance-although it is clear that the transfer of cutting edge military technology to America's adversaries endangers the lives of U.S. military personal and strengthens the resolve of those nations who wish to thwart American political objectives.[233]

The focus of this chapter is to evaluate the effectiveness of conducting SCIOs in cyberspace and to determine if this is technically possible, or if the attack might be reversed upon the initiator. The objective of SCIOs launched through a cyber environment is to protect US national security infrastructure, data and information. Based on a current review of US cyber security policy, current cyber security practices place focus on defense in depth practices with a mixture of software designed to detect malicious incoming activity, monitoring of outbound network traffic looking for anomalous messages, locking down of permissions of the user, and education of the users.[234]

Current cyber security strategies do not involve the use of honeypots or decoy networks, and reversing a cyber-attackers operation against the attacker is not a common protection practice within the United States or within the department of defense. There is no global enforcement body that targets and punishes countries, companies, and cyber actors for theft of intellectual property rights, stealing foreign government research and development, or employing malware to disrupt informational environments. Yet even having such an entity in place would not address the fundamental problem. The fundamental problem with the internet is that it was founded to support individuals access to information without any

---

[233] Office of the National Counterintelligence Executive (ONCIX), "Foreign Spies: Stealing U.S. Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011" (Washington, DC, October 1, 2011). Accessed April 11, 2015, https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[234] Nicole Keller,. "Cybersecurity Framework." *NIST* (August 01, 2017). Accessed August 04, 2017, https://www.nist.gov/cyberframework.

thought of security integrated into its development. It is unknown whether a global appetite exists to develop a new cyber infrastructure and not likely to be discussed in the near future. The only way to begin to form a solution for nefarious cyber actors is to manage the cyber actor. In doing so, we must raise the costs upon our adversaries.

John Reed has observed that "Denial and Deception is key to changing the way we look at these things, being proactive on the network, not in an offensive, aggressive way", but by creating capabilities that "make things more difficult for the adversaries" by giving them bad information and quickly identifying the attackers."[235] Engaging in offensive counterintelligence or CE operations in cyberspace appears to be a large part of the solution to managing the cyber actor and driving the cost up for adversaries and competitor. A private consulting company has suggested that businesses in the commercial environment have employed these techniques already.[236] As a representative of that company informed the magazine *Foreign Policy,* they are employing cyber deception techniques that are used to poison the data that attacker's exfiltrate from the network. The company was specifically engaged in using CE practices within the cyber realm to identify competitors, with the aim of allowing the cyber actor to "compromise" the network and steal data the company wanted the attacker to steal. The defensive practice is identifying a network compromise, studying the attacker, evaluating the data taken, and then inserting material that would include various malicious exploits of the company's own.[237]

---

[235] John Reed, "DOD Says Don't Worry about Hackers Accessing Key U.S. Weapons Designs," *Foreign Policy* (May 28, 2013). Accessed April 10, 2015, http://foreignpolicy.com/2013/05/28/dod-says-dont-worry-about-hackers-accessing-key-u-s-weapons-designs/

[236] "REQUEST DEMO BLOG CAREERS COMPANY CONTACT INDUSTRIES NEWS & EVENTS PARTNERS RESOURCES Skip links Skip to content Skip to footer TRAPX SECURITY WINS CYBER DEFENSE MAGAZINE AWARD 2017," Trapx.com, February 13, 2016, , accessed March 10, 2017, https://trapx.com/trapx-security-wins-cyber-defense-magazine-award-2017/.

[237] John Reed, "DOD Says Don't Worry about Hackers Accessing Key U.S. Weapons Designs," *Foreign Policy* (May 28, 2013). Accessed April 10, 2015, http://foreignpolicy.com/2013/05/28/dod-says-dont-worry-about-hackers-accessing-key-u-s-weapons-designs/

In Chapter 3, research concluded that adversary CE operations initiated by Cuba, East Germany, and Russia devastated the credibility of the CIA and US national security. US intelligence operations aimed at stealing foreign governments secrets came at a cost, especially when the US found out that a majority of the sources in Cuba, East Germany, and in Russia were CE operations initiated by the respective security services. The operations blinded the USIC from what was actually happening within the respective countries. In other words, US adversaries controlled clandestine channels of communication, effectively creating desirable outcomes for their operations.

Through the passage of false information to US intelligence officers, foreign intelligence analysts shaped the view of American leaders. For a period of time, the US believed that the USSR's military capabilities were far more powerful than they really were. The late Barton Whaley was asked about whether it was possible to resurrect a double-cross like system and his assessment identified two conditions and scenarios under which this could occur: through "(a) complete control over any single channel of communication; and (b) confidence in at least one feedback channel from the enemy that the system is working unsuspected."[238] Networks with servers and personal computers owned by the defender can manage the information coming in and going out. Using an assortment of cyber techniques that are common in physical practice within CE operations can create multiple feedback loops to determine who has stolen the data, where the stolen data has gone, the infrastructure set up to hide the stolen data, and depending on the tools used, tell the defender who is benefitting from the stolen information.

To put things in context, evidence that was collected when the famed KGB archivist Vasili Nikitich Mitrokhin defected to the United Kingdom in 1992 uncovered this startling

[238] Whaley and Aykroyd. *Turnabout and Deception*

discovery about the external source of much Soviet science and technology: "the Soviets estimate that by using documentation on the US F-18 fighter their aviation and radar industries saved five years of development time and 35 million roubles".[239] The cost equivalent in 1980 dollars is $55 million.[240]

Introduction to the Cyber Security Environment (Shaping)

Cyberspace, cyber security, and hacking are terms with which we have all become familiar. They are a key challenge for the US, particularly due to the strong dependence on cyberspace and the global reliance on the Internet.

To define the context of cyberspace for the purpose of this research, the following definition by Singer and Friedman was chosen: "cyberspace is first and foremost an informational environment, made up of digitized data that is created, stored, and most importantly, shared."[241] This definition is important because "cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow." [242] Essentially, cyberspace encompasses the global communications domain, which includes fiber optics, open/closed computer networks, cellular, various space-based communications, and the Internet.

Four common themes have emerged in research and have been validated by many other researchers.[243] First, hackers will always find a way to exploit new software and hardware. [244] Second, a basic malware exists and variants are created off that baseline.[245]

---

[239] Andrew and Mitrokhin. *The sword and the shield.*
[240] ibid.
[241] Singer and Friedman, *Cybersecurity and Cyberwar, What Everyone Needs to Know.*
[242] ibid.
[243] Shlomi Boutnaru, "The Four Horsemen of the Cyber Apocalypse," *TechCrunch* (January 10, 2015). Accessed February 28 2017, https://techcrunch.com/2015/01/10/the-four-horsemen-of-the-cyber-apocalypse/.
[244] ibid.
[245] ibid.

Third, this cyber threat is persistent and little investment can yield large returns.[246] Fourth, human error is inevitable.[247] The conditions for a double-cross or reversal of a cyber-attack operation must involve three phases:

- Deception; you have to invent or design a new network, or build off an existing network, with the purposes of luring and enticing a cyber actor intending on doing something malicious to visit and follow through.[248][249]
- Detection; the indication of a CNE activity occurring or attempt to deceive the network sensor or individual receiving emails with malicious attachments.[250][251]
- Reversal/double-cross; once the identification of the attack and tools used to perform the exfiltration of the data, the defender designs tailored tools to reverse the operation to playback the prepared material to entice the tasking element of the attacker to increase the frequency and steer the intruder's attacks.[252]

How Cyber-Attackers Attack

Cyber attackers have a cycle of operations, which are deliberate activities that require deep analysis when attempting to reverse them upon the attacker, and there are potential indications and warnings of an actor preparing to conduct an operation against a network. This is crucial because SCIO's success depends on ensuring that the attacker's confidence is

[246] ibid.
[247] ibid.
[248] Whaley, Barton and Susan Stratton Akroyd, *Textbook of Political-Mlitary Counterdeception: Basic Principles and Methods* (Washington, D.C.: National Defense Intelligence College, 2007); Whaley and Akroyd, *Turnabout and Deception*.
[249] Rid, Thomas. *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).
[250] Trend Micro, "Combating Advanced Persistent Threats (APT), Accessed January 21, 2017, http://www.trendmicro.com.au/au/enterprise/challenges/advance-targeted-attacks/index.html#understand-an-attack.
[251] Whaley and Aykroyd, *Textbook of Political-Military Counterdeception*, 43-90.
[252] ibid.; Whaley and Akroyd, *Turnabout and Deception*.

not shaken by any alarms sounded upon the initiation of the operation. Everything must look like a typical attack the attacker has performed flawlessly without alarm before.

