COVERT NETWORKS

A COMPARATIVE STUDY OF INTELLIGENCE TECHNIQUES USED BY FOREIGN INTELLIGENCE AGENCIES TO WEAPONIZE SOCIAL MEDIA

by
Sarah Ogar

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

Baltimore, Maryland
December 2019

Abstract

From the Bolshevik Revolution to the Brexit Vote, the covert world of intelligence has attempted to influence global events with varying degrees of success. In 2016, one of the most brazen manifestations of Russian intelligence operations was directed against millions of Americans when they voted to elect a new president. Although this was not the first time that Russia attempted to influence an American presidential election, it was undoubtedly the largest attempt in terms of its scope and the most publicized to date. Although much discussion has followed the 2016 election, there have not been much concerted historical analysis which situates the events of 2016 within the global timeline of foreign intelligence collection. This paper argues that the onset of social media has altered intelligence collection in terms of its form, but not in terms of its essence. Using the case study method, this paper illustrates how three different nations apply classical intelligence techniques to the modern environment of social media. This paper examines how China has utilized classical agent recruitment techniques through sites like LinkedIn, how Iran has used classical honey trap techniques through a combination of social media sites, and how Russia has employed the classical tactics of *kompromat*, forgery, agents of influence and front groups in its modern covert influence campaigns. This paper's case study analysis highlights the importance of bringing historical perspectives into the current discussion of digital intelligence operations.

Thesis Readers:

Kevin E. Cross, Michael S. Smith II

Acknowledgments

This examination of the tradecraft and techniques used in the weaponization of social media began in the Fall of 2016, as an attempt to help Americans understand the root causes of Russia's interference in the 2016 presidential election. Over the subsequent three years, my friends and family gave considerable support in the completion of this project.

My parents and family members allowed me the time to devote hours of research to this project. My friends gave me space when it was needed and relaxing diversions when they were also needed.

Professors Alexander Rosenthal and Adam Wolfson at Johns Hopkins University provided significant edits and advice. Professor Rhea Siers at Johns Hopkins University conferred a solid understanding of cyber and privacy law which greatly inspired the genesis and subsequent research of this thesis. Professor Mark Stout proved that comparative intelligence studies is not only interesting, but necessary for researchers who wish to fully comprehend the globalized world of modern intelligence collection.

Finally, I am indebted to the scores of historical and contemporary intelligence professionals for providing valuable firsthand accounts of their experiences working within foreign and domestic agencies.

Table of Contents

Intelligence Terms and Acronyms

active measures: a wide array of overt and covert activities designed to influence a group of people

agent: a human intelligence source who is recruited by and works on behalf of an intelligence agency

agent of influence: a witting or unwitting person who is used by an intelligence agency to exert influence over a person or group of persons

front group: a group established and controlled by an intelligence agency

handler: an intelligence officer responsible for the recruitment and handling of human assets

honey trap: the use of an attractive person to approach an intelligence target and collect information

***kompromat*:** comprising material (either real or fabricated) that is published in order to create negative publicity for an individual

HUMINT: Human intelligence or intelligence that is collected from recruited human assets

OSINT: the collection of publicly available information which analyzed and contextualized in order to bring value to an intelligence agency's customers

social media: forms of electronic communication (including websites and mobile applications) through which users create and join online communities to share information, ideas and various forms of digital content

tradecraft: the techniques, technologies and specialized methods employed in intelligence collection and analysis

USIC: the United States Intelligence Community, comprised of seventeen US government agencies

Introduction

In 2016, the United States Intelligence Community (USIC) reported that Russia's intelligence services attempted to influence the 2016 presidential election by targeting millions of Americans through a disinformation campaign on multiple social media platforms. Converting popular social media platforms like Facebook and Twitter into tools used to wage an election interference campaign against the United States was in some respects a novel strategy. Yet a thorough comparative analysis of this election interference campaign and the Soviet Union's covert influence operations during the Cold War suggests Russian intelligence had merely adapted the Soviet model for waging malign influence campaigns. Meanwhile, Russia is not the only state actor that has used social media to manipulate a foreign population. Notable attempts to use popular social media platforms to wage covert influence operations have also recently been attributed to Iranian and Chinese intelligence services. As these actors clearly view popular social media platforms as attractive tools that may be used to wage influence operations, it is necessary to consider ways to build resiliency against these activities. Refining current understanding of how social media may be used by these and other actors to update traditional intelligence operations among governments, the private sector, and civilian populations can help to achieve this objective.

The aim of this paper is to answer the question of which classical intelligence techniques are favored by specific foreign intelligence agencies when they employ social media as a weapon. In order to accomplish this aim, its author has examined relevant literature, and performed case study analysis of foreign intelligence operations conducted by Russia, Iran and China.

