OPEN SOURCE DATA JEOPARDIZING CLEARED PERSONNEL: INTELLIGENCE OPERATIONS OUTSMARTED BY TECHNOLOGY

ALEXANDER H. GEORGIADES

A Thesis

Submitted to the Faculty of Mercyhurst University

In Partial Fulfillment of the Requirements for

The Degree of

MASTER OF SCIENCE
IN
APPLIED INTELLIGENCE

RIDGE SCHOOL FOR INTELLIGENCE STUDIES
AND INFORMATION SCIENCE
MERCYHURST UNIVERSITY
ERIE, PENNSYLVANIA
DECEMBER 2015

RIDGE SCHOOL FOR INTELLIGENCE STUDIES
AND INFORMATION SCIENCE
MERCYHURST UNIVERSITY
ERIE, PENNSYLVANIA

OPEN SOURCE DATA JEOPARDIZING CLEARED PERSONNEL

A Thesis
Submitted to the Faculty of Mercyhurst University
In Partial Fulfillment of the Requirements for
The Degree of

MASTER OF SCIENCE
IN
APPLIED INTELLIGENCE

Submitted By:

ALEXANDER H. GEORGIADES

Certificate of Approval:

____
William J. Welch, M.S.
Instructor
The Ridge School of Intelligence Studies and Information Science

____
Dawn Wozneak, PH. D.
Assistant Professor
The Ridge School of Intelligence Studies and Information Science

____
David J. Dausey Ph.D.
Provost and Vice President for Academic Affairs
Mercyhurst University

December 2015

DEDICATION

To the men and women of the Intelligence Community who will no longer be able to conduct clandestine operations due to the loss of their sensitive information online.

ACKNOWLEDGEMENTS

My sincere thanks goes to Bill Welch, Dawn Wozneak, and Linda Bremmer for their patience and motivation in guiding me through this process.

My thanks also goes to my gracious and supportive wife Sarah, who I owe a few weekends to.

ABSTRACT OF THE THESIS

Thesis Title: Open Source Data Jeopardizing Cleared Personnel.

Thesis Subtitle: Intelligence Operations Outsmarted by Technology.

A Critical Examination

By

Alexander H. Georgiades

Master of Science in Applied Intelligence

Mercyhurst University, 2015

Professor William J. Welch, Chair

The availability and accessibility of Open Source Intelligence (OSINT) combined with the information from data breaches has affected cleared personnel in the United States Intelligence Community (IC) and Department of Defense (DoD) who conduct and support intelligence operations. This information when used in conjunction with biometric detection technology at border crossings has greatly improved the likelihood of cleared personnel from the United States Government (USG) of being identified and targeted by adversaries. The shift from traditional Tactics, Techniques, and Procedures (TTPs) used by cleared personnel (either operating in an overt or covert status) during the Cold War when biometric technology was not an obstacle, has caught the United States government intelligence services off-guard when conducting sensitive missions Outside of the Continental United States (OCONUS)

The consequences of not maintaining updated software and hardware standards have already affected U.S. intelligence operations and exposed cleared personnel. The computer breach at the Office of Personnel and Management (OPM), where millions of sensitive records from cleared personnel in the private and public sectors is the most recent example. This unprecedented loss of Personally Identifiable Information (PII) has been the unfortunate wakeup call needed for decision makers in the United States government to reevaluate how they handle, collect, store, and protect the information of cleared personnel in this digital age.

The analysis of competing hypothesis and other predictive analytical methods will be used to evaluate the data available to adversaries who target cleared personnel and the intelligence operations they support. Case studies, news articles, books, government, and industry reports will be used as supporting evidence to illustrate how the growth in biometric detection technology use in conjunction with the availability of OSINT and material from data breaches adversely affect intelligence operations.

The amount of information available to adversaries is at an unprecedented level. Open source forums provide detailed information about cleared personnel and government TTPs that can be used by adversaries to unravel intelligence operations, target cleared personnel, and jeopardize USG equities (such as sources and methods) in the field. The cleared workforce must learn from mistakes of complacency and poor tradecraft in the past to develop new methodologies to neutralize the effectiveness of adversaries who use OSINT and biometric technology to their advantage.

Social media use by cleared employees who reveal too much operational information about themselves or the projects they work on is one of the gateways that can be easily closed to adversaries. Cleared personnel must be mandated to limit the amount of information they publish online. By closing the door to social media and preventing the personal and professional lives of the cleared workforce from being used to target them, adversaries would not be as effective in jeopardizing or exposing intelligence operations overseas. Increased Operational Security (OPSEC) procedures must also be mandated to protect the programs and operations these cleared personnel work on, with an emphasis on covert officers who use false personas when operating overseas.

The information bridges that were created after September 11, 2001 to increase collaboration must be reevaluated to determine if the relaxation of classified information safeguards and storage of sensitive information is now becoming detrimental to USG intelligence operations and cleared personnel.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CI	Counterintelligence
CIA	Central Intelligence Agency
CONUS	Continental United States
CRS	Congressional Research Service
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FISS	Foreign Intelligence Security Service
HUMINT	Human Intelligence
HVT	High Value Target
IC	Intelligence Community
ISIS	Islamic State of Iraq and Syria
MSPP	Multi-State Plan Program
NGA	National Geospatial-Intelligence Agency
OCONUS	Outside of the Continental United States
OFCO	Offensive Counterintelligence
OPM	Office of Personnel Management
OPSEC	Operational Security
OSINT	Open Source Intelligence
PII	Personally Identifiable Information
RTP	Research and Technology Protection
TRP	The Rendition Project
TSCM	Technical Surveillance Countermeasures
TTPs	Tactics, Techniques, and Procedures
USG	United States Government

INTRODUCTION

Introduction to the Problem

The reliance and use of technology has improved productivity, effectiveness, and planning of intelligence operations in exponential ways since the Cold War. Massive amounts of information needed for business, education, research, and military planning are centrally located on the internet and on restricted classified computer systems available to personnel with a security clearance. Unfortunately, the United States government has become overly reliant on this technology and ease of accessibility to perform day-to-day functions. Its negligence in not implementing the appropriate up-to-date safeguards to protect this information has opened up a Pandora's Box of operational security issues not only for the clandestine personnel who engage in our most sensitive intelligence operations, but also for the mundane office workers and private contractors with a security clearance who support these operations in unglamorous roles.

The seemingly endless amount of sensitive government data and PII that needs to be stored and processed is at an unprecedented level and growing. Technology systems, such as massive server farms and memory storage facilities help to streamline the collection, handling, processing, and accessibility of this material in a timely fashion. Unlike hardened cyber targets, such as the Pentagon or other intelligence agencies that have more up-to-date security protocols, softer targets such as the Office of Personnel Management's network, have not been as prepared. Their out-of-date cyber security safeguards and antiquated data management system proved to be an attractive target for adversaries.

The data breach at OPM yielded the highest quality and amount of PII from security clearance holders in United States history. Data included information about cleared personnel's families, foreign contacts, foreign travel, home address history, educational history, divorces, bad habits, criminal records, and other sensitive information that can now be used by adversaries to target and exploit them. The counterintelligence ramifications of this breach against the USG's most sensitive employees is unprecedented. Utilizing this PII and combining it with OSINT and other data breaches (such as those from the airlines, healthcare systems, and the Ashley Madison adultery website to name a few) would paint an almost complete picture of travel patterns, habits, and operational details that may correlate with intelligence operations in the adversary's country. This data, when properly fed into state-sponsored biometric detection systems at border crossings, could possibly be used to identify or expose cleared personnel who transit certain countries OCONUS. The exposure of these cleared personnel may ultimately impact the effectiveness of the intelligence operations they directly conduct or support.

Background of the Problem

In the aftermath of the events of September 11, 2001, a herculean effort was underway to protect not only the United States, but also the homelands of allied nations from the threat of terrorism. The events of 9/11 catapulted the surge in biometric use on the battlefield to expedite the identification of criminals and terrorists, but it was also implemented at border crossings and other checkpoints throughout the world to identify problematic individuals. Unfortunately, the increased reliance and use of biometric detection technology had unintended negative consequences on individual members of the IC and DoD. Cleared personnel, some of whom operate with alternate identities overseas, are now more prone to compromise when crossing through checkpoints of hostile nations who utilize biometric identification technology. Traditional TTPs used by intelligence personnel that were extremely successful during the Cold War years prior to the mass use of biometrics, now had to quickly adjust their operational methods to evade detection or exposure. The threat to intelligence operations and the cleared personnel who support them is now at the most pronounced level than it has ever been, especially in the aftermath of the OPM breach, increased use of biometric detection technology that thwarts covert operators, and the availability of OSINT available to adversaries.

As far back as 2002, the USG knew that securing their networks was critical to national security. A number of recommendations were outlined in the Federal Information Security Management Act (FISMA) that was signed into law by President George W. Bush in 2002. The goals of FISMA were to mandate the implementation of agency-wide information security protection programs for systems and the data that is stored on those systems. (OPM IG, 2015, p. 1). Unfortunately there had not been as many significant breaches of information in the early 2000's as there were in the three years prior to and including 2015. Had there been more cyber breaches and loss of sensitive data, certain USG offices, such as the Office of Personnel Management, may have been more diligent about protecting their information. It took the OPM breach as the culminating cyber event for the USG to finally take a serious look at the impact of cyber intrusions and the potential effects these attacks have on cleared personnel and the intelligence operations they support.

Adversaries have already capitalized on the government's slow response to security upgrades and lack of PII protection. Due to the lax software and hardware security of not only the U.S. government's systems, but also of those in private industry (such as United Airlines, Anthem health insurance, and even the infidelity website Ashley Madison), adversaries have been able to compile vast amounts of sensitive information. When this data is aggregated, cleared personnel will be severely affected and in turn, affect the intelligence operations they conduct and support.

Statement of the Problem

The perfect storm of USG lethargy in implementing online safeguards of cleared personnel's PII data combined with the availability of OSINT and other information from data breaches have empowered adversaries to use this knowledge against the United States to negatively affect intelligence operations through their cleared personnel.

Most adversaries cannot compete with the military power or projected strength of the United States overseas; however, they have found a solution to this by targeting the online computer systems that hold the most sensitive data of cleared personnel. Adversaries compile information from countless online sources (to include stolen data from computer breaches) to target personnel in the public and private sectors who conduct and support intelligence operations. More advanced nations with cutting-edge biometric technology use OSINT and other PII to target cleared personnel who enter their countries through border crossings and other national checkpoints. Once these individuals are identified, host nation security services are able to target them for recruitment, compromise their false identities if they are not traveling in true name and even jeopardize their operation in-country by initiating advanced surveillance measures.

The ramifications of the OPM breach against cleared personnel, their families, their foreign contacts, and ultimately the operations they support have not yet metastasized. The situation is still too early to assess the overall damage to U.S. capabilities; however, it is only a matter of time before cleared personnel, most likely when crossing through border checkpoints equipped with biometric technology or at other overseas locations will be targeted for exploitation.

Purpose of the Study

The purpose of this study is to demonstrate that data breaches containing information of cleared personnel combined with the availability of open source material, can be used by adversaries, particularly at border checkpoints, to identify and target cleared personnel for exploitation or recruitment. By targeting cleared personnel, the intelligence operations they support will ultimately be jeopardized or compromised altogether.

The use of biometric detection technology by adversaries, most frequently used at border points of entry, adds an additional layer of scrutiny for both overt and covert cleared personnel who travel OCONUS. Depending on the level of hostility that country has towards the U.S. may determine the aggressiveness of border agents to scrutinize those cleared personnel. Furthermore, OSINT and the data obtained from the OPM breach may be fed into those biometric systems thus increasing the likelihood that border agents will be able to identify targets of interest for local intelligence officials to monitor while they are in country.

The increasing frequency of PII data losses and the ease with which adversaries utilize the internet and open source information have created previously unaddressed issues for the personnel who work in the cleared community. Prior to data loss from OPM, the United States had never lost such a large amount of PII from individuals who had a security clearance.

Due to the preponderance and availability of open source materials to adversaries, the U.S. government must increase operational security procedures and training for cleared personnel and improve the security measures for sensitive databases that retain millions of sensitive records from cleared personnel. Moreover, these recommendations will ensure the safety of not only the PII data of cleared personnel, but limit the exposure of those individuals to adversaries who may target them and the intelligence operations they support.