Singer and Friedman have defined an advanced persistent threat (APT) as "a cyber-attack campaign with specific, targeted objectives, conducted by a coordinated team of specialized experts, combining organization, intelligence, complexity, and patience."[253] The APT attack sequence is as follows:

Figure 2. The APT Cycle of Operations [254]

Step 1. Intelligence Gathering- The APT is given its assignment, which is initiated by identifying and researching potential targets who have a connection to the assignment. Based on the research, the APT develops a target package, which includes a target history, Facebook information, and other connection information. Based on this information, the ATP develops a customized or tailored attack.

[253] Singer and Friedman, *Cybersecurity and Cyberwar, What Everyone Needs to Know.*
[254] Kyle Wilhoit, "Incubation, Its Not All about Chickens" (Louisville, KY, Derbycon).

Step 2. Point of Entry: "The initial compromise is typically from a zero-day malware delivered via social engineering (email/instant messenger or downloadable file). A backdoor is created and the network can now be infiltrated."[255]

Step 3. Establishing Command Control and Communication: This is the act of directing the malware that was employed against the network to then compromise specific servers, personal computers, and applications for the purpose of exfiltrating the data of interest.

Step 4. Lateral Movement: "Once inside the network, attacker's compromise additional machines to harvest individual user network credentials, escalate privilege levels within one's network, unbeknownst to system administrators, and maintain control of one's network. "[256]

Step 5. Asset/Data Discovery: "Several techniques exist that are used to identify the noteworthy servers and the services that house the data of interest."

Step 6. Data Exfiltration: "Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed and often encrypted for transmission to external locations under attacker's control." [257]

In most cases, the APT's goal is to gain access to the targeted network without being detected, stay inside the network, exfiltrate undetected information, identify exploitable information about the network, and integrate the APT into the network command and control infrastructure. In simple terms, they don't want the target to know they are inside

[255] See Trend Micro Corporation's works: "Only a Custom Defense Effectively Combats Advanced Persistent Threats. Accessed February 17, 2016, http://www.trendmicro.com/us/enterprise/challenges/advancetargeted-attacks/index.html#understand-an-attack; and "Combating Advanced Persistent Threats," Accessed April 1, 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/tag/internet-of-things/
[256] ibid.
[257] ibid.

the network. The goal is to be unnoticed by network sensors, anti-virus programs, network defenders, and become part of the normal profile. The only way to begin to form a solution is to manage the cyber actor and raise the costs upon our adversaries. Engaging in offensive counterintelligence operations in cyberspace appears to be a large part of the solution to managing the cyber actor and raising the costs of intrusion for adversaries and competitors.

Literature Review

DCS in WW2, Wireless Radio Set

"The breaking of the Enigma, the German cipher machine, was the most importance intelligence triumph of this or any other war."[258]

In Ben Macintyre's "*Double Cross*", readers learn how British intelligence broke the mathematical code to the Enigma. The Enigma was the Germans' method of encryption, aimed at protecting their method of communications with their enemy agents operating in England, Europe, and Africa; as well as the encryption method of the German foreign embassies. With the ability to read the Germans' communications, the UK gained an invaluable tool because it became possible to identify Abwehr agents operating on British soil. MI-5, specifically the B-1A division CE quickly moved in to turn these agents to support the larger military objectives. As Masterman outlined in his study, which can be considered the source document for the double-cross, MI-5 and MI-6 then had three major elements to mount a successful deception: the ability to read the Germans' secret communications; control of the secret communication operators and handsets; and knowledge of German global espionage operations. The result was, as MacIntyre describes, that "the misinformation that the first compromised agent sent back to his handler was tracked through the Abwehr network and provided the key for the decryption of their

[258] Ben Macintyre, *Double Cross: The True Story of the D-Day Spies* (London: Bloomsbury, 2012)

modified cyber."[259] This ripple effect meant that "once the codes were cracked, MI-5 knew all of the operational agents within Great Britain and could uncover what the Abwehr did and did not know about the Allied war effort."[260] Manipulation of the wireless radio transmitter as a medium to pass true information and misinformation proved to be extremely effective, and the result was the success of D-Day.

Contemporary Literature on Offensive and Defensive Cyber Counterintelligence

Cyber anything is relatively a new topic and not able to be neatly organized. Offensive cyber counterintelligence (OCCI) can be defined as "interactions with the adversary to directly collect information about their intelligence collection operations or to deceive them."[261] The offensive action can be done from within a network or externally. CCI would employ all the traditional CE techniques. For example, "an Offensive CCI operation could be run to identify or mitigate adversaries already in your network" or "help create a honeypot inside your network to identify malicious actors on the network."[262] Defensive cyber counterintelligence (DCCI) is described as those "actions taken to identify and counter adversary intrusions before they occur as well as the efforts in identifying and minimizing the threat landscape."[263] The analysis is usually intertwined with all source intelligence that evaluates the network internally, looking for gaps and weaknesses that intruders can exploit, and working to bolster its defenses.[264]

---

[259] ibid.
[260] Adamya Sharma, "A Game of Human Chess: The Double Cross System and MI-5's Supremacy in World War II (Undergraduate Honors Thesis, University of Colorado Boulder, 2015). 32
[261] Tripwire Guest Authors, "Cyber Counterintelligence: From Theory to Practice." *Tripwire* (May 4, 2014). Accessed August 04, 2017. https://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/.
[262] ibid.
[263] ibid.
[264] ibid.

Through its analysis of the threat, DCCI determines the adversary's likely information interests when the network is compromised, and the server (honeypot) storing the documents is configured with tracking tools embedded with malicious code that is not easily detectable, as well as providing bait information that leaves the intruder desiring more.[265] Deception in cyberspace enters the discussion with the use of "fake or incorrect data," with the thought process being that "the adversary would retrieve files with the fake information, possibly corporate intellectual property such as a secret recipe, believing it to be real."[266] One challenge that accompanies with this concept is that "organizations struggle to effectively perform proper architecture and maintenance of their systems as well as the proper acquisition and use of traditional defense systems let alone the establishment of advanced systems."[267] The other challenge is that a target of the cyber threat would have to agree to sacrifice some material of value to the target.

Roles in Deception, Counter-deception, and Attribution in Cyberspace

"Confusing and fooling the enemy has allowed many and under-manned and out-gunned commander to win a decisive victory or an asymmetric force to win at a lower cost and risk."[268]

This section outlines the roles in cyberspace that are crucial to framing the problem, the phases, and levels of deception an actor must achieve to effectively launch SCIOs through this medium. In "A Tricky Situation: Deception in Cyberspace", Neil MacEwan focused on the art of deception employed against the weakest link in the computer security chain: the network user, citing several examples with nexuses to US based criminal activities and internationally-based activities. The primary tactic of these criminal actors is the employment of sophisticated social engineering scenarios. MacEwan described social

265 Wilhoit, "Incubation, It's Not All About Chickens"
266 Tripwire Guest Authors, "Cyber Counterintelligence"
267 ibid
268 Martin, "Military Deception Reconsidered."

engineering as "the latch lifting in trickery", and once the latch to the gate is lifted, the sky is the limit.[269] He concluded that deception employed against a person is a primary component, upon which the development of more sophisticated social engineering scenarios will increase, and one can assume that after the fact, more people will assist in "lifting the latch".[270]

"Deception on behalf of the cyber attacker" is little different than a case officer approaching a target posing as someone else, better known as a false flag. What has been seen is that the tactics, techniques, and procedures are essentially the same in both criminal and nation or state-sponsored cyberattack activities. Attribution is extremely difficult, as attackers enjoy their anonymity and employ deceptive techniques designed to keep the defenders continually guessing.[271]

"Counter-deception on behalf of the defender" is much like a security service officer waiting for indications from a technical or human intelligence source that a penetration exists. However, the defender has to deceive the human asset assisting with cyber targeting, if applicable, and determine if other vulnerabilities exist. The defender must gain deep knowledge of the intruder: who they really are, what they want, when they will attack, where will they likely attack, why they are attacking, and how the defender can alter or reverse the attack to the benefit of the home network.