A section focused on Russia's efforts to interfere in the 2016 United States presidential election considers how Russian intelligence services employed well-known intelligence techniques that were once utilized by the Soviet Union. A section focused on Iranian regime's activities in the cyber domain examines the Islamic Republic's steadily expanding online covert influence campaigns, which indicate Iranian intelligence services favor the use of digital honey traps. A section focused on China's online intelligence operations examines how Chinese spies have developed expertise with generating personal introductions online that have resulted in successful agent recruitments.

Meanwhile, this paper exposes how foreign intelligence agencies are taking advantage of sociological changes caused by the digital environment, and social media in particular, to expand their capabilities to wage large-scale influence operations, as well as to recruit new assets.

Since its onset in the 1990s, social media has quickly become inextricable from contemporary interpersonal interaction. Although numerous researchers have explored social media's general effects on interpersonal communication, few researchers have addressed questions about how social media has affected the field of intelligence collection.

Significance of the Topic

Foreign intelligence agencies and foreign intelligence entities (or FIEs, which also includes international terrorist groups) have employed social media and other digital tools to gain access to businesses, governments, and individuals. As Russia's infamous influence campaign of 2016 illustrated, social media allows FIEs to directly access a

larger segment of the general population in the United States than FIEs were capable interacting with during the Twentieth Century.

In its *2019 National Intelligence Strategy* (NIS), the Office of the Director of National Intelligence (ODNI) observed:

> Rapid technological advances are allowing a broad range of FIEs to field increasingly sophisticated capabilities and aggressively target the government, private sector partners, and academia. FIEs are proactive and use creative approaches—including the use of cyber tools, malicious insiders, espionage, and supply chain exploitation—to advance their interests and gain advantage over the United States. These activities intensify traditional FIE threats...[1]

Private firms within the information technology security sector seem to agree with ODNI's assessment regarding foreign intelligence agencies' weaponization of social media and increasing reliance on cyber tools. Cyber security firm FireEye assessed that, "Nations across the globe are putting a premium on improving their cyber capabilities," which often includes tapping into the social networks of cyber criminals and the utilization of commercially available cyber tools.[2] In reference to Iran's growing cyber program, cyber security firm F-Secure has urged media organizations and platforms to

---

[1] Office of the Director of National Intelligence, *2019 National Intelligence Strategy of the United States,* Washington, D.C.: GPO, 2019, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

[2] Sarah Geary, "Rise of the Rest: APT Groups No Longer from Just China and Russia," *FireEye* (blog), April 26, 2018, https://www.fireeye.com/blog/executive-perspective/2018/04/rise-of-the-rest-apt-groups-no-longer-from-just-china-and-russia.html.

"consider the specific risks posed by state actors involved in cyber-attack and abuse of native product functionality."[3] FireEye recently assessed that Iran created a network of fake social media personas which "impersonated Republican political candidates that ran for House of Representatives seats in the 2018 U.S. congressional midterms."[4] In March of 2019, cyber threat intelligence firm RecordedFuture released a report which analyzed data from various Western social media platforms from October 2018 through February 2019 to assess ways in which China exploits social media to influence the American public.[5] The firm's researchers concluded that China's covert influence techniques differ greatly from those of Russia. Namely, while Russian covert influence agents aggressively attack and detract from adversaries via social media, Chinese covert influence personas "overwhelmingly present a positive, benign, and cooperative image of China" and opt for more of a softer and diplomatic approach in order to achieve China's specific foreign policy goals.[6]

Within the public sector, various government agencies are reaching out to private sector entities in order to develop a collective strategic understanding of the adversary behind these threats. In 2017, the FBI created an Office of Private Sector (OPS) which seeks to proactively reach out to owners of America's privately held infrastructure and

[3] Ed Parsons and George Michael, "Understanding the Cyber Threat from Iran," *F-Secure,* (accessed November 24, 2019), https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran.
[4] Alice Revelli and Lee Foster, "Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests," *FireEye* (blog)*,* May 28, 2019, https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html.
[5] Insikt Group, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion," *RecordedFuture,* March 6, 2019, https://www.recordedfuture.com/china-social-media-operations/.
[6] Ibid.

address the threats which stem from this privately held infrastructure.[7] At the 2019 RSA Conference, FBI Director Christopher Wray highlighted how public and private sector engagement of cyber threats can be mutually beneficial, citing the FBI's efforts to reach out to social media providers leading up to the 2018 midterm elections.[8] Cyber Command has also extended public invitations to engage on countering the cyber threat to American citizens and infrastructure.[9] In December 2017, Jeanette Manfra, assistant secretary for the Office of Cybersecurity and Communications at the Department of Homeland Security (DHS) announced that DHS was seeking to "to move beyond only offering voluntary assistance" to the American private sector by increasing the use of proactive memoranda of agreement in advance of cyber-related threats to public security.[10] The Cyber security firm FireEye believes that regardless of the malicious cyber activity, "Understanding the adversary is the key to protecting against attacks because, while you can't foresee all attacks, you can at least use intelligence from the past to inform possible future assaults and help mitigate consequences. Consuming adversary intelligence is important to enterprises because in order to protect yourself, you need to know both who will come after you and how they will come after you."[11]