Research Questions

The increased use of biometric technology at international border crossings that is supplemented with data collected online, through social media or from data breaches, have made planning operations more difficult as the potential exposure of the identities, travel patterns, and behaviors of those conducting these operations may be subject to exploitation. By targeting the individuals who carry out these operations OCONUS, U.S. clandestine operators (and even those in overt status who operate with their true names) are exposed to a myriad of problems by host nations. Honey pots, which are situations created most notably by hostile intelligence or security services against visiting personnel, are a classic TTP used to entrap cleared individuals by manipulating an embarrassing sexual situation or circumstance and later using it to blackmail or recruit them. Embarrassing information gleaned from OPM breach (such as problems with alcohol, mental illness, divorce, or sexual proclivities) will be used by hostile host nations to recruit or outright blackmail cleared personnel to operate against the United States. While open source research may be conducted by Foreign Intelligence Security Services (FISS) on cleared personnel prior to their entry into a hostile country, biometric detection and identification technology in the form of facial recognition, iris scans or fingerprint reading devices may be used to identify or expose those individuals who enter the country under an assumed name.

Definition of Terms

Open Source Intelligence, data breaches, and biometrics are the emerging tools adversaries can use to affect intelligence operations by detecting, exposing, and targeting the cleared personnel who support them. The data from the OPM breach, OSINT, and other readily available information may collectively contribute to the biometric databases that foreign governments use to initially detect cleared personnel who may be operating clandestinely in their countries.

Open Source Intelligence is "information of potential intelligence value that is available to the general public" and is one of the easiest intelligence disciplines to utilize. (Clark, 84). The most popular and readily available locations to search for this type of information are on social media websites such as Facebook or LinkedIn, amongst a litany of many others. Far too often members of the DoD and IC frequently post too much personal information about their social lives and even the cleared projects they work on. This information is easily searchable by FISS or non-state actors (such as terrorist groups) and other adversaries who may utilize this information to develop targets of interest or learn more about intelligence activities that would otherwise be unknown to them.

Data breaches occur most frequently in cyberspace, although before the predominant use of the internet and computers in the workplace, data in hard copy could easily be stolen or compromised as well. With the increased use of computers and other technology to make daily work processes more productive, sensitive data, such as the information contained within Standard Form 86, commonly known as the SF-86, has all been digitized or placed on a computer. The SF-86 is the document used by the USG (and stored on OPM databases) to review biographical and historical data for personnel applying and re-applying for a security clearance that allows their access to classified and controlled information. The Standard Form 86 contains the most sensitive PII on every cleared employee in the government, private industry, and academia.

Biometric technology comes in many different hardware platforms such as fingerprint scanners, iris scanners, facial recognition, palm readers, and voice detectors. These various types of biometrics are most frequently used at border crossings as the go-to method to initially detect not only clandestine operators with false documents, but also to identify criminals and terrorists. This technology is also used on the battlefield by the U.S. military and other agencies. Personnel on the ground in a conflict zone can collect fingerprints, iris scans or other similar information from suspected terrorists or criminals they encounter. The purpose of this collection is to cross reference their information with databases that may reveal additional information useful to the soldier on the ground. Biometrics are also used to “enroll” third country nationals or other non-military personnel on government bases and military compounds to keep track of who were on those installations and their activities in one centralized database for quick reference.

Nature of the Study

Through a series of unclassified case studies and analysis of government and industry reports where either cleared personnel or operations were compromised or otherwise revealed to the public, the effects of OSINT, data breaches, and the use of biometrics to detect cleared personnel will be examined to show how intelligence operations have been compromised. The outcomes of the use of these tools by adversaries will be examined to show how they will affect cleared personnel and the intelligence operations they support.

Relevance and Significance of the Study

By analyzing the impact of the OPM data breach and case studies involving how adversaries utilize open source information and data from other online breaches, the author will demonstrate how adversaries use this information to negatively affect intelligence operations and the cleared personnel who support them. Furthermore, the author will present theoretical examples of how aggregated open source information combined with materials from data breaches may be used by adversarial biometric detection technologies at border crossings to identify and target cleared personnel who may engage in operational intelligence activities in their country. Through these case studies, the author will argue for strengthened operational security protocols, changes in TTPs, and limiting the amount of information cleared employees post on their online social media accounts.

Assumptions and Limitations

In conjunction with the information collected from OPM, the airlines, and the health care industry, the hospitality sector would be the next logical industry for adversaries to target. Records from hotel databases would nearly complete a full picture of potential operational activity, travel history, and other movements of U.S. personnel throughout the world. Beyond the historical data from hotels, there would be very little else needed to create a potential High Value Target (HVT) list of cleared government and industry personnel for potential recruitment, blackmail or general exploitation by FISS both domestically and internationally.

When FISS collectively aggregate all of this stolen data, it will not be hard for them to determine persons of interest within the Department of Defense, the Intelligence Community or other sensitive USG locations who are either working clandestinely or under a false alias overseas. Once these individuals are identified, hostile security services have an array of TTPs to manipulate or otherwise control their targets to act against the best interest of the United States.

The major limitation to this study is access to classified information. Presumably a classified damage assessment on the ramifications of the OPM breach will be released to senior law makers and cleared personnel within the IC and DoD. The classified version will most likely reveal specifics about the TTPs used in the breach, the culprits, and what the USG needs to improve with regard to OPSEC practices. While classified information will most likely yield specifics, there is enough information in the public domain to make inferences as to the actual damages and types of intelligence operations that may be affected.

Organization of the Study

The study will be divided into five chapters. The study will examine the background of open source intelligence and how adversaries use OSINT in conjunction with biometric detection technology to impact cleared personnel who may engage in the planning or direct participation in intelligence operations OCONUS. Several case studies, most notably the OPM breach, the tracking of Central Intelligence Agency (CIA) airplanes used for rendition flights, and the botched entry and exit methods used by suspected Israeli Mossad agents when they assassinated Mahmoud Al Mabouh in Dubai, will be examined to illustrate how open source information used in conjunction with technology (biometrics in the case of Al Mabouh) have negatively impacted intelligence operations.

LITERATURE REVIEW

Introduction to the Literature Review

The literature review will address three topics of research related to the negative impact that open source information in conjunction with stolen PII data and biometric identification technology will have on intelligence operations and the cleared personnel who support them. Access to classified reporting on the ramifications of these losses and those who were directly affected by enhanced biometric screening procedures by adversaries as a result is beyond the classification of this review. Fortunately, ample reporting and literature is available to accurately determine and develop a general sense of the long-term impact to intelligence operations and cleared personnel.

In the first section, the literature review will examine tradecraft TTPs used primarily during the Cold War era. This will set the basis for the rest of the thesis to demonstrate how intelligence officers could operate (to a certain extent) more freely during this time period because biometric detection technology was not as prevalent as it is during the present time. The first section will also explore how insider threats created significant problems for intelligence officers and the operations they supported during the Cold War era.

The second section will ascertain the impact of open source intelligence has when used by adversaries against the United States. Specifically, the second section will support this by reviewing articles discussing the use of social media by The Islamic State of Iraq and Syria (ISIS) to target U.S. military personnel and the Robin Sage Experiment that used a LinkedIn social media account under false pretenses to interact and expose cleared government and industry professionals.

In the third section, the Congressional Research Service (CRS) report on the cyber intrusion into the OPM breach will be reviewed and the potential impact of the stolen data will be correlated with recommendations made in the Final Audit Report by the OPM Office of the Inspector General coincidentally published just a few months prior to the breach. In particular, this will examine how the stolen PII will affect cleared personnel and ultimately impact intelligence operations by jeopardizing the identities of those who support and execute those operations.

Lastly, the fourth section will focus on an in-depth review of biometric detection technology. Specifically, an explanation of biometrics, how the technology works, the most common types, how they are defeated, the threats posed to intelligence agents, and the author's observations and personal experience with biometrics at Washington Dulles International Airport in 2015.

All four sections will be supported with research from nine books, 17 news articles, 12 comprehensive government and industry reports on tradecraft, insider threats, OSINT, data breaches, and biometrics detection technology. Advances in OSINT and biometrics technology change at a rapid pace; therefore the information cutoff for this review will be November 2015.

Theoretical Framework

The literature review relies on analyzing government reports, news articles, and case studies to answer how adversaries use biometric technology in conjunction with the availability of open source information to affect intelligence operations and cleared personnel. The documents focus on defining three areas including open source intelligence, data breaches, and the use of biometrics. When these three sources of information are combined, they give adversaries a clearer picture and understanding of who the cleared personnel are that support these intelligence operations and how to target them, specifically when they are subjected to biometric screening procedures prior to entering an unfriendly country. By targeting the personnel who support these missions, adversaries have found a way to directly engage the United States DoD and IC in ways that have left the USG unprepared.

Review of the Research Literature

Tradecraft

The world of intelligence operations and espionage activities were in many ways easier to manage and execute during the Cold War era, prior to the prevalence of the internet, nonstop connectivity through digital devices like iPhones, and the availability of vast amounts of open source data available to adversaries.

Practicing good tradecraft, specifically during the Cold War and up through the mid-1990's, may have involved the use of multiple passports, various disguises, and other classic examples of the "traditional" covert agent or intelligence officer. Many of those methods are still in use today but their effectiveness has been drastically reduced mainly due to the widespread use and prevalence of OSINT and biometrics detection technology.

Intelligence officers operating covertly overseas during the Cold War also relied on more simplistic backstopping mechanisms to prevent adversaries from discovering their true identities, affiliations with front companies and involvement in intelligence operations. Backstopping is the practice of setting up fictitious companies or affiliations with real companies that have addresses, telephone numbers, business cards, and other realistic business literature or materials needed for intelligence officers to pass themselves off as a legitimate representative of that company. (Kessler, 1992, p.116) and (Albarelli, 2009). The entity is usually a corporation or business that is completely fictitious, exists only on paper or is a legitimate corporation that functions in a normal capacity, but strikes an agreement with the U.S. government to provide validation that an undercover intelligence officer is a legitimate employee. (Kessler, 1992, p.115). Backstopping is an important tradecraft method for intelligence officers who are undercover because they need to have a seemingly legitimate reason for being in that particular country or operating in that area while usually working a mundane day-job. Ideally the intelligence officer is a representative of a corporation who is there to conduct some sort of business, research or study as part of his cover persona. (Kessler, 1992, p.115) and (Albarelli, 2009).

During the Cold War era and even in the decades prior, the use of backstopping measures by U.S. intelligence agencies were difficult to scrutinize from an overseas country thousands of miles away. "The illegal officer would slip into a country anonymously and establish an innocuous business as a cover for his intelligence activities. The business often had nothing to do with the officer's intelligence assignment...and it had to be completely plausible and verifiable…" (Batvinis, 2007, p. 136). Unfortunately in present day times, this is not the case any longer. With simple open source searches of company names, telephone numbers, addresses, and employees, an adversary cold partially deconstruct the façade of a CIA front company and associated intelligence operations connected to that company. (Grey 2006, p.124). Google Maps would be helpful to the adversary in discovering if the front company looked legitimate.

The "Street View" setting within Google Maps may show a realistic sign on the company's building façade or if it was an abandoned building in an industrial park with no markings. A search of LinkedIn, Facebook or other social media websites would not be difficult to ascertain a good portion of a company's true employees or their business activities. Usually a legitimate corporation, especially one with a large amount of employees, international partnerships, and successful business endeavors, would have some semblance of a coherent online social media presence for nothing more than advertising and marketing purposes. If a front company has a very limited social media presence, adversaries may be more suspicious of its legitimacy because of its minimal online presence and eagerness to conduct legitimate business. The CIA rendition flights, their kidnapping operation in Italy, the CIA front companies, and other associated logistical functions were all exposed with the availability of open source data by journalists and adversaries alike. (Hendricks, 2010, p. 260-261). These case studies will be explored in greater depth later in chapter 4.

Another important tradecraft method used during the Cold War was the use of multiple passports with either different names or from different countries. The holder of these passports did not have to worry about biometric detection technology at international border checkpoints because it did not exist during the Cold War era. More often than not, the intelligence agent operating under a false name had to worry about how authentic the passport looked to the customs official or border guard. "An agent would enter a country on one passport and depart using another passport under a different name and nationality and with a forged entrance visa attached. An agent might use as many as ten different passports while moving from country to country, creating the impression of being ten different persons." (Batvinis, 2007, p. 141).

The use of false passports in present day times is more difficult with the preponderance of biometric screening and identification technology that can recognize not only false passports, but detect if the correct person is using the passport that was issued to them. (Jacobs and Poll, 2011, p.434). Using false passports in first world nations, especially at border crossings with highly sophisticated biometrics detection and scanning software is extremely risky endeavor. Recent TTPs, like the ones the suspected Israeli Mossad agents used during their assassination operation in Dubai in 2010, highlights the lengths they went through to obtain passports that passed scrutiny at customs. (Epstein, 2014, p.113). While the passports they used were authentic, they were based on stolen identities of duel nationals from Israel and other nations in Europe. (Epstein, 2014, p.110-113). This method is not exactly ideal as the true owners of those passports were extremely upset when the media publicized their names and addresses as being suspected Mossad agents when in reality they had their identities used for the auspices of creating false documents to be used in an assassination operation. (Epstein, 2014, p.111).