"Attribution" has three goals in cyber defense. First is the tactical goal to determine how the attacker compromised the network and what they wanted. Second is the strategic goal that focuses on identifying the attacker and its goals, and finally there is the aspect of

---

[269] Neil MacEwan, "A Tricky Situation: Deception in Cyberspace," *The Journal of Criminal Law*, 77 (October 1, 2013).
[270] ibid.
[271] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1/2 (2014)

communicating the results of the investigation.[272] In 1981, the US intelligence community was able to achieve attribution in cyberspace when it learned that the KGB was illegally acquiring various US technologies that could aid Soviet commercial and industrial areas of business (economic espionage). The US tampered with software that would control the regulation of natural gas flowing through a pipeline and allowed the KGB to steal the software, which had a Trojan horse embedded. Attribution came in the form of a 3-kiloton explosion inside Russia that destabilized the Soviet's ambition to be a principal provider of natural gas to Eastern and Central Europe.[273]

Deceptive Concepts of Operation in Cyberspace-Incubation/Illumination Operations

Contemporary deception technologies designed to deceive the APT into believing it has compromised its target is essential to the tactical success of SCIOs. Incubation and illumination operations have been demonstrated to reverse the APT's CNE and allow the defender to insert specially prepared data to impose a cost upon the attacker and illuminate their path of exfiltration, which leads to increasing the success of attribution. The uniqueness of this concept is that it also allows the defender to analyze the attacker's tools within a controlled environment, facilitating the exploitation of the tool's signatures to improve existing network sensors.

As Kyle Wilhoit explained, "malware incubators allow a researcher to execute malware in what appears to an attacker to be their targeted environment."[274] In other words, if a network's intrusion detection system is able to steer an attacker into an environment that mimics the intended target environment, it is a success. The incubators can mimic these

[272] Rid, *Cyber War Will Not Take Place*.
[273] Whaley and Aykroyd, *Turnabout and deception*.
[274] Kyle Wilhoit, "Incubation, It's Not All About Chickens." Louisville, KY: Derbycon, 2014.

characteristics of the network: whatever scaled network environment, host naming conventions, operating systems and system vulnerabilities are based on the software out at the time; other private network connections; and the installment of decoy documents.[275] Decoy documents are designed to entice the cyber actor to extract them from the network, and can be embedded with beacons, malware, and other additional tools designed to exploit the path of extraction.[276] The lifecycle of incubation reveals a series of stages:

- Preparation: occurs when the first signs of malware are introduced into the network, application, or mimicked cyber environment. Identifies the target of the malware (operating system, documents, data, and specific information) and additional details about who is behind the attack.
- Incubation: this is the phase where things get "warmed up" and the manipulated information is prepared for identification by the attacker and then packaged for exfiltration. It also allows for full forensic review of the malware, which can aid in creating other opportunities for global detection of the same actor elsewhere.
- Illumination: a phase that helps assess the damage of the attacker, potentially identifying the motivation and intended customer of the exfiltrated data.
- Verification: the difference between the concept of operations development and this notion is that the development of "incubation" during the verification phase goes offensive to "poke" attackers with salted documents that are designed to hatch inside the attacker's network.[277]

---

[275] ibid.
[276] Brian M. Bowen, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. "Baiting Inside Attackers using Decoy Documents," in *Security and Privacy in Communication Networks*, SecureComm 2009. edited by Yan Chen, Tassos D. Dimitriou and Jianying Zhou J. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 19. (Berlin: Springer, 2008), 51-70.
[277] Kyle Wilhoit, "T318 Chicken of the APT Understanding Targeted Attackers with Incubation" (presentation, Derbycon 4, 2014). Accessed April 9, 2017, https://archive.org/details/derbycon4.

Kyle Wilhoit initially began to demonstrate the concept of incubation by building a network environment that mimicked a utility company, replicating the network of a municipal water system by using specialized software and real industrial controllers. From the internet, it looked like a water plant in Ashburn, VA. [278] The results were eye opening. Within a couple of weeks, the attacker "stole passwords, engineering PDFs and data that would let them back into the computers through a remote access system for employees",[279] so that they could return at any time and access the network. This concept will work in the US's favor because the United States is so highly sought after by cyber adversaries/competitors, particularly when it comes to theft of technology research and development information.

In 2014, Threat Stream, a subsidiary company of Google, conducted a study with another "decoy" system that was designed to look like another "industrial control computer" and entice hackers in an effort to determine what country was the most heavily targeted by cyber actors. The study replicated the decoy network to make it appear that it was located in U.K., U.S., Amsterdam, Tokyo, Brazil, and Singapore".[280] "Over a three-month period, the US was by far the biggest source of attack traffic (more than 6000 attacks), followed by China (more than 3500), Russia (more than 2500), the Netherlands and France."[281]

---

[278] Michael Riley and Jordan Robertson, "Ugly Gorilla Hack of the U.S. Utility Exposes Cyberwar Threat," *Bloomberg* (June 23, 2014). Accessed April 10, 2015, https://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat

[279] ibid.

[280] Jordan Robertson, "A Decoy Computer Was Set Up Online," *Bloomberg* (September 23, 2014). Accessed January 10, 2016, https://www.bloomberg.com/news/2014-09-23/a-decoy-computer-was-set-up-online-see-which-countries-attacked-it-the-most.html.

[281] ibid.

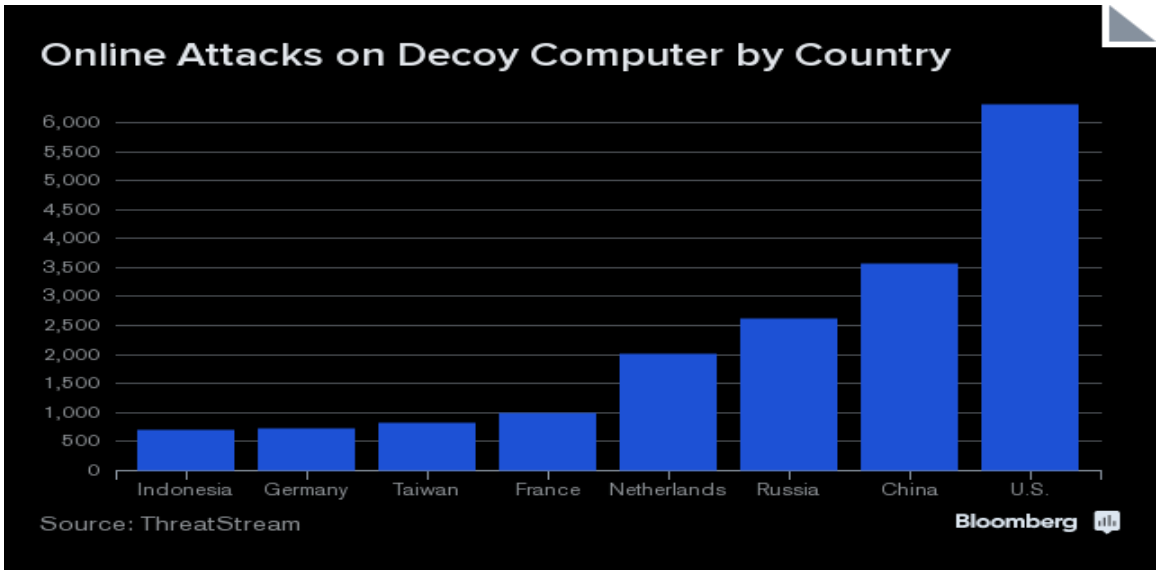

Figure 3. Country-based Count of Online Attacks on Decoy Computers [282]

The current US defense strategy is to build resilience in its current systems and employ an in-depth defense strategy. However, as research has shown, attackers approach a network from a specific angle, expecting the network to have in depth security and defense strategies. With that said the in-depth defense strategy is also among the most difficult network security solutions to maintain and clean up following a network compromise. Based on a review of the information, to date, nothing has addressed the 2013 Defense Science Board's Report call to "decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise DoD systems."[283]

In terms of decreasing the confidence of would-be attackers, two steps must be taken. First, one has to impose a cost for engaging in the determined illegal activity. Second, the cost must be great enough to reduce the confidence the actor has in who they tasked to carry out the CNE. However, the cost cannot be immediately felt, the objective is to induce the adversary into acting on behalf of the illegally transferred data.

[282] ibid.
[283] US Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat" (Washington, DC, 2013).

Creating a network through decoys, honeypots, and incubators employs deception. All of these factors are essential when attempting to get the hacker to believe that he or she has penetrated the target network's defenses. CE techniques, used by passing intended information through the controlled network environment, are also incorporated. However, depending on the actor and the specific target in mind (document, network, and person), CE techniques through physical controlled or double agent operations would improve the credibility of the documents or network environment. Using salted documents would aid in the attribution and exploitation of the hacker, allowing the recipient of the hack to covertly follow the theft of the documents.

From this literature review, we see that SCIOs in cyberspace can strategically assist the US government in enhancing, amplifying, and inflicting technological or military surprise. This was found through adversary and US initiated operations. They can be used to identify what is really worth protecting based on your adversary information needs to a source, protecting the elements that are truly unknown, and enhancing or amplifying its capabilities through the conditioning of the analytical and cyber environment of the adversary by ensuring the confidence in their clandestine sources of information. However, while OCOs show much promise, limitations exist. As we saw with Stuxnet, such activities can also give one's adversary a jump-start to its own OCO program.

In closing, adversary cyber investments yield maximum returns. Second, attribution is very hard to carry out. Third, US cyber policy has yet to effectively address protection of intellectual property, research and development, and other national security information. Another option has to be found outside of the traditional concepts put forward and borne out of a Cold War mentality, especially in times when economies are entangled and positions of power are being challenged. Taking advantage of one's adversaries' covert exfiltration

channels to steal sensitive US proprietary information is probably one of the greatest advantages of the United States. Regardless of the cyber attacker's identity (state or non-state actor), it is clear that in terms of tactics, techniques, and procedures, attackers study their target and adjust the attack based on what they have learned or have been given, with the goal being to infiltrate the network and exploit the target covertly. SCIOs reverse the hacker's TTP to become the advantage of the SCIO initiator.

Deception in Cyberspace-Decoy Operations

> *"The focus of this dissertation is on a defense system of an offensive nature, intended to confuse and deceive adversaries by leveraging uncertainty, to reduce the knowledge they ordinarily have to target systems, or they may be used to provide false information to an adversary that causes a detectable reaction."*[284]

In 2011, Brian Bowen used his PhD thesis to make the following point about using network and host decoys to detect malicious actions by hackers or malware and educating users on potentially vulnerable actions: "although the threats and adversaries may vary, in each context where a system is threatened, decoys can be used to deny critical information to adversaries, making it harder for them to achieve their target goal."[285] The purpose of Bowen's thesis was to lay out "a design for host and network deception infrastructure",[286] and the framework was tested successfully. The plan of the operation was to survey the threat landscape facing the potential target and design a system enabling seamless network generation and host decoys to fool the attacker.[287] Three principal factors were tested, using a wide variation of potential attackers: the "believability of the generated decoy"; "their

[284] Brian M. Bowen, "Design and Analysis of Decoy Systems Computer Security" (PhD Thesis, Columbia University, 2011).
[285] ibid., 17
[286] ibid., 18
[287] ibid.

ability to detect attackers"; and the accurate measurement of the target's network to ensure that scalability is tailored for the activity.[288]

As Bowen declares, his research made the following contributions: [289]

- A novel set of generally applicable properties are proposed to guide the design and deployment of decoys and maximize the deception they induce for difference insiders who vary by their level of knowledge and sophistication.
- A large-scale automated creation and management system for deploying decoys that can indicate malicious insider activity. This provides a means for ordinary users to deploy decoy documents without having to setup sophisticated honeypot systems and sensors.
- The use of decoys properties to measure the success of the proposed decoy systems. In particular, we focus on the two most important properties of decoys – believability and detectability – for metrics on which the systems are evaluated.
- A novel architecture based on a 'record, modify, replay' paradigm to automatically generate large quantities of decoy traffic that are injected into the network. The system continuously regenerates decoys to prevent an adversary from learning how to recognize bait over time. We analyze the believability of the generated traffic with human judges and present results from field experiments. We provide a statistical analysis to show the believability of the traffic when automated tools are used.

[288] ibid.
[289] ibid., 17-18

- A novel approach for malware detection that relies on the use of decoy injection where by bogus information is used to bait and delude information stealing malware, forcing it to reveal itself during the exfiltration or exploitation of the monitored information. We demonstrate the believability of the simulations experimentally with human judges and statistical means. We show malware can be detected with various types of web and financial decoys.
- A novel approach to measuring an organization's security posture using decoys that demonstrates an expanded role of decoys for providing utility in measuring security and trapping user mistakes for educational purposes.

Principal Test Area Results

Automatic Generation of Decoy Results: This specific contribution, when tested, determined that normal users outside of specific US government networks could design decoy systems that can detect inside user malicious activities. As a result, it reduced the reliance on sophisticated honeypot systems.

Decoy Networking Results: The system developed by Bowen was able to automatically generate decoys that were believable, and it was difficult to determine what documents were real and which were not. Using human test subjects to identify the real documents resulted in "only 49% accuracy on average, equivalent to random guessing."[290] Bowen's test also proved that the system design, which was used on a real wireless network, was able to detect surveillance and exploitation of the network that was being tested.[291]

[290] ibid., 83
[291] ibid., 84

***Decoy Host System Results*:** Bowen and his team created an application called "BotSwindler" for "a bait injection system designed to delude and detect crimeware causing it to reveal itself during exploitation of monitored decoy information."[292] Using the "Turing Test" and BotSwindler, Bowen's team successfully convinced humans of the veracity of their simulations "about 46% of the time."[293] One of the ripple effects of the technology is BotSwindler's ability to steal the attacker's malware, which could be used for network sensor pattern identification and intrusion detection.

Security Metrics Results: The use of decoys was introduced as an educational tool to assist network use and measure the organization's security posture with the aim that "users can be trained using decoy technology to be cognizant of potential threats."[294] The potential for educating users on networks to detect cyber-attacks or deception shows promise, as the better educated a user, the greater the capability to detect network compromises. This is a continuously sought after objective by the DoD and private sector.

Analysis of the Data and Application to Thesis Concept

Decoy Networks

Bowen's analysis proves multiple points. For the purposes of this thesis, it is important to note the following:

- Decoy systems work by exploiting the attacker without the attacker's knowledge. The decoy system also helps to ferret out insiders who are clandestinely providing information to adversarial entities.
- Results indicate that the believability of documents can be enhanced through inside information, which opens the door to manipulating the information in order to get

[292] ibid.,114
[293] ibid.
[294] ibid., 121

an adversary to act on the false intelligence. Previous experience has shown that the adversary wants verification when provided with manipulated information. Therefore, if one engages in an SCIO using a physical person and a controlled network, and employs as a double agent (deliberately passing information from a target and amplifying and validating the information), this minimizes the chances of a deception operation being detected by the initiator of the attack.