Theoretically, tradecraft measures for intelligence officers in present day times need to have a strong social media presence under their cover names with extensive backstopping procedures to avoid detection. Adversaries may turn to open source information to conduct a cursory due diligence check on a suspected intelligence officer or organization they have suspicions about. (Mercado, 2009, p.79). If there is sufficient information online, especially though their social media accounts, a superficial search may pass muster and the intelligence officer may continue undetected with their alias cover name. If there is zero social media or any affiliation with the front company, the intelligence officer may be seriously questioned as this is highly unusual in today's digital society.

Insider Threats to Intelligence Operations

Intelligence operations that were compromised by adversaries during the post-World War II era and through the Cold War were usually due to spies or insider threats. One of the greatest intelligence failures of the CIA during the Vietnam War involving an insider threat occurred during Project Tiger. The operation was led by the CIA station chief in Saigon, William E. Colby and involved the parachuting of 250 South Vietnamese agents into North Vietnam in 1961. (Weiner, 2007, p.246). The operation had disastrous consequences. Of the 250 agents involved in the operation, 217 of them were recorded as killed, missing or suspected of being double agents for the North Vietnamese. Years later, it was learned, the deputy chief for Project Tiger, Captain Do Van Tien, had been passing intelligence to Hanoi the entire time. (Weiner, 2007, p.246).

The insider spying for North Vietnam during Project Tiger is one example of many insider threats and successful spying operations conducted by adversaries against the United States. Insider threats have occurred in present times as well. The most notable recent insider threat, Eric Snowden, created grave damage to a number of National Security Agency surveillance programs. The classified information he stole was through a computer and downloaded onto removable memory sticks, a TTP that was not available prior to the late 1990s. The classified data released online, even though it's currently in the public domain, is still considered classified by the U.S. government. (Lowenthal, 2008). Unfortunately due to these standing laws, the author cannot cite specific examples of compromised intelligence operations by Eric Snowden within this chapter without violating his government non-disclosure agreement signed as a condition of retaining a security clearance. The details of Eric Snowden's leaks of classified National Security Agency information are readily available through a rudimentary search of the internet.

Other more recent threats that will compromise intelligence operations have occurred with the governmental offices who maintain the information of cleared personnel. Specifically, the loss of data from the OPM breach, which will be discussed in length later in the chapter, was the fault of a government office and not the fault of any one intelligence officer or insider threat. The amount of data available on government computers that connect to the internet was never a problem during the Cold War-era and in prior decades as it is today. Now intelligence officers have to worry about their PII being compromised due to a computer breach or other reckless loss than from a trusted insider who purposely releases the information to adversaries.

The following parts of this chapter will focus on case studies and how intelligence operations have been affected by OSINT, data breaches, and biometric detection technology used at international borders by adversaries that is based on aggregated open source data to target cleared personnel.

Review of the Methodological Literature

Open Source Intelligence

The availability of highly accurate information compiled in easy to search locations on the internet about government employees and private industry contractors with security clearances has increased exponentially over the course of the last few years.

The use of this information has inadvertently or by design jeopardized intelligence operations and OPSEC in general, such as the so-called “rendition flights” by the CIA where detainees were flown to foreign countries for the auspices of enhanced interrogations.

The exploitation and analysis of social media has also helped adversaries against the United States in a number of ways. While Facebook is the most popular social networking website, LinkedIn provides more accurate and centralized biographical data on its users who voluntarily supply the information. Adversaries have used this data to accurately identify cleared personnel working on classified programs, make linkages and assumptions to other cleared personnel, and discover sometimes sensitive operational data about intelligence programs. (Ryan, 2009, p. 1).

The Robin Sage Experiment

In 2009, Thomas Ryan, the co-founder and managing partner of Provide Security, LLC, conducted the Robin Sage Experiment. The social experiment was described in his report titled “Getting in Bed with Robin Sage,” in which he first presented the findings at the Black Hat conference in 2010. The experiment sought to “exploit the fundamental levels of information leakage –the outflow of information as a result of people’s haphazard and unquestioned trust.” (Ryan, 2009, p. 1).

The experiment was unique in that it went further than just scanning the internet for sensitive information on cleared personnel or operations, but instead targeted the personnel who support (and perhaps conduct) these operations by actively targeting them through a live social media account.

The 28-day experiment was the first of its kind to use LinkedIn as a means to virtually recruit and interact with senior-level U.S. government and industry personnel in sensitive roles. Ryan did this by creating "Robin Sage" a fictitious female persona who worked as a cyber threat analyst at the Naval Network Warfare Command. Through her false academic credentials and convincing online background, to include an attractive profile picture and other social media accounts, such as Facebook and Twitter, Robin Sage managed to interact and collect information on a number of senior individuals in the DoD and the IC. The experiment was so successful that Robin Sage was offered free conference tickets, employment opportunities, asked to comment (and in theory influence) on-going DoD policy white papers, and other incentives. (Ryan, 2009, p. 1).

Ryan's experiment was important because it successfully proved the concept that a fictitious LinkedIn persona with additional seemingly convincing social media accounts managed to attract, interact, influence, and elicit information from personnel in sensitive positions (most of whom held security clearances). Inevitably these interactions if created by adversaries "could have resulted in the breach of multiple security protocols" and even "violated OPSEC and PERSEC procedures." (Ryan, 2009, p. 2). Lastly, adversaries may use this TTP to not only influence future policy or publications through their authors, but also to acquire key biographical data to target intelligence personnel who support classified operations.

The use of open source information was also used by journalist Steve Hendricks, who wrote the book "A Kidnapping in Milan" to track down CIA personnel now living in the United States. (Hendricks, 2010). These operatives were involved in the 2003 kidnapping of Abu Omar in Italy and exposed by open source means by Italian authorities. This case will be further reviewed in the last section of the literature review.

ISIS Targets Military Personnel

Terrorist groups overseas have already begun using open source information to target the U.S. military. On March 23, 2015, a group calling itself the Islamic State Hacking Division posted the details of 100 U.S. military personnel online. (Fantz, 2015). The group acted on behalf of ISIS and quickly spread the PII information throughout the internet with the intent of providing the targeting details to would-be lone wolf attackers. Initially, the USG thought there was a cyber breach of PII; however, later it was determined by a Daily Beast article that "at least two-thirds of the troops on the ISIS 'hit list' had been featured on public Defense Department websites designed to promote the military…" and that "…the 'hit list' seems to be little more than a bit of creative Googling." (Youssef, 2015). A CNN article also noted that "…ISIS members and sympathizers have been scouring social media sites trying to glean as much information as possible about service members, and have even threatened the spouses of military personnel online." (Fantz, 2015). Although sensitive personal information about operational personnel is available online "pro-ISIS hackers have never been responsible for a major cyber breach, but their capabilities are growing." (Fantz, 2015).

The use of information available online to target military personnel by adversaries could be considered inevitable. There is very little members of the DoD and IC can do to prevent this aside from limiting the amount of information they post online. Even so, there are countless public records websites available to paying members that offer PII for DoD and IC members once a person's name is known. (Hendricks, 2010). Aside from information found within a target's social media accounts, data could also be compiled from real estate websites, county tax records that reside in the public domain that reveal addresses and other open source tools used to gather personal information online.

The use of publically available information has also been used by advocacy groups and journalists to expose intelligence operations relating to the CIA's rendition program. While advocacy groups and journalists are not considered a traditional adversary, they too can create grave damage and exposure to intelligence operations and cleared personnel.

Data Breaches

Office of Personnel Management Inspector General's Report

Undoubtedly the worst breach of PII from cleared personnel who work and support intelligence operations was not found online through open source means but stolen through a cyber intrusion. The breach was noticed by the Office of Personnel Management in April 2015, but not publically announced until June 2015. This counterintelligence windfall by what many suspect was an operation conducted by the Peoples Republic of China, strikes at the core of the cleared community due to the data that was exfiltrated. Surprisingly, one month prior to the announcement of the breach, OPM's own inspector general's office completed its Final Audit Report outlining cyber areas of concern in OPM's systems.

The Final Audit Report's goal was to audit the information technology security controls of OPM's Multi-State Plan Program (MSPP). This mandated report was conducted in accordance with FISMA and identified several weaknesses in the portal plan of action and milestones that were classified with a low risk rating. (OPM IG, 2015,

p. 5). The weak security controls are precisely what adversaries easily bypassed to gain access to millions of records from cleared personnel.

Automated vulnerability scans conducted by an independent contractor yielded a number of problems as well. Software patches and service upgrades were not always conducted in a timely manner and that caused unnecessary vulnerabilities which supported the MSPP Portal. (OPM IG, 2015, p. 9). This was in direct violation of the Federal Information System Controls Audit Manual (FISCAM), which outlined how software should be updated frequently to guard against known vulnerabilities that would expose sensitive information to online theft. (OPM IG, 2015, p. 9).

Outdated software that ran on a number of OPM's systems was also found to be non-compliant and in violation of FISCAM. Without immediate remediation, "noncurrent software may be vulnerable to malicious code such as viruses and worms." (OPM IG, 2015, p. 10).

By far the most profound revelation from the Inspector General's report was that the MSPP's web application was configured in an unsecure manner that allowed for the susceptibility for malicious attack methods. (OPM IG, 2015, p. 10). The five malicious methods in need of correction were redacted from the Inspector General's report and unavailable to the public at this time. Presumably one if not all five of these redactions were the uncorrected root causes that allowed the adversary to breach OPM's security and steal millions of files containing the most sensitive PII of the USG's cleared personnel.

The OPM audit was successful in identifying points of failure and other vulnerabilities within the system that housed sensitive PII on cleared personnel.

Unfortunately the report came too late as the computer systems were breached one month after publication. Even so, the recommendations would have taken months to implement and it is still unclear if those recommendations would have stopped an adversarial attack.

The aftermath of this breach caused a significant problem for the USG. The Congressional Research Service prepared a report on the breach for Congress in July 2015. There were immediate national security implications and attention quickly focused on how the stolen OPM information would be used by adversaries against cleared personnel and what, if any, intelligence operational material could have been gleaned from the information contained within the individual security clearance forms stolen from OPM. “Some suspect that the Chinese government may build a database of U.S. government employees that could help identify U.S. officials and their roles or that could help target individuals to gain access to additional systems or information. National security concerns include whether hackers could have obtained information that could help them identify clandestine and covert officers and operations.” (Finklea, 2015).

Due to the classified nature and emerging situation of the OPM breach, comprehensive reporting on the impact to actual cleared personnel and intelligence operations has been limited and conclusions can only be inferred until the OPM damage assessment is declassified. The literature review of the OPM breach will therefore encompass a series of related news articles and governmental and private reports that when collectively assessed, will generate a clear picture of how cleared personnel and intelligence operations may be affected.

The Director of National Intelligence, James R. Clapper Jr., testified about the breach in October 2015. This was the first public glimpse of the immediate impact of the breach against cleared personnel. Director Clapper and other U.S. officials indicated that CIA personnel were pulled out of the U.S. embassy in Beijing, China, as a precautionary move. (Nakashima & Goldman, 2015). They were concerned that cleared State Department personnel who had their records stolen in the OPM breach could have their names cross-referenced with the personnel at the Beijing embassy. Personnel who were not listed as State Department personnel were likely to be CIA officers posing as State Department officials undercover. (Nakashima & Goldman, 2015).

Biometrics

The term “biometrics” has many connotations depending on how and with whom it is used. For the auspices of this study, biometrics will refer to hardware or software technology capable of reading or analyzing iris, palm, fingerprint, facial or voice attributes to identify or authenticate a user. This definition closely aligns with the one used by the SANS Institute that categorizes the four factors of physical attributes used to authentic users with biometric hardware. (Zimmerman, 2011, p. 2).

Biometric detection technology is a critical information security tool used primarily by governments to authenticate users for simple tasks such as the verification for a driver’s license or for entry into the country at a border checkpoint. “They are inherently more reliable than password-based authentication as biometric traits cannot be lost or forgotten (passwords can be lost or forgotten); biometric traits are difficult to copy, share, and distribute (passwords can be announced in hacker websites); and they require the person being authenticated to be present at the time and point of authentication.” (Jain, Ross & Pankanti, 2006, p. 125). Biometrics are not only used to positively identify a person, but also to negatively identify them, i.e. the person is not who they claim they are. (Jain & Kumar, 2010).