Bowen's theory also has some limiting factors:

- Bowen acknowledges that the technical capabilities show promise, but their development is yet immature,[295] and both the scale of the network and the technology to manipulate the attackers' malware need additional enhancements. Other concepts and technology could be combined in order to increase the technical capabilities of BotSwindler. For example, another security researcher, Kyle Wilhoit, developed a similar process called "illumination operations", which was designed specifically to reverse the attacker's malware and exploit the attacker's cyber infrastructure.[296] This technique is similar to Bowen's, but uses cyber incubators, which mimic the cyber environment that the adversary was attempting to penetrate. The incubators trick the malware into hatching, which allows the defenders to study that attack in progress.
- Due to the immaturity of the technology and the testing process set up to determine the skill of the attacker, no assessment of the attack was conducted after the intruder had entered the network. The attacker was assessed through the credibility of documents, meaning the document had to have substance and contain information that actually interested the actor. If a bottom-up testing process were to be

[295] ibid., 125
[296] Wilhoit, "T318 Chicken of the APT"

developed with the integration of other technology, the chances the owner of the targeted network controlling the outcomes of an intrusion would be markedly improved.

Illumination Operations

Wilhoit extends Bowen's concept by creating a network environment that the APT can penetrate. The illumination process involves creating a network that operates in parallel to the APT targeted network. The creation of this "sandboxed" environment allows the network defenders to thoroughly monitor the APT's malware, thus enabling live study of the tools being employed against the network, what the intruder is searching for, and its communications plan.

- This process allows for the defender to manipulate the malware, and the manipulated data creates an opportunity for the defender to exploit the intruder through the manipulated data the APT is focused on stealing. The technical manipulation of the malware transforms the APT's malware into a Trojan horse to the initiating APT, accessible to the defender at any time. This in effect would create a reversal of APT CNE operations, enabling the defender to not only control the manipulated data the APT is stealing, but also to use the homing technology to monitor internal and external malware movements, enhancing and bolstering network security.

Conclusion

SCIO operations are modeled after the double-cross system and can be initiated through various means (human, technical, cyber) in order to enhance and amplify the strategic defense objectives of the United States.

Question: Are SCIOs possible in cyber-space, and is it technically feasible to reverse Computer Network Exploitations (CNE)? Are SCIOs a viable option to increasing the cost and risk of states, organization, and groups who attempt to exploit stolen US Government data? Can this be achieved with existing capabilities and techniques?

Answers: First, SCIOs are possible in cyber-space and commercial market trends, as seen by the use of intelligent deception techniques by US health care and IT companies in particular. The commercial market movement towards this technique indicates that deceptive networks are being used to reverse APT CNE and learn from their attacks to bolster cyber defenses.[297] Second, the question should have probably been phrased differently: are SCIOs in cyber-space a viable option to increasing cost and risk of states, organization, and groups who attempt to exploit US Government data? Based on current US cyber strategy, it appears these techniques are gaining traction within the commercial space; meanwhile the Department of Defense is focusing energies in other areas of network defense and shaping policies to affect the global non-governed cyber environment. So the answer to the question is "It depends." For SCIOs to be a viable option in cyberspace, the US must invest in basic science gains that benefit the US economy, along with defense research and development that feed commercial solutions. The US government must also understand that a majority or the information/data these actors pursue is outside the US government network domain. Based on current APT CNE data, it appears that as a whole,

[297] Yoel Knoll, "Why Healthcare IT Teams Love Intelligent Deception. @CloudExpo (January 13, 2017). Accessed August 24, 2017, http://cloudcomputing.sys-con.com/node/3980354.

the APTs are a vacuum for US data. They break in, harvest the information, and then stay behind to establish an ability to remotely access the network at a later time.[298] However, through the review of the recently developed concepts of illumination operations (Wilhoit) and systems operations (Bowen), it was shown that a great deal of work is required in ahead of time to prepare the data and network to look plausible and scaling the network properly is very timely.

The need for plausibility is an element that has not been fully analyzed within this body of research. The network preparation and material have to be believable in order for the sale of the APT's CNE operation to be successful. However, increasing the believability of the operation depends on the material that has been placed on the decoy system for the cyber actor to exfiltrate.[299] Tactically, the defender has to deceive the APT into believing it has infiltrated its network defenses, so the internal network design has to be legitimate, and the defender has to ensure the APT remains unaware that it has been detected.

The strategic aspect is the quick reversal and feed of material to the APT to ensure they think their CNE is secure and successful. The APT must believe the material is genuine and is what they have been tasked to steal, and the material must be believable enough to entice the APT to continue to come back. One flaw was found in this approach: without the human element, the operation could be compromised from the start. Using a trusted insider or someone with knowledge to feed the APT targeting information to attack the network in the manner or means necessary to be exploited in the front end increases the likelihood the operation and material will strategically impose a cost that is beneficial to the US.

---

[291] Singer and Friedman, *Cybersecurity and Cyberwar*; Wilhoit, "T318, Chicken of the APT"; Rid, *Cyber war will not take place*, 35-139

[299] Bowen, "Design and Analysis of Decoy Systems Computer Security"

This technique poses challenges, as knowingly giving up legitimate secrets or commercial research and development has not been visited legally or reviewed against current US policy. The technology to engage in effective cyber security deceptions exists today in the form of illumination operations, incubation, and decoy systems. However, what is lacking is a robust system to synergize defensive and offensive CI activities. SCIO is a hybrid contemporary definition for the famed British Double-Cross system.

Hypothesis: A cyber SCIO using a contemporary network environment would be little different than what the British employed during World War II. The computer and network are the new wireless radio set and selected transmission system for already recruited double agents or agents waiting for adversarial recruitment and employment. SCIOs are technically feasible based on tested and approved research, thus representing a viable option to increasing the costs and risk of states, organizations, and groups who exploit US government data. Historical research leads to a conclusion that when integrated with physical agents, SCIOs in cyberspace will effectively increase the believability of the data provided from both channels of clandestine communication, thus creating opportunities to elicit a response favorable to the initiator or defender. However, the scalability and capacity to conduct large-scale SCIOs cannot be evaluated at this time unless physically tested.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

"To Marshall and his associates, the lessons were clear. The side that recognized and exploited such advances gained not just an edge in warfare but an overwhelming advantage; for the side that missed the chance, the consequences could be fatal."[300]

Summary of findings

The defining and shaping of strategic counterintelligence was conducted through the research and study of historical counterintelligence operations. These operations employed military, diplomatic, and industrial establishments, using them as channels of information to deliberately manage an adversary's clandestine intelligence collection operation. The methods of information transmitted through the adversary's clandestine intelligence collection operation incorporated the use of humans—both witting and unwitting, technical penetrations, and wireless interceptions.

The cyber domain is the main domain of the contemporary world. There is a continuous flow of new hackers and programmers, leaving the US security establishment in no short supply of work. These are the current assumptions:

- Violent Non-State Actors (VNSAs) are engaging in offensive and passive intelligence operations aimed at protecting their networks, illicit finances, and communications.
- VNSAs and Violent State Actors (VSAs) are adopting hybrid warfare as a military strategy. That poses a direct threat to the US and will challenge its intelligence community, which is responsible for providing indications and warnings.
- VSAs that engage in cyber-espionage challenge the US's economic security, and there is no end in sight. The US needs a left-of boom like approach, placing great

[300] Peter Boyer, "DOWNFALL: How Donald Rumsfeld Reformed the Army and Lost Iraq," *The New Yorker* (November 20, 2006). Accessed March 31, 2017, http://www.newyorker.com/magazine/2006/11/20/downfall-2

emphasis on multi-modal cost imposition strategies to deter non-state actors, and VNSAs. The goal is to drive the target's moves, not wait for them and react.

Key Findings

Chapter 2, "Can Violent Non-State Actors deceive a State and Can States Deceive a Violent Non-State Actor (VNSA)?" explored the use of strategic counterintelligence and operational concepts derived from historical case studies, presenting information through successful and unsuccessful attempts made by both a non-state actor and state actor. The results demonstrated that VNSAs could effectively deceive state intelligence services, and state intelligence services also effectively deceived VNSAs, showing that running coordinated double-cross like operations is extremely effective at deceiving the target, especially for the purposes of a larger objective. The predominant theme of significant concern is the VNSA's ability to run sophisticated double-cross like operations against highly competent state intelligence services. The ability for a VNSA to deceive a state actor has been done with great success, especially in terms of influencing state actor's leadership. Actors like Hezbollah deserve the most attention and focus, and allied services should work hard to destabilize them.

Chapter 3, "Employment of U.S. Controlled Technology Transfer to Aid U.S. Cost Imposition Strategies", explored whether an SCIO initiated by the state (US) is an effective method to deliver a cost imposition strategy. The selected examples prove that SCIOs, as defined in this research, can be effective against a state actor, and the costs they impose meet the criteria for SCIOs to be a strategic instrument or platform to impose a cost on adversary. The research reveals that the US previously engaged in clandestine operations to counter Cold War adversaries attempting to acquire US

restricted technologies, yet the US has also been victim to state adversary CE operations that have triggered US defense investments based on deceptive information.

Chapter 4, "Double-Crossing the Computer Network Exploitation (CNE) through the Deception of the Advanced Persistent Threat (APT)", assessed whether SCIOs are effective in cyberspace and if they can be successfully developed. The results point to a high likelihood (pending technical feasibility) that double-crossing APTs is feasible. The traditional medium was the wireless radio set that was used to transmit information clandestinely and handled by a controlled asset on the end of the handset.[301] We saw that the cyber environment is a particularly conducive medium for double cross operations. A cyber SCIO using a network would be little different, except for the new wireless radio set. Most importantly, already recruited double agents are waiting for adversarial recruitment approaches.

In conclusion, Chapter 5 provides: a) Counterintelligence Net Assessment and b) Research Contributions to US Defense and Security Studies.

Counterintelligence Net Assessment: Shaping of US Strategic CI

"Any intelligent fool can make things bigger and more complex. It takes a touch of genius – and a lot of courage – to move in the opposite direction" [302]
- Albert Einstein

Andrew Marshall, Director of the Pentagon's internal think tank, who conceived the concept of during the Cold War, led the famed Office of Net Assessment. The Office of Net Assessment's purpose was to provide an alternative to traditional analysis, which forces the Department of Defense to assess its adversary using "a method of broad analysis

[301] Masterman, *The Double-Cross System in the War of 1939 to 1945*.
[302] Jeroen De Flander, "Jeroen De Flander: Strategy Execution Chief," Accessed January 1 2016, https://jeroen-de-flander.com/strategy-quotes-update/

normally characterized by simultaneously focusing on two or more competitors or opponents through a comparative process."[303]

One of the primary analytical points of a net assessment is the synthesis of red (adversary) and blue (friendly) strategy into a single place.[304] A Strategic Counterintelligence Net Assessment should be implemented to review/analyze these sets of broad items:

- Define the political, defense, and future context for analyzing the problems. What is the current and future security environment? Using system-initiated operations, can the challenges we face now and in the future be shaped to advance US national security objectives or tools?
- Identify the trends of reporting coming out of political, defense, academic, and industrial channels of information.
- Can asymmetries be found that can be employed to exploit a gap and gain a competitive edge?
- Assess foreign perceptions/world views, seek them out, and use them to acquire an advantage.
- Outlining of go-it-alone or allied scenarios.
- Assessment of balance: Can the US do this based on current policies and international agreements? Can it use a proxy to employ the strategy?
- Introduction of game theory and modeling with current and future capabilities passed through a double-cross like system to an adversary: This should be mindful of understanding how the adversary will be shaped. There should also be development

[303] Paul Bracken, "Net Assessment: A Practical Guide," *Parameters* (Spring, 2006).
[304] Bracken, "Net Assessment: A Practical Guide."

of SCIO equations specific to affect US military outcomes by increasing the effect of surprise.[305]

- Review of US foreign intelligence and offensive counterintelligence operations to assess returns on operational investments: An example would be utilizing the Cuban initiated double agent operations launched against the CIA, which compromised US clandestine agent covert communications not only in Cuba, but within countries that fell within the USSR. These should be compared to traditional foreign intelligence operations in order to determine similarities and differences.

The conclusion should enable a strong understanding of how US strategic counterintelligence should be developed, as well as current capabilities, such as the capacity to engage multiple actors, and advantages/disadvantages of US strategic counterintelligence.

Research Contributions Specific to US Defense

US Military Operations and Capabilities

SCIOs employed to protect a sensitive capability, technology or operational response plan have a high likelihood of increasing the impact of surprise when engaging an adversary/challenger. Much like Russia's military doctrine of reflexive control, which relies on covert influence, cyber espionage, and sabotage operations, SCIOs are a highly effective response to covertly compromising countries that employ reflexive control like doctrines. As this research revealed through a review of reflexive control and hybrid warfare literature, many techniques rely on the same principles: exploiting an adversary through asymmetric operations, the use of transnational criminal organizations, proxy use, and a focus on breaking the will of the target so the initiator gets a desired pre-planned outcome.

[305] Michael E. O'Hanlon, *The Science of War: Defense Budgeting, Military Technology, Logistics, and Combat Outcomes* (Princeton, NJ: Princeton Universty Press, 2009).

SCIOs, within this context, take the US's vulnerabilities and weaknesses and turn them into a strength that can further US military operations and capabilities by providing the adversary/challenger with corroborated true information. When analyzed, they provide policy prescriptions to the adversary/challenger's leadership decisions calculus. In effect, SCIOs deliver a cost to the adversary challenger engaging in espionage through the controlled release of specific technologies that the adversary/challengers desire to learn about. SCIOs then compromise the adversary/challenger through physical/cyber double-agent operations that prove the benefits of the information provided to the adversary/challenger intelligence entity. The other cost levied on the adversary/challenger is that through this SCIO process, adversary/challenger espionage activities will be compromised through CE tradecraft.[306]

The introduction of cyber to SCIOs only enhances the effectiveness of the SCIO and its objectives. The use of decoy systems has real promise for current cyber-attack threats. Decoy-based malware can be used to further exploit the attacker's covert communications system, and decoy systems can harvest information and begin to shine the light on the proverbial "who ordered the attack" attribution problem.[307]

This research combined multiple concepts to define strategic counterintelligence and what its operations should look like. It frames the concept of strategic counterintelligence as having a direct impact on:

- Research and technology protection programs integrated into defense oriented advanced research agencies, program offices, and command war planning protection schemes. Although defensive, the operational activities produce

[306] Andrew, *Defend the Realm*; Masterman, *The Double-Cross System in the War of 1939 to 1945*; Acosta, "The Makara of Hezbollah"; Ilardi, "Irish Republican Army Counterintelligence"
[307] Bowen, "Design and Analysis of Decoy Systems Computer Security"; Holbrook, "Emerging Cyber Threat Informatics"

opportunities to enhance the system, technology, activity, and plan they are meant to protect.

- Protection of US critical defense, commercial, and civil infrastructure.
- Compromising VNSA operations and infrastructure for US or allied exploitation.
- Defeating foreign denial and deception operations and engaging adversary/challenger doctrine.
- Protecting US economic security and imposing a cost upon actors engaged in economic espionage activities.
- Providing uninfluenced information to National Security Council and Defense leadership, reducing the chances of decision-making directed by the adversary of challenger.
- Reducing bureaucratic sole requirements of "each is responsible for its own house approach to counterintelligence", and increasing the level of support to aide broader US requirements.[308]
- Moving from traditional case driven approaches to system driven approaches, taking lessons learned from historically effective CI services, and establishing penetrations within the target before actively going to look for someone who has access to information that the US needs to acquire.