Biometric detection technology is only increasing in use. “Virtually all law enforcement agencies worldwide use Automatic Fingerprint Identification Systems.” (Jain & Kumar, 2010, p.1). The Immigration and Naturalization Service Accelerated Service System was one of the first biometric detection systems installed at a major U.S. airport in the mid-1990s. (Jain & Kumar, 2010). Revenues from the worldwide biometric market are estimated to be around $13.8 billion. (Brannen, 2015).

Facial recognition is the most common and widely used biometric detection technology. (Jain, Ross & Pankanti, 2006). “The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships or 2) the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces.” (Jain, Ross & Pankanti, 2006, p. 126).

Fingerprint recognition is the second most widely used biometric detection technology. (Jain, Ross & Pankanti, 2006). Fingerprints are highly reliable, especially from multiple fingers for identification purposes. They are not completely accurate in all cases as a small portion of the population may have fingerprints that are affected by aging, environment reasons or from those in manual labor who have a large number of cuts or bruises. (Jain, Ross & Pankanti, 2006).

Other biometrics, such as hand geometry, iris, keystroke, signature, and voice identification are all increasingly being used by government agencies, but not to the level of facial and fingerprint detection. The identification of a user who participates in biometric screening becomes more susceptible with each type of biometric technology they participate in.

Can they be defeated?

Biometric fingerprint scanners, facial recognition, and iris readers can all be defeated in controlled environments or laboratory testing, but to the common person who faces this technology screening at the international airport or other customs check points, they are nearly impossible to defeat. “A biometric system is prone to numerous errors: failure to enroll, false accept rate, and false rejection rate.” (Jain & Kumar, 2010, p. 7). The biometrics system is also dependant on a host of other factors for success such as the quality of the collected information (such as clear fingerprints or iris scans), size of the database, variations in the operating environment, and several other technical factors that go beyond the scope of this review. (Jain & Kumar, 2010).

In 2002, Tsutomu Matsumoto developed “finger sleeves” made out of gelatin to mimic a finger tip and other physical attributes of human fingers. (Roberts, 2006, p. 6). “In testing, these had a high acceptance rate from fingerprint readers using optical or capacitive sensors. In addition, fake fingers could be enrolled in the system with a 68-100% acceptance rate.” (Roberts, 2006, p. 6). Without defeating the biometric technology in person (with a fake finger at a scanner for example), adversaries may also target the biometric processing systems that store the information. This may be a more enticing option for adversaries because if they access the biometric databases, they may have the option to manipulate the data for their own purposes. As the prevalence of biometric detection technologies increases around the world, adversaries will only increase their eagerness to defeat them.

Biometrics Success

Facial recognition biometric technology was used to assist the FBI in identifying one of the Boston bombers in 2013. Dr. Marios Savvides, Professor and Director of the Biometrics CyLab at Carnegie Mello University, is one of the leading experts on facial recognition technology in the United States. During a telephone interview in August, 2014, Dr. Savvides explained how his team's use of facial mapping algorithms were applied to a surveillance camera photo provided by the FBI during the early stages of the Boston Marathon bomb investigation. Coincidentally, the FBI had an office within the same building as Dr. Savvides and his team on the CMU campus. An FBI Special Agent brought down a surveillance photo of a partial face from the bombing scene and Dr. Savvides and his team quickly went to work. Within a few days, his researchers were able to reconstruct the opposite side of the face from the surveillance picture that was obscured by a shadow. A digitally enhanced composite photograph of the suspect developed through the use of facial recognition biometric technology eventually lead the FBI to identify Dzhokhar Tsarnaev as one of the Boston bombers. (Carnegie Mellon CyLab, 2013).

Threats to Cleared Personnel

The use of biometric detection technology by adversaries at border crossings has become more effective with the availability of open source information and the PII of the cleared community taken from OPM, United Airlines, Anthem health insurance, and the Ashley Madison adultery website. This information when aggregated in advanced analytic databases can be used to identify cleared personnel when traveling overseas, who their associations are, their health problems or sexual proclivities. All of this sensitive data can be used by adversaries to develop a strategy to recruit or blackmail the cleared employee for their own benefit.

Once the biometric data is collected and recorded, it is usually a permanent record. This advanced technology is making it harder for U.S. covert agents and overt industry personnel with security clearances to maintain their operational security through foreign border crossings and checkpoints. Congressman Adam Schiff noted that "technology at times is a double-edged sword. On the one hand, advances like those in the field of biometrics make our ability to identify and track bad and dangerous actors much better. On the other hand, these same technologies have the potential to help others track and identify us." (Brannen, 2015).

In 2008, a national security presidential directive and homeland security presidential directive was released by the George W. Bush administration outlining the importance of biometrics for identification and screening to enhance national security. It stated that "the executive branch has developed an integrated screening capability to protect the nation against known and suspected terrorists. The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen known and suspected terrorists and other persons who may pose a threat to national security." (Bush, 2008).

The United States primarily uses biometrics at border crossings as well as on the battlefield in foreign countries. Biometric technology is located at almost every domestic airport and major border crossing. Exact numbers remain sensitive data and are not published by the U.S. government.

The most prevalent type of biometric technology used at U.S. airports and major border crossings are facial recognition cameras. The author has observed various types of cameras and manufacturers and there does not appear to be any semblance of uniformity in terms of technology across all airports and border crossings.

On March 11, 2015, U.S. Customs launched a biometric facial screening program at Washington Dulles International Airport outside of Washington, DC. (Aguilar, 2015). As part of a random selection of incoming passengers, customs agents will take a digital photograph of the passenger and have it digitally compared to the photograph on the passport's digital microchip. The biometric program will generate a number that will determine if the passenger will need additional screening. (Aguilar, 2015). This biometric screening technology is primarily used to verify the identity of the individual whose name is on the passport. It is unknown if the United States IC has collected such a large enough volume of high quality PII from foreign intelligence operatives to screen for spies through biometric technology as much as adversaries have stolen from the U.S. through OPM and other data breaches.

In June, 2015, the author observed two lines of airline passengers upon entering the international customs area of Washington Dulles International Airport. If passengers were registered, the one line had the option to use the Trusted Traveler Program. The second line was for everyone else or for those who were not enrolled in the Trusted Traveler Program. The Trusted Traveler line had a row of kiosks where a passenger would place their right hand onto the glass that scanned their fingerprints. Within a few seconds, the fingerprints were searched through the DHS database of previously compiled information that the user had already volunteered during an interview with customs officials. After the fingerprints were quickly processed, the author's biographical data populated the screen. Following a series of customs-related questions that could be answered on the kiosk touch screen, the user was prompted to have their picture taken. A few seconds after that, a unique customs entry form with picture was printed. The entire process usually lasts less than 5 minutes. The unique Trusted Traveler customs form would then be given to an officer prior to leaving the secure terminal. In theory, the Trusted Traveler Program verifies the eligibility of the individual enrolled in the program to bypass the long lines usually encountered at customs desks. One of the vulnerabilities of this program is if the traveler is conducting illicit activities, such as smuggling contraband goods, it may not be detected through an individual screening. Additionally, a customs officer will not have the opportunity to assess any suspicious movements or unusual body language from the traveler because they have gone through a kiosk screening process as opposed to an individual screening process from a customs officer. The unusual body language or other suspicious behavior frequently detected by customs agents is sometimes conducive with lying or nervousness that may be grounds for additional screening procedures.

The passengers in the general entry line, depending on the country of origin, frequency of travel to the U.S., visa status, and other variables selected by the border agents, determine the necessary biometric screening procedures required for entry. The author has observed fingerprint scanning and facial recognition biometric procedures as recently as June, 2015; although no company logos or names were observed on the actual biometric devices.

While the use of biometrics can help to identify terrorism suspects even with the partial use of a photo and little other evidence (such as in the case of the Boston Marathon bombers), adversaries can also use biometrics at border checkpoints to identify intelligence officers and obstruct their operations. A rare glimpse into the exposure of a classified operation due to biometric identification technology occurred in 2010 when a suspected Israeli Mossad team conducted an assassination mission in Dubai. This case study will be explored more in depth in chapter 4.

Chapter 2 Summary

The research literature set a baseline for how intelligence agents used certain tradecraft during the Cold War and how their operations could be affected by insider threats. The review was organized into OSINT, data breaches, and biometrics. These three sections explored how adversaries use various TTPs to identify, target, and expose cleared personnel and their intelligence operations. Information collected via OSINT methods and data breaches is also used to populate biometric databases to initially identify covert and overt cleared personnel at border crossings and ultimately jeopardize their intelligence operations.

There are several weaknesses to the study. The primary weakness is the access to classified reporting on the direct impact to other intelligence operations and cleared personnel who may have been jeopardized due to OSINT and biometric detection technology. In addition, there was a small amount of official updated literature available from the government or industry related to these matters. When this information is eventually released, it must be incorporated and analyzed in a comprehensive manner. The literature review was therefore focused on utilizing mostly news articles and limited publications to support the basis for OSINT and data breaches used in conjunction with biometric identification methods to jeopardize intelligence operations and the cleared personnel who support them.

METHODOLOGY

Introduction

The purpose of this study is to explain how adversaries use open source methods and information collected from data breaches as a means to impact or otherwise jeopardize U.S. intelligence operations and the cleared personnel who support them. This aggregated data likely feeds sophisticated biometric screening programs (and relationship mapping or analytical programs) by foreign governments to identify, expose, and target cleared personnel who travel overseas. If those cleared personnel (both in overt and covert capacities) are discovered, the intelligence operations they support domestically or overseas may be compromised.

This chapter will present an overview of the research design and case studies utilized to prove how intelligence operations and their personnel are and will continue to be affected by the use of OSINT and information from data breaches in conjunction with biometric screening technology by foreign governments and adversaries.

Research Design

The information analyzed for this study was found entirely through open source research. Only data from mainstream media outlets and reputable academic publications and government reports were considered. Case study methodologies were chosen to collect information primarily in the areas of open source intelligence of operational TTPs, data breaches of cleared personnel PII, and biometrics as a means for adversaries to expose or otherwise affect cleared personnel and the intelligence operations they support. Open source information was the only design method available because access to classified information surrounding the TTPs by adversaries and foreign governments who use OSINT, information from data breaches, and sensitive biometric technology were inaccessible due to their classified nature. The data was compiled into three categories related to the research question.

Selection of Cases

The first category of case studies selected were how adversaries utilized open source information, primarily found on the internet or in other publically available locations such as court records, to affect cleared personnel and intelligence operations. Within this category, research was conducted into how social media is used to affect intelligence operations and the cleared personnel who support them. TTPs used by ISIS such as searching for the names and addresses of military and government personnel and using that information to target them are one of the specific examples that adversaries have used. The Robin Sage experiment also demonstrated how social media can be used, in this case by creating false LinkedIn profiles, to recruit and interact with cleared personnel who work on sensitive and sometimes classified government programs. The experiment demonstrated how adversaries may use similar TTPs to create vast networks of online profiles and then penetrate the social networks of personnel who work on sensitive programs. By doing so, adversaries learn more about these programs than may be available to the general public as well as building targeting profiles and learning who other personnel are who work on these programs. These same open source TTPs were also used by reporters and anti-torture advocates to uncover the CIA's rendition program. By using court records and online databases of flights, advocates were able to piece together a very comprehensive picture of many rendition flights.

Data breaches were the second topic researched as this is the primary modus operandi used by adversaries to compile sensitive data on cleared personnel. Information stolen or otherwise obtained from OPM, United Airlines, Anthem insurance and the Ashley Madison websites were evaluated and assessed to determine that when all of that information is combined, it creates a devastating counterintelligence profile of cleared personnel who conduct and support intelligence operations. These massive profiles, such as the "Facebook of Everything" (to be discussed in chapter 4) the Chinese are allegedly compiling, will most likely be analyzed to determine how certain cleared personnel will be targeted, what their past travel patterns have been, what sort of operations they may have supported overseas and equally as important, how they can be susceptible to identification at border crossings through biometric identification procedures.

Evaluating how biometric technology affects intelligence operations by targeting the cleared personnel who support them was the final subject method researched. Two high-profile case studies were evaluated to demonstrate how biometrics, with the help of OSINT and stolen information from data breaches, could be used to jeopardize intelligence operations. The discovery of a CIA operation in Milan, where agents left behind too many digital footprints was the most prolific example. The botched operation in Dubai by suspected Mossad agents was the second most notable classified operation exposed and affected by the use of biometrics.