In closing, this concept is not immature. History has provided numerous examples of the successes and failures of these types of activities designed to enhance and further a nation's strategy. It is now time to operationalize them.

[308] Van Cleave, "Counterintelligence and National Strategy."

Bibliography

Ackerman, Spencer. "CIA Didn't Vet Double-Crossing Suicide Bomber." *Wired*, October 19, 2010: Online.

Acosta, David. *The Makara of Hizballah: Deception in the 2006 Summer War.* Thesis, Monterey: Naval Postgraduate School, 2007.

Andrew, Christopher. *Defend The Realm: The Authorized History of MI5.* Edited by Vintage. New York: Vintage, 2009.

Asimov, Isaac. *Pebble in the Sky.* New York: Tom Doherty Associates, 1950.

Board, Defense Science. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.* Official USG Report, Arlington: Department of Defense, 2013.

Boutnaru, Shlomi. "The Four Horsemen of The Cyber Apocalypse." *The Crunch.* Online, January 10, 2015.

Bowen, Brian M. *Design and Analysi of Decoy Systems Computer Security.* PhD Thesis , Graduate School of Arts and Sciences, Columbia University, New York City: Columbia University, 2011.

Boyer, Peter. *DOWNFALL: How Donald Rumsfeld reformed the Army and lost Iraq.* . New York, November 20, 2006.

Bracken, Paul. "Net Assessment: A Practical Guide." March 2006: 90-100.

Campbell, Duncan. *Carry on Spying-and Dying?* London: New States Society, October 20, 1989.

Clark, Liam. *Freddie Scappaticci Was Our Most Valuable Spy in the IRA during the Troubles: British Army Chief.* April 20, 2012. http://www.belfasttelegraph.co.uk/news/northern-ireland/freddie-scappaticci-was-our-most-valuable-spy-in-ira-during-the-troubles-british-army-chief-28739868.html (accessed Jan 01, 2016).

Committee, U.S. Senate Armed Services. *Senate Armed Services* . March 11, 2014. http://www.armed-services.senate/ (accessed March 01, 2016).

Constantin, Col Dr. Craisor. "Potential National Measures To Counter Hybrid Warfare." *Romanian Military Thinking*, 2015: 17-27.

Cowden, Robert. "OSS Double-Agent Operations in World War II." *Studies in Intelligence* , 2014: 65-75.

Cowden, Robert. "OSS Double-Agent Operations in World War II." *Studies in Intelligence* , 2014: 65-75.

De Flander, Jeroen. *Jeroen-de-Flander.com.* 01 01, 2016. https://jeroen-de-flander.com/strategy-quotes-update/ (accessed 01 01, 2016).

Department, Defense. *Department of Defense Dictionary of Military and Associated Terms.* Military Report, Ft. Belvoir: Defense Technical Information Center, 2010.

Department, U.S. Defense. *Dictionary of Military and Associated Terms.* . Arlington, VA, 01 01, 2005.

Dilanian, Ken, and Brian Bennett. *Al Qaeda bomb plot was foiled by double agent.* May 09, 2012. http://articles.latimes.com/2012/may/09/world/la-fg-bomb-plot-20120509 (accessed June 15, 2014).

Duffy, Peter. *Double Agent* . New York: Scribner, 2014.

Dulles, Allen. *The Craft of Intelligence* . Guilford, CT: Lyons Press, 2016.

Eastham, Todd. *Yemen underwear bomber was 'Saudi double agent'.* London, May 09, 2012.

Ehrman, John. "Toward a Theory of CI: What are We Talking About When We Talk about Counterintelligence?" *Studies in Intelligence*, 2009: Online.

Ehrman, John. "What are We Talking About When We Talk aboug Counterintelligence ." *Studies in Intelligence* , June 2009: 5-18.
Ekman, Kenneth Col USAF. "Applying Cost Imposition Strategies against China." (Strategic Studies Quarterly) Spring (2015): 26.
Engineering, National Academy of, and National Academy of Sciences. *Finding Common Ground: U.S. Export Controls in a Changed Global Environment* . Policy, Washington D.C. : National Academies Press, 1991.
Executive, Office of the National Counterintelligence. *Foreign Spies: Stealing US Economic Secrets in Cyberspace.* Report to Congress, Washington D.C.: Director of National Intelligence , 2011.
Ferguson, Cody. *INCREASING EFFECTIVENESS OF U.S. COUNTERINTELLIGENCE: DOMESTIC AND INTERNATIONAL MICRO-RESTRUCTURING INITIATIVES TO MITIGATE CYBERESPIONAGE.* Thesis, Monterey: Naval Post Graduate School, 2012.
Fisher, Max. "What We Can Learn From Saudi Intelligence ." *The Atlantic.* Washington D.C, Nov 01, 2010.
Giles, Lionel. "Allendale Online Publishing." *University of Alberta.* 01 01, 2000. https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf (accessed Jan 24, 2016).
Gore, Christoper.
Gosler, John. "Digital Dimension." In *Tranforming U.S. Intelligence* , by Jennifer Sims and Burton Gerber, 96-114. Washington D.C.: Georgetown University Press, 2005.
Herbolzheimer, Claus. "Preparing for a Black Swan Cyberattack." *Harvard Business Review*, September 2016: Online.
Hoffman, Frank G. *Conflict In The 21st Century: The Rise of Hybrid Wars.* CETO, Potomac Institute for Policy Studies, Arlington: Potomac Institute for Policy Studies, 2007.
Holbrook, Michael. *Emerging Cyber Threat Informatics: Exploiting Emerging Black Hat Tactics, Techniques, and Targets Through Comparative, Left-of-Boom Analytics.* Thesis, GLobal Security Studies, Johns Hopkins University, Baltimore: Johns Hopkins University, 2013.
Hoover, J. Edgar. ""Is There a Spy Menace?"." *Cinncinnati Enquirer*, July 14, 1940: 74.
Ilardi, Gaetano Joe. "Irish Republican Army Counterintelligence." *Intelligence Journal of Intelligence and Counterintelligence*, December 2009: 1-26.
Jasper, Scott. "Deterring Malicious Behavior in Cyberspace." *Strategic Studies Quarterly* Spring (2015): 60-85.
Knickmeyer, Ellen, and Siobahn Gorman. *Al Qaeda Double Agent Had Western Roots.* New York: Wall Street Journal, May 10, 2012.
Kostin, Sergei, and Eric Raynaud. *Farewell: The Greatest Spy Story of The Twentieth Century.* Las Vegas: Amazon Crossing, 2011.
Kowalewski, Annie. "Disinformation and Reflexive Control; The New Cold War." *Georgetown Security Studies Review* (Center For Security Studies at Georgetown University's Edmund A. Walsh School of Foreign Service), Feburary 2017.
Kulick, Amir. "Hizbollah vs. the IDF: The Operational Dimension." *Institute of National Security Studies*, 2006: 29-33.
Lee, Bradford. "Strategic Interaction: Theory and History for Practitioners." In *Competitive Strategies for the 21st Century: Theory, History, and Practice*, by Bradford Lee, edited by Thomas Mahnken, 28-43. Stanford, California: Stanford University Press, 2012.
Lichfield, John. "How the Cold War was won... by the French." *Independent*, September 17, 2009.