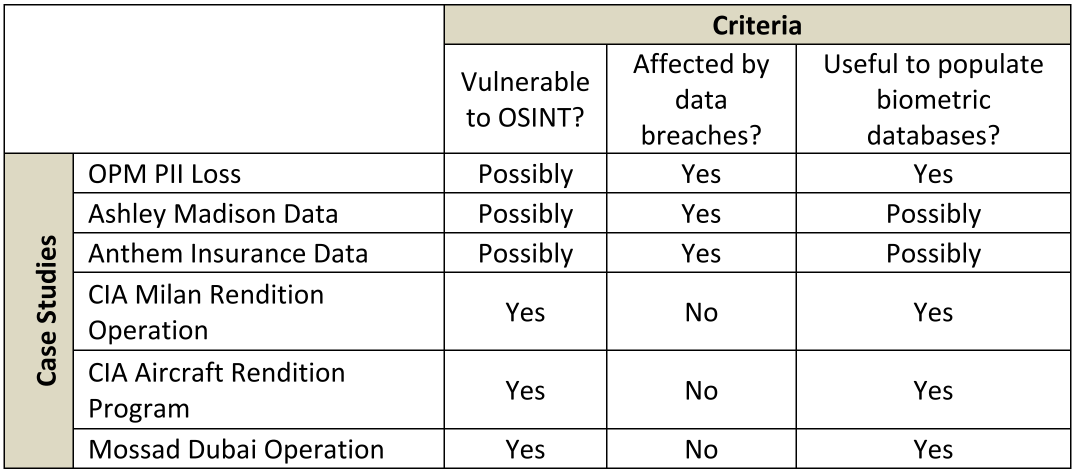
Data Collection

All of the information for this study came from open source materials. There was one relevant book dedicated to the kidnapping in Milan by CIA agents and one relevant book dedicated to the CIA's rendition program. Historical tradecraft and other TTPs were discussed in the third book. The Inspector General's Final Audit Report served as the most significant government publication on the OPM breach. The remainders of case study materials were sourced through media outlets, government and private industry reports and reputable news websites. Detailed findings and damage assessments on these cases remain classified.

Data Analysis Procedures

A matrix was developed using the six case studies in one column while creating three questions as criteria to determine if the cases were appropriate for this study. The cases were selected based on the significant amount of PII lost and exposure of the intelligence operation due to biometrics or data breaches. The focused analysis concentrates on the six case studies because they have common denominators, such as poor security protocols, poor operational security, and the negative impact against the intelligence operation.

A structured focused comparison matrix example was used with information from open source methods, books, industry reports, government publications, and academic journals. The results were collectively assessed to determine if the case study characteristics were relevant for this study. Several case studies were not included because there was not enough open source research material available to make a valid argument for their use or it could not be directly proven that OSINT or biometrics detection were utilized to jeopardize a specific intelligence operation.



		Criteria		
		Vulnerable to OSINT?	Affected by data breaches?	Useful to populate biometric databases?
Case Studies	OPM PII Loss	Possibly	Yes	Yes
	Ashley Madison Data	Possibly	Yes	Possibly
	Anthem Insurance Data	Possibly	Yes	Possibly
	CIA Milan Rendition Operation	Yes	No	Yes
	CIA Aircraft Rendition Program	Yes	No	Yes
	Mossad Dubai Operation	Yes	No	Yes

Figure 3.1: Structured Focused Comparison Matrix Example

Assumptions and Limitations of the Research Design

There are a limited number of comprehensive books on the topic of open source intelligence and data breaches as it relates specifically to affected intelligence operations and inclusive of biometric detection technologies. Due to the fact that the details of these data breaches are still emerging and the level of classification of intelligence operations and cleared personnel who may have been affected by this data, the literature is limited to news articles, government and industry reports, a comprehensive book on the CIA rendition flights, and a comprehensive book on the exposed CIA kidnapping operation in Milan. General background material on tradecraft, insider threats, and circa-Cold War case studies that reinforce the thesis were found within four additional books on policy, intelligence analysis, and historical references.

The key assumption is that the combined information taken from OPM, United Airlines, Anthem health insurance, and the Ashley Madison website will be used by adversaries to target cleared personnel who travel (or who are stationed) outside of the United States. The tool used by adversaries to initially identify these personnel will be biometric technology and screenings at airports and other points of entry by adversarial nations. Another key assumption is that the aggregated data from the aforementioned data breaches will be used to populate the biometrics databases that will be used to cross reference travelers at points of entry.

Lastly, the data breach at OPM was presumably conducted by the Chinese government or those hackers working on behalf of the Chinese government. The information stolen from OPM has not been released or sold on the internet, which leads many to assume that the attack was state-sponsored. The data breaches that occurred against Home Depot and Target had their financial data available for sale on the internet shortly after the intrusions. (Finklea, 2015). Since the Chinese and Russians have a cordial relationship, especially on security and intelligence matters, it is presumed that the Chinese will share portions (if not all) of the OPM data on U.S. cleared personnel with Russian intelligence services. Numerous news articles and scholarly publications allude to this fact, although no U.S. government representatives have officially gone on the record to confirm it publically.

Credibility

The credibility of the cases used in this study has been validated by the parent organizations that lost the information. The Office of Personnel Management, Anthem health insurance, United Airlines and the Ashley Madison website have all confirmed their data was compromised or stolen. The CIA will not confirm the botched operation in Milan or confirm that their front companies or aircraft were connected to the rendition flights. There is sufficient evidence in the public domain that adds credence to the facts of the case as were previously outlined in the literature review. For the final case study, the successful yet embarrassing assassination in Dubai by the Mossad was never confirmed by the government of Israel. Due to the overwhelming forensic, biometric and open source information also presented in the literature review from reputable sources, it is highly likely that the Mossad were responsible for that operation.

Transferability

The findings and supporting evidence presented in this study are transferable to the Department of Defense, the Intelligence Community as well as to corporate America who handle, process, and support classified information for the U.S. government. By understanding what went wrong in each case study, those examples can be learning points taken back by senior leadership to their parent organizations for improvement and to avoid future problems. The embarrassing exposure of information and operations from the majority of these cases may serve as learning points to prevent future intelligence operations from going as poorly as the ones from the case studies have. Ultimately the recommendations in this study may already be included in updated TTPs within certain government organizations and agencies. Due to the classified nature of the outcomes and revised TTPs, this will most likely never be confirmed publically through authorized means.

Ethical Issues

There are ethical issues with the information described in this study, but precautions were taken not to inflict further damage on the actual identities of the cleared personnel who had their PII stolen or intelligence officers who had their identities exposed due to recreation of open source records by adversaries.

The researcher presumes that FISS, such as the Chinese and Russians, do not care about the damage they cause to U.S. cleared personnel with OSINT and data breach information. Specifically, the PII from the OPM breach as well as the data from the Ashley Madison adultery website would be of particular value to recruit a U.S. spy although their use would be highly unethical.

The names of cleared personnel who were compromised with these breaches will not be further published in this study; however, the information is easily found on the internet. The researcher could easily have cited specific cleared individuals who currently work for the CIA and other intelligence agencies that were exposed from data breaches or piecing together open source information found from the internet as adversaries have done in the pats. By citing specific names, this would easily prove how data was used by adversaries to expose cleared personnel and intelligence operations; however, the researcher chose to reference these cases in a way that would not further jeopardize their identities or operational details in writing.

Chapter 3 Summary

The researcher compiled, analyzed, and presented the information with the primary goal of demonstrating how aggregated data will be used by adversaries to target cleared personnel who support intelligence operations. To accomplish this, the researcher used case studies, which were selected based on a criteria matrix that identified them as either being vulnerable to OSINT, affected by information from data breaches or compromised due to adversarial biometric detection. Each of the case studies was unique enough to qualify under at least one of the selected criteria. Open source information was used to validate the key points within each case, although some of the key assumptions are based on facts that may still reside in the classified realm and are unavailable to the researcher.

RESULTS

Introduction

Intelligence operations and the cleared personnel who support them are impacted by adversaries who have access to open source intelligence, stolen information from data breaches, and biometric technology that is used to identify, target or expose overt and covert personnel when traveling OCONUS. The Literature Review identified case studies that fell into the aforementioned three categories. The results of those case studies and how adversaries use OSINT, data breach information, and biometric technology to affect intelligence operations will be discussed in this chapter. In addition, commonalities between the most significant case study examples from each category and their vulnerabilities will be evaluated.

CASE 1: OPM Breach

The information obtained from The Office of Personnel Management data breach in 2015 was the most damaging to the Intelligence Community to date. The information stolen will initially impact cleared personnel and ultimately impact intelligence operations once the information is aggregated to biometrics systems and further analyzed by adversaries. Specifically, the U.S. government's Standard Form 86 on individuals (who each had to fill out the form) were stolen and these documents contained the biographical details and other PII for each individual who applied for a security clearance. The details within the forms included the applicant's PII, information on their families, foreign contacts, associates, travel history, educational history, criminal activity, drug use, and other sensitive information related to their private lives.

To be considered for a U.S. security clearance, the U.S. government Standard Form 86 must be filled out and submitted for review. The SF-86 states that "The United States (U.S.) Government conducts background investigations and reinvestigations of persons under consideration for or retention in national security positions as defined in 5 CFR 732 and for positions requiring access to classified information under Executive Order 12968." Providing information on this form is voluntary and if it is not provided, the applicant's eligibility will be adversely affected. Lying about the information on the form is even worse because it is a punishable offense. Following the investigative process, a formal interview is sometimes conducted to allow the applicant to provide updated or more specific answers to questions on the SF-86. The initial investigation of a new applicant can take anywhere from six months to one year. A security clearance is valid for five years. Ninety days before the five-year expiration point, a re-investigation process is initiated. The re-investigation process can be completed by an OPM investigator within 6 months. As long as the investigation is open, the applicant (if it is a reinvestigation) is allowed continued access even if the five years has expired.

Adversaries will most likely use the stolen OPM information to target cleared personnel who conduct and support intelligence operations. When adversaries have enough biographical and background data on cleared personnel, they will be able to map out that person's life. When that person's life is mapped out, the adversary will have a full understanding of the traits, habits, weaknesses, strengths, and other personal attributes. This information is critical for adversaries to develop a targeting plan to either blackmail, recruit or otherwise neutralize the abilities of that cleared person who belongs to a specific intelligence operation or program.

The information stolen from the OPM breach also includes foreign contacts and foreign travel. If the Chinese intelligence services used this information from the SF-86, for example, they would know who that intelligence officer spoke with, if that officer visited China and when. The Chinese could then track down those Chinese nationals (some of whom may be U.S. IC assets spying on their own country) and neutralize their usefulness to the Americans. The Chinese could target the assets family for retribution; target the asset himself, pass false information to that asset to provide to the Americans as well as a host of other offensive counterintelligence operations that would severely impact the effectiveness of U.S. intelligence missions involving China.

According to CrowdStrike founder Dimitri Alperovitch, Chinese hackers are using information gained from the breaches of the U.S. Office of Personnel Management, as well as intrusions into the Anthem health insurance networks, to build a complete profile of federal employees in what the company calls a “Facebook of Everything”. (Herridge & Dean, 2015). If this is true, the Chinese would have the upper hand in identifying cleared personnel or reconstructing intelligence operations with the help of OSINT. Biometric identification technology would also be used at their border checkpoints to identify cleared personnel based on the information in their purported “Facebook of Everything.”

China’s “Facebook of Everything” emanates from their view on intelligence collection as “a thousand grains of sand”, where Chinese intelligence officers would recruit agents with limited tasking in a host country to collect only a small piece of information. (Hannas, Mulvenon & Puglisi, 2014). Collectively, this information (or proverbial sand) when compiled together would form a complete picture or “beach.” (Hannas, Mulvenon & Puglisi, 2014).

Information from the SF-86 also includes where a cleared individual went to school and who their employers were for the last seven years. This information is extremely valuable to adversaries, especially if used in conjunction with biometrics at border crossings. If and when the information stolen from the OPM breach is aggregated and used as a reference database within biometrics software (such as finger print readers, iris scans or facial recognition), adversaries will instantly know if a U.S. cleared person is arriving to their country under an alias identity or their true identity. Either way, the host nation intelligence services could immediately begin surveillance or other monitoring operations against the cleared person while in-country. If the cleared person is there for an intelligence operation, such as to recruit or meet with a local asset, that mission is now compromised. The ramifications for that asset would also be quite dire, especially in China where espionage laws are more severe than in the United States. If the cleared person is in that country on vacation, for example, the host nation intelligence service could also target the officer for recruitment, blackmail or other adverse actions, especially if they discover that the individual has a gambling, drug, alcohol or sexual addiction that was listed on their SF-86.

The vulnerabilities that have been exposed in the OPM data breach case study are poor network or software computer security within U.S. government databases and centrally storing the most critical data on cleared personnel within databases that connect to the open internet. Additionally, OPM may choose in the future to segregate the SF-86 data so that it is not centrally stored in one location for adversaries to attack.

The damage done by the Chinese-affiliated hackers (who many leading experts suspect are the culprits of the OPM breach) has by all appearances created irreversible harm to cleared personnel and ultimately the intelligence operations they support. Generations of intelligence officers, analysts, and other support personnel have been permanently compromised and the ramifications of this monumental data breach will almost certainly continue to be felt for years.

CASE 2: Ashley Madison Website Data Breach

In July 2015, the private data of more than 33 million users worldwide were stolen from Ashley Madison computer networks by a hacking team called The Impact Team. (Farmer, 2015). The stolen information combined with data from the OPM breach as well as from Anthem and United Airlines (that will be discussed in the following sections) provides a very comprehensive picture of who in the cleared community may be susceptible to espionage or blackmail if they were members of that website. "The Pentagon also is scouring the leaked list of clients and their sexual preferences from the Ashley Madison cheating website to identify service members who may have violated military rules against infidelity and be vulnerable to extortion by foreign intelligence agencies." (Bennett & Hennigan, 2015). The Ashley Madison data could easily be populated in the Chinese "Facebook of Everything" and become an even more comprehensive database used to target cleared personnel. The top Democrat on the House Intelligence Committee, Adam B. Schiff also indicated that the immense data troves could reveal marital problems that foreign intelligence services could utilize to identify and target someone for blackmail or espionage activities. (Bennett & Hennigan, 2015). Due to the emerging situation as of November 2015, there is a limited-to-no analysis or specific examples available from official unclassified reports from the government or industry security professionals on the ramifications of these incidents. Presumably, members of the DoD and IC will be reprimanded, fired, forced to resign or reassigned from sensitive positions if they were proven to be subscribers of that website, thus affecting any intelligence operations that may have been a part of or supported.

CASE 3: Anthem Health Insurance Data Breach

Private information gleaned from medical records, such as the data that was stolen from health insurance company Anthem, also helps adversaries identify vulnerabilities of cleared personnel. (Constantin, 2015). Once these vulnerabilities are identified, FISS may use this information to blackmail or recruit cleared personnel and turn them back against the United States for espionage purposes if the exposed health problems are embarrassing to the general public or their family.

In February 2015, Anthem was the victim of a cyber breach that affected about 78 million people. The company failed to encrypt the data and succumbed to simple phishing attempts, where fake emails were sent to information technology professionals who clicked on links that allowed backdoor access to adversaries to their systems. (Hiltzik, 2015).

Phishing attempts are a common TTP used by criminals and other hacking organizations to persuade individuals to click their malicious website link within an email. Generally only a small percentage of users who receive phishing emails actually open them, but it only takes one user to let the adversary into the network. Hackers presume this, which is why they send out so many emails.

Medical information stolen from Anthem has yet to appear on the black market, indicating that the attack was most likely state sponsored and not conducted by for-profit criminals who in-turn would sell the information on the black market. (Bennett & Hennigan, 2015). This TTP is similar to the OPM breach as that information has not appeared on the open market for sale either. These two data breaches have lead many in the IC to suspect the Chinese of being responsible for both attacks, perhaps in a coordinated attack, as part of a greater plan to target the information of cleared personnel and their most sensitive information.

CASE 4: United Airlines Data Breach

The Chinese are suspected of also penetrating the computer networks of United Airlines according to the Director of National Intelligence, James Clapper. (Peterson, 2015). "Since United is a major contractor for the U.S. government travel, experts say that could mean that a vast cache of information about the movements of specific government or military officials are now in the attackers' hands." (Peterson, 2015). The former senior counselor for cyber security and technology to the FBI director, Paul Tiao, believes that this stolen information could be used in conjunction with the OPM and Anthem data to potentially blackmail or otherwise coerce cleared personnel into committing espionage. (Peterson, 2015).

The information would be extremely valuable to adversaries as it could piece together past travel of cleared personnel. This travel history could be cross-referenced with the adversarial country's entry and exit records to determine if the individual who flew into their country was using an alias or their true name with the help of biometric detection as well as other OSINT. The ramifications to past intelligence operations whose support personnel was jeopardized through this breach could be severe to future operations.

CASE 5: CIA Exposure of Milan Operation

While data breaches of sensitive information on cleared personnel are of grave concern, sometimes the intelligence operations are uncovered through simpler means, such as through open source intelligence. Complacent CIA officers left behind a significant digital breadcrumb trail for Italian authorities to follow, which lead to the exposure of a CIA rendition abduction.

In early 2003, Hassan Mustafa Osama Nasr, otherwise known as Abu Omar, was abducted by CIA officers in Milan, Italy. (Hendricks, 2010). While the rendition of a suspected terrorist was nothing out of the ordinary, especially in the early years after the September 11, 2001 attacks, what made this case so significant was the ease in which 22 CIA agents were discovered by Italian authorities.

The Italian government used a number of biometric digital footprints left behind by the CIA team to uncover Abu Omar's kidnapping in Italy. The most egregious discoveries were the repeated use of the same Subscriber Identity Module, otherwise known as SIM cards and phones used by the CIA near the site of the kidnapping. (Fisher, 2013). In Europe, the buyer of a SIM card is usually required to provide some sort of identification prior to the purchase. When Italian authorities traced the SIM cards to the stores that sold them, copies of several passports were discovered. (Hendricks, 2011). While some of the passports were false, the photos on the identifications were of the agents. Furthermore, by digitally tracking where the SIM cards were used throughout the city through cell phone tower records, the Italian investigators were even able to pinpoint the hotels where the agents were staying. Some of the phones even dialed and received calls from the CIA headquarters in Virginia. (Fisher, 2011). From there, hotel records were uncovered with the identities of the officers and the front companies they claimed that they worked for. Some of the CIA officers even used their hotel loyalty point numbers in their true names, which further exposed and jeopardized their identities. (Hendricks, 2011). Based on the check-in data at the hotels, investigators (and later Steve Hendricks, the author of *A Kidnapping in Milan)* were able to track down the CIA front companies the agents claimed they worked for as their false cover. Italian authorities were even able to determine which flight Abu Omar was taken out of the country from by examining the relative positions of the SIM card users to the proximity of the U.S. military base and the CIA officers. (Hendricks, 2011).

All of these identification issues could have been prevented if the CIA were not complacent in their security methods. Practicing good OPSEC generally involves a five step process dependent on the operation. Identifying critical information, analyzing the threat, analyzing the vulnerabilities of the operation, assessing the risks and finally, applying the appropriate security measures for mission success. (U.S. Department of the Army, 2014).

If the CIA in Italy had not been complacent and applied the five step OPSEC process, their mission would have had fewer blunders. By using cash instead of credit cards to pay for hotel rooms, the CIA agents could have made it harder for authorities to discover their whereabouts as credit card numbers can be correlated with other purchases. Switching out the SIM cards and using new cell phones (while also paying cash to obfuscate their origin) would have also made their movements harder to track by authorities. Sacrificing a few hundred hotel loyalty points would have prevented their true identities and past travel from also being discovered.

Ultimately in 2005, 22 CIA operatives were tried in absentia for Abu Omar's kidnapping. (Donadio, 2009). Almost eight years later in 2013, Robert Lady, the CIA station chief in Milan who led the operation was arrested in Panama at a border crossing with the use of biometric identification technology, presumably on the Italian arrest warrant. (Fisher, 2013). Almost 10 years later in 2015, Sabrina de Sousa, another CIA operative convicted in absentia for participating in the Milan kidnapping was arrested in Portugal at a border crossing with the use of biometric identification technology, also presumably on the Italian arrest warrant. (Kowsmann, 2015).

Since the operation took place in 2003, at least two CIA officers were initially identified through the use of biometric technology and temporarily apprehended. Presumably if the remainder of the CIA officers choose to travel outside of the U.S. and pass through a biometric screening process, they too may be identified or even extradited to face Italian courts.

CASE 6: CIA Exposure of Rendition Aircraft Operations

The Federal Aviation Administration supplies flight data to a number of online websites that in turn, produce real-time live feeds of where aircraft are operating throughout the world. These online databases accessible to the general public also provide advanced notice of aircraft landings at airports. In addition to online flight databases, plane spotters (civilians who station themselves near airports with binoculars to view aircraft as a personal hobby) and published flight plans on the internet could all be sourced to reconstruct past flights originating in the United States. (Grey, 2006).

A security feature that enabled anonymity available on these flight-tracking websites was seldom used by the CIA or its contractors who coordinated these rendition flights. (Grey, 2006). “Time and time again, they seemed to ignore the most obvious ways of keeping their operations secure.” (Grey, 2006). Even the identities of the corporate officers listed on several of the CIA front companies were all the same, thus linking seemingly different aircraft corporations and contractors in different states together with each other. (Grey, 2006). Once the name of the front companies and officers were discovered, open source searches were able to track down specific flight logs that revealed even more details about CIA flights and the companies who arranged them. “Whatever you can find out as journalists, be assured there are other more hostile governments who have found it out already.” (Grey, 2006). By using OSINT to track future CIA flights (used for rendition or other sensitive intelligence missions) it would not be past the purview of hostile nations or even terrorist groups to make preparations at the landing site to compromise the operation for example. The planes, companies that support them, and cleared personnel could also be targeted based on available open source records.

The exposure of CIA flights has so far been used by journalists or past detainees to embarrass or sue the USG in court. By far the biggest group to amass the most comprehensive record of CIA rendition flights using open source methods has been The Rendition Project (TRP).

The TRP is a collaborative research initiative run by two professors from the Universities of Kent and Westminster in England who successfully used a number of open source methods to track and analyze CIA’s rendition aircraft and the front companies that operated those flights. Their website even states that “The extensive analysis on this site is underpinned by an unrivalled body of primary material, such as prisoner testimonies, declassified documents, flight records, company invoices and court documents. Together, these help to build an unparalleled picture of the CIA's torture program. ” Through open source information, TRP has accurately compiled a database of over 11,000 rendition flights, identified more than 60 prisoner transfers that were matched to particular flights, discovered the profiles of over 18 aircraft and uncovered multiple front companies operating these flights on behalf of the CIA. (The Rendition Project, 2015). In spite of its best efforts, the CIA most likely had not planned for its front companies and aircraft flight paths to be so easily reconstructed based on open source information available to the general public. In 2003, a billing dispute between two aircraft contractors served as the initial impetus for TRP to begin compiling open source information on the CIA.

Sportsflight, a small aircraft brokering business based in New York sued Richmor Aviation in 2003 for breach of contract. (Finn & Tate, 2011). These two virtually unknown companies inevitably revealed the first clues to these classified flights that were contained within court records. Their employer, the CIA, used Sportsflight and Richmor to coordinate and conduct rendition flights for a number of high-value detainees during the early years after the attacks on September 11, 2001. While the details of some of the actual flights were protected under the state secrets privilege, more than 1,500 documents from the trial and appeals court did reveal a number of embarrassing facts. (Finn & Tate, 2011). “These logs show multiple calls to CIA headquarters; to the cell and home phones of a senior CIA official involved in the rendition program; and to a government contractor, Falls Church-based DynCorp, that worked for the CIA." (Finn & Tate, 2011). The court documents from this lawsuit were one of many sources of information used by TRP to recreate the flight paths of CIA's rendition flights. While some may advocate that TRP is not an adversary of the United States, nevertheless, they managed to expose and reconstruct the CIA's rendition flights that forced President Obama to subsequently reevaluate and highly regulate the frequency of these once highly sensitive classified operations.

CASE 7: Israeli Mossad Exposure of Kidnapping Operation

Mahmoud al-Mabhouh, a senior Hamas commander was killed in his Dubai hotel room in 2010. The significance of this operation was that the suspected Israeli Mossad team that conducted the assassination was quickly identified through the use of biometric technology and other digital forensic evidence left throughout the city. Similar to the circumstances that exposed the CIA operation in Milan, the Israelis were smart enough to never use their real names in travel documents, on credit cards or other credentials.

The local authorities were able to determine that fake passports were used to enter the country by the agents and subsequently their real photographs were published worldwide. A total of 27 intelligence agents were exposed through the use of biometrics and digital forensics to piece together a timeline with immigration records from the airport, credit card receipts, mobile phone records from phone towers, fingerprints and surveillance footage. (Brannen, 2015). After the story broke, the Chicago Tribune conducted a more extensive analysis of the records from the operation. "Using commercially-available database search tools– the same tools debt collectors use to find delinquent debtors–they uncovered more than 2,600 CIA employees, 50 internal agency telephone numbers and the locations of some two dozen secret CIA facilities around the United States." (Lord, 2015, p. 686). The operatives involved in the exposed operation will most likely not be able to conduct similar operations in Dubai as their real biometric data is now on permanent record.