Maceda, Jim, Richard Engel, and Robert Windrem. "Source: CIA Bomber's intel led to successes." January 06, 2010: Online.
MacEwan, Neil. "A Tricky Situation: Deception in Cyberspace." *The Journal of Criminal Law*, October 2013: 517-534.
Macintyre, Ben. *Double Cross: The True Story of the D-Day Spies.* New York: Broadway Books, 2013.
Mahnken, Thomas G. *Cost-Imposing Strategies: A Brief Primer.* Primer, Washington D.C. : Center for a New American Security , 2014.
Manhken, Thomas G. "Thinking About Competitive Strategies." In *Competitive Strategies for the 21st Century Theory, History, and Practice* , by Thomas Manhken, 7-9. Stanforc: Stanford University, 2012.
Martin, Charmaine L. *Military Deception Reconsidered.* Thesis , Naval Postgraduate School, Monterey: Naval Postgraduate School, 2008.
Martin, Charmaine. *Military Deception Reconsidered.* Thesis, Monterey: Naval Post Graduate School, 2008.
Masterman, J.C. *The Doube-Cross System.* Guilford: Lyons Press, 1972.
McAfee. *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II.* Report, 2014: Center of Strategic International Studies, 2014.
McGhee, James. "Liberating Cyber Offense." *Strategic Studies Quarterly*, 2016: 46-63.
Mitnick, Kevin. *Brainy Quote.* January 01, 2000. https://www.brainyquote.com/quotes/authors/k/kevin_mitnick.html.
Mobley, Blake. *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection.* New York: Columbia Univerity Press, 2012.
Mullen, Michael ADM. "From the Chairman: It's Time for a New Deterrence Model." *Joint Forces Quartely*, 2008: 2-3.
O'Hanlon, Michael E. *The Science of War: Defense Budgeting, Military Technology, Logistics, and Combat Outcomes.* Princeton: Princeton University Press, 2009.
Perry, Mark, and Alastair Crooke. *How Hezbollah Defeated Israel: Winning the Intelligence War.* Prod. Conflict Forum. London, October 12, 2006.
Pincus, Walter. *The Washington Post.* November 10, 1995. https://www.washingtonpost.com/archive/politics/1995/11/10/cia-sent-white-house-35-questionable-reports/a70e280e-4147-48ce-9e6d-82ddb1607316/?utm_term=.c18c673c420f (accessed January 1, 2016).
Press, National Academies. *Technology, Policy, Laws, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities.* Policy Report, Washington D.C.: National Academies Press, 2009.
Reidel, Bruce. *Khost CIA Attack: Lessons One Year Later.* Washington D.C. , December 29, 2010.
Report, WMD Commission. *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.* Report to President, Washington D.C.: U.S. Government Printing Office, 2005.
Rid, Thomas. *Cyber War Will Not Take Place.* New York: Oxford University Press, 2013.
Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies*, 2014: 10.
Riggio, Bill. *CIA agents killed in suicide attack 'a gift from Allah'.* Online, March 1, 2010.
Riggio, Bill. *Transcript of interview with Jordanian suicide bomber Khurasani.* Online, March 01, 2010.
Riley, Michael, and Jordan Robertson. *UglyGorilla Hack of the U.S. Utility Exposes Cyberwar Threat.* New York City, June 14, 2014.

Robertson, Jordan. *A Decoy Computer Was Set Up Online.* New YorkCity, September 24, 2014.
Schweizer, Peter. "Victory: The Reagan Administration's Secret Strategy that Hastened the Collapse of the Soviet Union." *The Atlantic*, 1995: 87-90.
Security, Center for Strategic International. *Net Losses: Estimating the Global Cost of Cybercrime.* Public, Washington D.C.: Center for Strategic International Security, 2014.
Services, Records of the Office of Strategic. *History of the United States Counterintelligence.* Official , College Park: National Archives, 1943.
Shane, Scott, and Eric Schmitt. *Qaeda Plot to Attack Plane Foiled, U.S. Officials Say.* New York , May 7, 2012.
Sharma, Adamya. *"A Game of Human Chess": The Double Cross System and MI-5's Supremacy in World War II.* Honors Thesis , Boulder: University of Colorado, 2015.
Sherman, Kent. "The Need for an Intelligence Literature." *Studies in Intelligence* , 1955: 3.
Sims, Jennifer. *"Twenty-First-Century Counterintelligence: The Theoretical Basis for Reform," In Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence.* Washington D.C.: Georgetown University Press, 2008.
Sims, Jennifer, Burton Gerber, and John MacGaffin. "Transforming U.S. Intelligence." In *Clandestine Human Intelligence: Spies, Counterspies, and Covert Action*, by John MacGaffin, 79-95. Washington D.C.: Georgetown University, 2005.
Singer, Peter W., and Allan Friedman. *How It All Works. Cybersecurity and Cyberwar: What Everybody Needs to Know.* New York: Oxford University, 2013.
Singer, Peter, and Allan Friedman. *Cybersecurity and Cyberwar.* New Yord: Oxford University, 2013.
Snegovaya, Maria. *Putin's Information Warfare In Ukraine.* Academic Report, Washington D.C.: Institute For The Study Of War, 2015.
Society, Internet. *Internet Society.* December 10, 2003. www.internetsociety.org/internet/what-internat/history-internet/brief-history-internet (accessed December 10, 2014).
Sterner, Eric. "Retalitory Deterrene in Cyberspace." *Strategic Studies Quarterly*, Spring 2011: 62-79.
Tavares, Ernest S. *Operation Fortitude: The Closed Loop D-Day Deception Plan.* Research Report, Air Command and Staff College, Maxwell AFB: Air University, 2001.
Teague, Matthew. *The Atlantic.* April 01, 2006. http://www.theatlantic.com/magazine/archive/2006/04/double-blind/304710/ (accessed Janurary 01, 2016).
Technology, National Institute of Standards and. *Framework for Improving Critical Infrastructure Cybersecurity.* NIST Cybersecurity Framework, Gaithersburg, MD: NIST, 2014.
Tzu, Sun. *Brainy Quotes.* UNK, December 1, 2014.
Van Cleave, Michelle. *Counterintelligence and National Strategy.* Washington D.C. : National Defense University , 2007.
Van Cleave, Michelle K. *Counterintelligence and National Strategy.* Executive Brief, Washington D.C. : National Defense University , 2007.
Van Cleave, Michelle. "Strategic Counterintelligence: What Is It and What Should We Do About It?" *Studies in Intelligence* , 2007: e.
Vatanka, Alex. *Hezbollah Deputy Leader Expresses Gratitude for Iran and Syria.* Washington D.C. , Jan 27, 2017.
Warrick, Joby. "CIA: Systematic Failures Led to Suicide Attack." *Washingtonpost.Com*, October 20, 2010: Online.
Wege, Carl Anthony. "Hizballah's Counterintelligence Apparatus." *International Journal of Intelligence and Counterintelligence* , August 2012: 771-785.

Weiner, Tim. *The New York Times*. November 10, 1995. http://www.nytimes.com/1995/11/10/us/presidents-got-11-tainted-reports-senator-says.html (accessed January 1, 2016).
Weiss, Gus W. "The Farewell Dossier." *Intelligence Studies*, 1986.
Wilhoit, Kyle. "Incubation, It's Not All About Chickens." *Derbycon* . Louisville: Derbycon, 2014. Online.
Wilhoit, Kyle. *T318 Chicken of the APT Understanding Targeted Attackers with Incubation.* online: Youtube, December 21, 2014.
—. "Trend Micro." *www.trendmicro.com*. October 10, 2014. www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks (accessed December 02, 2014).
Windrem, Robert, and Richard Engel. *NBC News*. January 04, 2014. http://www.nbcnews.com/id/34687312/ns/world_news-south_and_central_asia/#.WPxA8FN94o8.

CURRICULAM VITAE

Graduate School
John Hopkins University

John Gaitan

Date of Birth: July 11, 1980

John.Gaitan@gmail.com

American Public University System
Bachelor of Arts, September 2006

Graduate Thesis Title:
Strategic Counterintelligence: An Approach to Engaging Security Threats to American Security

Major Professor: Dr. Mark Stout