Data and Analysis

A comparison matrix was created to visualize the most significant case studies affecting intelligence operations and if the information was valuable to adversaries. The results of the comparison matrix were weighed based on a maximum total score of 6 per column. A "YES" in the column was weighed as "1" and a "NO" was weighed as "0". The totals were placed at the end of each row and column.

		Summary of Adverse Impacts					
		Information Available Online	Information From Data Breaches	Affects Intelligence Operations	Affects Cleared Personnel	Enhances Biometric Detection	Overall Score
CASE STUDIES	OPM Breach	NO	YES	YES	YES	YES	4/5
	Ashley Madison Breach	YES	YES	NO	YES	YES	4/5
	Anthem Insurance Breach	YES	YES	NO	YES	YES	4/5
	United Airlines Breach	NO	YES	YES	YES	YES	4/5
	CIA Exposure - Italy	YES	NO	YES	YES	YES	4/5
	CIA Exposure - Aircraft	YES	NO	YES	YES	YES	4/5
	Mossad Exposure - UAE	YES	NO	YES	YES	YES	4/5
	Overall Score	5 out of 7	4 out of 7	5 out of 7	7 out of 7	7 out of 7	

Figure 4.1: Structured Focused Case Study Matrix

The first column in the matrix labeled “Information Available Online” scored a 5 out of a possible 7. Each of the rows in the column ranked “YES” except for the first one and fourth one that ranked “NO.” The OPM Breach row was marked as such because as of November 2015, information stolen from OPM has not been published anywhere on the internet. The rest of the rows were marked “YES” because each one had data that was available to adversaries online that directly affected intelligence operations.

The second column labeled “Information from Data Breaches” scored a 4 out of a possible 7. The OPM, Ashley Madison, Anthem Insurance, and United Airlines case studies all scored a “1” (or yes) while the two CIA case studies and the one Mossad row scored a “0” (or no). The United Airlines row had only one “NO” in the “Information Available Online” column because the data has not yet appeared online. The latter three operations had information available online to adversaries but their operations were not compromised due to a specific data breach.

The third column scored a 4 out of a possible 7. The OPM breach has been covered extensively in the past chapters and the main reason for it scoring a “1” is because of the PII lost for each individual with a security clearance. The Ashley Madison adultery website breach and the Anthem insurance data breaches were significant, but they did not specifically jeopardize intelligence operations. The information when aggregated with the OPM data makes a strong case collectively for affecting cleared personnel but not their intelligence operations directly. The two CIA case studies and the Mossad row were all marked with a “YES” because each mission had specific variables that adversaries used to directly impact their operations.

The fourth column in the comparison matrix scored a maximum 7 out of 7 for impact to intelligence operations by adversaries. Each case study had a series of issues that affected cleared personnel such as sloppy operational security, complacency, poor trade craft, poor computer security or a host of similar variables.

The fifth column also ranked a maximum 7 out of 7. The information from each case study could all collectively be used by adversaries to feed data into their biometrics databases. When the information is stored, aggregated, analyzed and quickly referenced, it creates a monumental counterintelligence threat to cleared personnel and intelligence operations.

The sixth and final column (“Overall Score”) yielded interesting results as each row ranked 4 out of 5. Each row had at least one “NO” beginning with the OPM breach and the United Airlines breach as the data from both case studies has not yet appeared online. Both the Ashley Madison and the Anthem insurance data breaches both had “NO” under “Affects Intelligence Operations” while both CIA operations and the Mossad mission had “NO” under “Information from Data Breaches.”

None of the case studies ranked all “NO” in the rows, nor did any case study rank all “YES” in the row. This is a valuable point because the data demonstrates that while no one case study is crucial, all of the data combined together creates a significant problem for cleared personnel, which ultimately affects intelligence operations.

The most significant case study within the matrix is the OPM data breach failure. The main reason for this is because the biographical data and other PII for each individual who holds (or held) a security clearance is already aggregated into one organized file called the SF-86 as mentioned earlier in this chapter. The information contained within each SF-86 is of greater value to foreign intelligence agencies and other adversaries than the information from the rest of the case studies combined.

Chapter 4 Summary

The results that have emerged in this chapter outline the importance of each case study and how when analyzed collectively, the information will assist adversaries to impact intelligence operations and the cleared personnel who support them.

Seven case studies were discussed and each one was affected by either open source intelligence, a data breach, susceptibility to biometric detection technology or a combination of all three. The impact of each case study had severe consequences on the intelligence operation or the cleared personnel who conduct the mission. The lasting consequences of these case studies will impact not only the operation, but on all future operations and how they are conducted to avoid the mistakes of the past.

The Summary of Adverse Impacts matrix illustrated the five factors that impacted each of the seven case studies. Most importantly, all seven case studies suggested that they directly affected cleared personnel and all enhanced biometric detection used by adversaries.

CONCLUSIONS

Introduction

The biggest impact to intelligence operations by adversaries has been the availability of vast quantities of open source intelligence, the availability of material from data breaches, and the effectiveness of biometrics detection technology that uses OSINT in their core databases to detect cleared personnel.

Open source intelligence is now one of the cheapest and easiest tools for adversaries to use against cleared personnel who conduct and support intelligence operations. By targeting cleared personnel, adversaries are able to affect intelligence operations without having a large army, equipment or the means to directly attack the United States. Instead, they use open source information along with data stolen from computer breaches to piece together a larger picture and understanding of past and possibly future intelligence operations and operational TTPs. With that compiled knowledge, adversaries will have a greater advantage and chance for success against compromising U.S. intelligence operations in the future.

The risk of exposure and targeting of cleared personnel both in overt and covert status by adversaries is at the highest point it has ever been due to the availability of so much background information found through open source methods. When that information is combined and analyzed along with the data from the OPM breach, the adversary will have a significant advantage against U.S. cleared personnel. The aggregated information will also drastically increase an adversary's biometrics technology detection program at border crossings to identify covert personnel and therefore limit the effectiveness of intelligence operations in that country.

The effects of OSINT and data breach materials, combined with biometric technology used at border crossings by adversaries to detect overt and covert cleared IC and DoD personnel poses a continual threat for the foreseeable future.

Summary of the Study

The study focused primarily on the use of case studies to illustrate how adversaries have successfully used open source intelligence and data breach information in conjunction with biometrics technology to negatively affect intelligence operations and the cleared personnel who support them. Case studies were chosen based on the availability of open source material and if an aspect of the intelligence operation or personnel were affected by adversarial interference or exposure.

The case studies were broken down by adversaries who use OSINT, information from data breaches, and the use of biometric detection technology to affect intelligence operations. The case studies were each analyzed then compared to show the commonalities and shortcomings from each one. Lastly, the case studies were organized into a comparison matrix that assigned either a "1" or a "0" value to illustrate which attributes were the most effective against intelligence operations and cleared personnel.

Discussion of the Findings

U.S. intelligence operations are easier for adversaries to negatively affect because of the large quantity of OSINT and data breach information available to them through the internet. The rapidly advancing improvement in biometric technology is also being utilized to impact intelligence operations. When cleared personnel pass through overseas border crossings, this biometrics scanning technology is used to intercept, expose or identify cleared personnel who conduct and support intelligence operations. The information that populates many of these biometric software databases comes from OSINT or even from breached materials, such as the PII from The Office of Personnel Management in 2015.

The stolen OPM material was the most detrimental towards individuals with a security clearance who support or previously supported intelligence operations. Millions of SF-86 security clearance forms were stolen and these were extremely valuable because they contained PII and other critical information that was already aggregated to each person. This now saves the adversary an immeasurable amount of time organizing and cataloging the data for future use, presumably for biometric detection, amongst other means.

The biggest impact to intelligence operations by adversaries who used open source methods was the exposure of the CIA's front companies, personnel, and aircraft connected to their rendition operations. The entities were exposed through open court documents (such as banking and other financial records), telephone calls, and incorporation documents found online at state departments.

Countless front company names, post office box addresses, office addresses, phone numbers, covert and overt identities, affiliated legitimate companies, bank accounts, aircraft tail numbers, and other backstopping apparatuses necessary to conduct these intelligence operations were permanently compromised through open source means. The amount of time and effort needed to rebuild these capabilities would cost well into the millions of dollars. The real damage was not to the backstopping methods or even cleared personnel and their careers, but to the irreparable harm it caused to the reputation of the United States in the eyes of the world. Ironically, the damage caused to the U.S.

was first uncovered by journalists and reporters who were investigating initial reports of CIA aircraft and illegal kidnappings, such as the one conducted by the CIA in Milan, Italy. Ultimately, the exposure and embarrassment of the entire rendition program led the United States government to reevaluate the program and to eventually close down portions of it under the Obama administration.

The exposure of CIA aircraft and front companies operating aircraft on their behalf also exposed the details and intricacies of the 2003 Abu Omar kidnapping by CIA agents in Milan, Italy. Italian investigators used a host of open source methods and even some digital forensics to reconstruct the kidnapping operation. Between the use of true names and credit cards used at hotels, not switching out cellular phones and calling cards, the entire operation could have succeeded without these complacent actions and bad tradecraft. The poor operational security and sloppy operational TTPs used by the CIA agents made it easy for the Italian investigators to piece together and reconstruct the majority of their operation. Reporters and other adversaries were able to piece together the CIA's movements, operational details, tradecraft, and organizational TTPs all through open source methods. This same open source research methodology also lead to adversaries exposing multiple CIA front corporations, true identities of covert officers, mailing addresses, aircraft tail numbers, and other legitimate corporations who were doing business with the CIA. The damage leveraged against these rendition-related operations ultimately proved to be catastrophic for the CIA as the program was drastically reduced and other elements were outright eliminated.

The Israeli Mossad assassination mission in Dubai was the most significant intelligence operation that was compromised due to biometric technology. The Israeli

Mossad was suspected by many leading experts as the organization that coordinated and executed the mission but it was never confirmed by the Israeli government.

The goal of the mission, to assassinate Mahmoud Al-Mabouh, was successful. The unsuccessful part of the mission came after the fact when Dubai investigators were able to reconstruct the movements of the suspected Israeli operatives based on biometrics and open source information left behind. Operational movements, identities, TTPs, front companies, and other logistical supporting elements were all exposed.

The authorities in Dubai initially used video surveillance cameras to look for the perpetrators who killed Al-Mabhouh. When they reconstructed the movements of the suspects back to their arrival at the airport, the authorities located their passports and photographs.

The biometric detection technology used at the Dubai international airport only collected copies of the passports and no other data was collected from travelers, such as finger prints, iris scans or facial recognition images. The authorities were able to ascertain only the data available on a scanned copy of the passports used by the Mossad agents, but no other biometrics (such as retina or fingerprint scans) were collected by border agents. Shortly after the passport details were discovered, the authorities from the United Arab Emirates quickly publicized the photographs and issued international arrest warrants. The Israeli operation further spiraled out of control and completely unraveled when the authorities discovered that the names used within several of the passports were those of real Israelis located in other countries. In essence, the Mossad conducted identity theft and passport fraud of real citizens and were not only caught red-handed, but publically embarrassed in the international media. While other intelligence operations have been embarrassing to their governments, this particular mission was the most highly publicized in recent years.

Even though the passport details were false, the pictures within the documents were real. It is safe to assume that the UAE government more than likely entered the photos of the Mossad agents into the facial recognition software it used with biometric scanning technology at the border. The UAE may also have information-sharing agreements with other countries in the region and it would also be highly likely that those countries also have the same photographic evidence incorporated into their biometric detection systems.

The impact of biometrics on cleared personnel who operate undercover with an alias or with their true identity is most likely quite severe. Due to the sensitive and classified nature of their activities abroad and the fact that the Israeli government has not even accepted responsibility for the Dubai assassination mission leads the researcher to conclude that their future operational activities utilizing these passport TTPs will be extremely limited.

Limited information was available as to the effectiveness of adversarial biometrics technologies that compromised cleared personnel and intelligence operations from the United States due to the sensitive and classified nature of U.S. intelligence activities. Access to classified findings in general from the Intelligence Community would have contributed or influenced the overall results of this study in several ways. The first way would have been accessing damage assessments usually conducted after a security breach or other penetration by FISS against an intelligence mission or component and incorporating those results into this study. The second way would be to assess and evaluate what, if any, tactics, techniques or procedures that may have been adjusted after a mission was compromised. Thirdly, access to classified information would have revealed if there were any other OPSEC procedures recommended prior to an operational intelligence failure. The OPM IG report published prior to the breach was extremely valuable (and timely) for this study, but similar reports were not available for recommendations to adjust clandestine TTPs after the OPM damage was already done.

The OPM data breach, which most security experts agree was conducted by hackers linked to the Chinese government, stole such a large amount of material on cleared personnel (to include the author's SF-86) that it will take years for the ramifications and impact to intelligence operations to come to full fruition. The fact that the stolen OPM data was not released on to the internet is also testament that an adversarial government was most likely responsible for orchestrating the theft.

Implications for Practice

The U.S. government needs to take three actions to protect the effectiveness of future intelligence operations.

The first is to build new backstopping entities such as cover identities and front companies connected with those identities. The personas and corporations need to have significant social media presence as well as additional public records with strong verifiable references. These entities need to be created post-OPM breach and "aged" in a way to reflect significant transactional history and business activity. These measures are necessary because any information listed on the SF-86 paperwork lost by OPM will most likely have a reference or connection to false organizations and covert personas utilized by cleared personnel in past or current intelligence operations. The counterintelligence information gleaned from the OPM breach is a windfall for the adversary that carried it out. It will take decades to repair the damage done to cover personas and front organizations used to conduct intelligence operations.

The second action the U.S. government needs to take is to hold adversaries accountable by conducting and publicizing cyber operations commensurate with those that have been perpetrated upon the DoD, IC, and U.S. industry. The DoD and IC are most likely already conducting significant offensive cyber operations, but their success need to be publicized as a deterrence to others who may contemplating an attack through cyber means. The frequency of cyber-attacks against U.S. interests will most likely increase if there is a perception that there will be no consequences or repercussions from the United States against those who perpetrate these actions.

The third and final action the U.S. government needs to take is to protect any new SF-86 applications from ever being on a computer system that connects to the internet. If the records would have been segregated in a stand-alone computer network that did not connect to the internet in the first place, adversaries would not have been capable of remotely connecting to those systems from thousands of miles away and stealing the data. Increased spending to strengthen these antiquated networks should have occurred years ago. The OPM Inspector General's report outlined similar recommendations prior to the massive breach and for reasons yet unknown, those software and hardware upgrades were simply never executed.

Recommendations for Further Research

The effects of the massive OPM data breach of cleared personnel PII and other valuable biographical information has yet to come to fruition for the public to evaluate.

Within the classified space, it may be safe to assume that the U.S. IC has already made correlations between the information stolen from OPM and the impact that it has had on past, current, and future intelligence operations and the cleared personnel who support them. Suffice to say that until this information is published in a declassified damage assessment, the author and future researchers of this topic will have to remain patient before stronger correlations can be made to intelligence operations that have been jeopardized.

Additional database breaches of PII and other sensitive information will only exponentially increase. Aside from financial data being stolen from companies like Target or Home Depot, the hotel and hospitality industry seems to be the most hardened so far as they have not had a significant breach as the other industries have, yet. If and when a major hotel chain and its customer data is exposed, it will be the last major piece of market data needed for an adversary to compile a nearly complete profile of personnel who conduct and support intelligence operations.

Conclusions

In the advent of this new digital era where the majority of critical information is placed on a computer that somehow connects to the open internet, the United States government needs to prioritize cyber security as their number one area in need of significant strengthening.

The successes of intelligence operations ultimately rely on the cleared personnel who create, conduct, and support them in a variety of ways. The Department of Defense and Intelligence Community learned a hard lesson after the catastrophic loss of data from the OPM breach. Generations of intelligence officers – both past and present – are permanently affected in a way that was out of their control. Many of them will never be allowed to travel to certain countries where they previously operated under alias identities. Others who have close friends, family and business associates located overseas have also been permanently affected. The ramifications of information loss from OPM will affect cleared personnel and the intelligence operations they supported for decades to come.

The battles of the future are already emerging in cyberspace, where critical information vital to U.S. national security operations and cleared personnel are stored. This information needs to be protected and maintained in a more secure manner as the frequency of cyber-attacks will most likely increase over time. In a way, the United States government, who is responsible for being good stewards of this critical information, is able to start over again with regard to protection of PII and other sensitive data. They need to take the lessons learned from the OPM breach and other data theft case studies and use that knowledge to reinforce and strengthen their unclassified networks.

Instead of pursuing more advanced technology to protect this information, perhaps the U.S. needs to look at their long-time adversary for clues on more antiquated and novel ways of securing information. In 2013, The Federal Guard Service, which oversees the secure communications for the Kremlin and the protection of Russian President Vladimir Putin, published an online invitation for businesses to bid on a contract to provide German made typewriters and carbon paper. (Irvine, 2013).

Nikolai Kovalev, the former director of Russia’s Federal Security Service, told Izvestiya (the Russian state-owned news agency): “From the point of view of security, any means of electronic communication is vulnerable. You can remove any information from a computer. There are means of defense, of course, but there’s no 100 per cent guarantee they will work. So from the point of view of preserving secrets the most primitive methods are preferable: a person’s hand and a pen, or a typewriter.” (Irvine, 2013).

Mr. Kovalev’s 2013 quote was in response to operational intelligence that was released on WikiLeaks, the online website that publishes classified documents from whistleblowers. The information was related to a surveillance program that compromised the communications President Dimitri Medvedev during the 2009 London G20 meetings.

The United States would be wise to think outside of the box and look to the past instead of the future for ways to protect sensitive information that could be used to compromise intelligence operations and cleared personnel as the future of the United States’ national security depends on it.

REFERENCES

Albarelli, H.P. (2009). *A Terrible Mistake: The Murder of Frank Olson and the CIA's Cold War Secret Experiments.* Waterville, OR: Trine Day, LLC.

Aguilar, M. (2015, March 19). *The Government is Testing Myriad Invasive Biometric Surveillance Methods*. Retrieved from http://gizmodo.com/the-government-is-testing-myriad-invasive-biometric-sur-1692480582

Batvinis, R. (2007). *The Origins of FBI Counterintelligence*. Kansas City, KN: University Press of Kansas.

Bennett, B., & Hennigan, W.J. (2015, September 16). *China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say*. Retrieved from http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html

Brannen, K. (2015, April 6). *To Catch a Spy. Biometrics is Making It Far More Difficult For The U.S. Intelligence Community To Conduct Clandestine Operations*. Retrieved from http://foreignpolicy.com/2015/04/06/to-catch-a-spy-biometrics-cia-border-security/

Bush, G. (2008, June 5). *National Security Presidential Directive (NSPD) 59 and Homeland Security National Directive (HSPD) 24.* Washington, DC: White House Office of the Press Secretary.

Carnegie Mellon CyLab. (2013, May 8.) *CyLab's Marios Savvides Appears on CNN in Wake of Boston Marathon Bombing Investigation.* Retrieved from http://www. cyblog.cylab.cmu.edu/2013/05/cylabs-marios-savvides-appears-on-cnn.html

Clark, M. Robert (2007). *Intelligence Analysis: A Target Centric Approach* (2nd ed.). Washington, DC: CQ Press.

Constantin L. (2015, July 30). *OPM, Anthem Hackers Reportedly Also Breached United Airlines.* Retrieved from http://www.pcworld.com/article/2954872/opm-anthem-hackers-reportedly-also-breached-united-airlines.html

Donadio, R. (2009, November 4). *Italy Convicts 23 Americans for C.I.A. Renditions.* Retrieved from http://www.nytimes.com/2009/11/05/world/europe/05italy.html

Epstein, R. (2014). *Prisoner X.* Victoria: Australia: Melbourne University Publishing Limited.

Fantz, A. (2015, March 23). *As ISIS Threats Online Persist, Military Families rethink Online Lives.* Retrieved from http://www.cnn.com/2015/03/23/us/online-threat-isis-us-troops

Farmer, B. (2015, August 31). *British Spies Trawl Ashley Madison Leak for Intelligence.* Retrieved from http://www.telegraph.co.uk/news/uknews/defence/11830594/British-spies-trawl-Ashley-Madison-leak-for-intelligence.html

Finklea, K. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: In Brief* (CRS Report No. R44111). Washington, DC: Congressional Research Service.

Finn, P., & Tate, J. (2011, August 31). *N.Y. Billing dispute Reveals Details of Secret CIA Rendition Flights.* Retrieved from https://www.washingtonpost.com/world/national-security/ny-billing-dispute-reveals-details-of-secret-cia-rendition-flights/2011/08/30/gIQAbggXsJ_story.html

Fisher, M. (2013, July 18). *The Story of How a Milan CIA Station Chief Became a Fugitive, Now Caught in Panama.* Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2013/07/18/the-story-of-how-a-milan-cia-station-chief-became-a-fugitive-now-caught-in-panama/

Grey, Stephen (2006). *Ghost Plane: The True Story of the CIA Torture Program.* New York, NY: St. Martin's Press.

Hannas, C., Mulvenon, J.C. and Pugli, A.B. (2014). Chinese Industrial Espionage: Technology Acquisition and Military Modernization. *Foreign Affairs, 210-215.*

Hendricks, Steve (2010). *A Kidnapping in Milan: The CIA on Trial.* New York, NY: W.W. Norton & Company.

Herridge, C., & Dean, M. (2015, September 16). *China reportedly compiling 'Facebook' of U.S. government employees.* Retrieved from http://www.foxnews.com/politics/2015/09/16/chinas-facebook-us-government-employees/

Hiltzik, M. (2015, March 6). *Anthem is Warning Consumers About Its Huge Data Breach. Here's a Translation*. Retrieved from http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html

Irvine, C. (2013, July 11). *Kremlin Returns to Typewriters to Avoid Computer Leaks*. Retrieved from http://www.telegraph.co.uk/news/worldnews/europe/russia/10173645/Kremlin-returns-to-typewriters-to-avoid-computer-leaks.html

Jacobs, B. and Poll, E. (2011). *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government.* The Hague, Netherlands: Asser Press.

Jain, A. and Kumar, A. (2010). *Biometrics of Next Generation: An Overview.* Department of Computer Science and Engineering Michigan State University, East Lansing, MI.

Jain, A., Ross and A., Pankanti, S. (2006). *Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and security*, Vol. 1, No. 2.

Kessler, R. (1992). *Inside the CIA.* New York, NY: Pocket Books.

Kowsmann, P. (2015, October 8). *Ex-CIA Agent Detained in Portugal Over 2009 Kidnapping Conviction in Italy.* Retrieved from http://www.wsj.com/articles/ex-cia-agent-detained-in-portugal-over-2009-kidnapping-conviction-in-italy-1444324821

Lord, J. (2015). *Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age.* International Journal of Intelligence and Counterintelligence, 28:4, 666-691, DOI: 10.1080/08850607.2015.1022464.

Lowenthal, M. M. (2008). *Intelligence: From Secrets to Policy* (4th ed.). Washington, DC: CQ Press.

Mercado, S. (2009). *Secret Intelligence: A Reader.* New York, NY: Routledge.

Nakishima, E. & Goldman, A. (2015, September 29). *CIA Pulled Officers From Beijing After Breach of Federal Personnel Records.* Retrieved from https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html

Peterson, A. (2015, July 29). *What Would Chinese Hackers Want to Go After An Airline?* Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/07/29/why-would-chinese-hackers-would-want-to-go-after-an-airline/

The Rendition Project. (2015, October 16). *The Rendition Project.* Retrieved from http://www.therenditionproject.org.uk/

Roberts, C. (2006). *Biometric Attack Vectors and Defences.* Retrieved from https://ourarchive.otago.ac.nz/bitstream/handle/10523/1243/BiometricAttackVectors.pdf

Ryan, T. (2009). *Getting in Bed with Robin Sage*. Las Vegas, NV: Provide Security, LLC.

U.S. Department of the Army. (2014 September 26). *Operations Security*. Army Regulation 530-1. Washington, DC: U.S. Department of the Army.

U.S. Office of Personnel Management Office of the Inspector General Office of Audits. (2015). *Final Audit Report: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Multi-State Plan Program Portal* (Report Number 4A-RI-00-15-013). Washington, DC: U.S. Government Printing Office.

Weiner, T. (2007). *Legacy of Ashes: The History of the CIA.* New York, NY: Random House, Inc.

Youssef, N.A. (2015, March 23). *'ISIS Hackers' Googled Their Hit List; Troops' Names Were Already on Public Websites*. Retrieved from http://www.thedailybeast.com/articles/2015/03/23/isis-hackers-googled-their-hit-list-troops-names-were-already-on-public-websites.html

Zimmerman, M. (2011). *Biometrics and User Authentication.* Retrieved from http://www.sans.org/reading-room/whitepapers/authentication/biometrics-user-authentication-122