As noted in ODNI's NIS, the top mission priority for the US Intelligence Community is to collect "strategic intelligence" or in other words, to collect intelligence

[7] "Enhancing Engagement Efforts to Stay Ahead of the Threat," FBI, February 2, 2017, https://www.fbi.gov/news/stories/office-of-private-sector.
[8] "Wray Stresses Private Sector-FBI Collaboration Against Cyberthreats," *Meritalk*, March 6, 2019, https://www.meritalk.com/articles/wray-stresses-private-sector-fbi-collaboration-against-cyberthreats/.
[9] Justin Lynch, "Cyber Command wants to partner with private sector to stop hacks," *Fifth Domain,* July 21, 2018, https://www.fifthdomain.com/dod/cybercom/2018/07/31/cyber-command-wants-to-partner-with-private-sector-to-stop-hacks/.
[10] Derek B. Johnson, "DHS plans to step up cyber agreements with private companies," *Federal Computer Week*, December 21, 2017, https://fcw.com/articles/2017/12/21/section9-dhs-cyber-johnson.aspx.
[11] Adam Meyers, "Meet the Advanced Persistent Threats: List of Cyber Threat Actors," *FireEye*, February 24, 2019, https://www.crowdstrike.com/blog/meet-the-adversaries/.

which "addresses issues of enduring national security interest."[12] As the above examples illustrate, foreign intelligence agencies' weaponization of social media and other digital tools remains an enduring national security interest. Therefore, it is critical for academic researchers to explore the classical strategies that inform new iterations of intelligence operations taking place in social media.

If the classically influenced strategies behind social media intelligence operations escape critical examination, then there will likely be no changes to the inherent security structures within social media. It is promising that the US government is trying to be proactive in its outreach to private companies, but part of this should include an intelligence primer regarding the innerworkings and cultural heritage of the adversary. Without historical insight into how foreign intelligence agencies target citizens, public discussion will likely remain focused on the technical aspects of social media platforms themselves and not on the underlying motivations and tactics that have brought today's foreign intelligence agencies to target digital citizens within the social media sphere.

The topic of foreign intelligence operations in social media offers researchers the opportunity to bring the historic activities of intelligence professionals into the broader public discussion. To date, much of the available information surrounding intelligence operations in social media has solely focused on their immediate effects as well as the emotional responses to them, rather than focusing on the histories and processes behind them. In order to produce more fruitful discussion around this topic, this paper will examine cases from past and recent foreign intelligence operations that will illuminate today's expanded intelligence environment.

[12] Office of the Director of National Intelligence, *2019 National Intelligence Strategy of the United States.*

Main Theme and Chapter Themes

The goal of this paper is to answer the question of how modern foreign intelligence agencies apply classical intelligence techniques to the modern sphere of social media. In order to answer this question, this paper will employ the method of case study and give the reader visibility into the historical influences on the strategies that are currently being used to influence American values, perceptions, and beliefs. Because intelligence operations often result in compelling narratives and are ultimately a series of interlinking processes, the case study method was chosen to examine this topic.

To thematically divide the content of the following three chapters, each chapter will be devoted to one of America's most notable intelligence adversaries. Specifically, this paper will examine the ways in which three of America's foreign intelligence agencies (Russia, Iran and China) use social media to incorporate and enhance traditional foreign intelligence techniques in their modern operations. In terms of choosing which nations to study, these nations were chosen based on their high amount of publicly available information, the adversarial nation's relevance to US foreign policy, and the nation's consistent ranking as a US intelligence priority. Though many nations collect intelligence on the United States, the adversarial nations of Russia, Iran and China possess not only the intent, but also the proven capability to carry out sophisticated foreign intelligence campaigns through social media. For these reasons, Russia, Iran, and China were chosen as the nations for analysis within the following chapters.

This paper is organized into this introductory chapter, three chapters of analysis, and a concluding chapter. Each of the following analytical chapters will center its case study narratives around a single country and then highlight a specific intelligence

technique which has been observed in modern social media operations carried out by the specific country. The ensuing chapters will perform this analysis by comparing two cases of intelligence operations for each country: one operation conducted during a pre- or nascent social media era, and one operation conducted in a post-social media environment. By performing this case study analysis, this paper will help researchers and members of the public better understand the current intelligence operational environment and provide a starting point for future intelligence research.

The first chapter will explore the Russian technique of covert influence in the various forms it has taken when employed to target American voters during federal political elections. After reviewing relevant literature and providing historical background regarding Russia's covert influence machinery, this chapter will compare two case studies of Russian electoral interference. The first case will examine Russia's covert influence efforts directed against the 1984 US presidential election, and the second case will examine Russia's covert influence efforts directed against the 2016 US presidential election. Comparative analysis of these cases will examine the common intelligence techniques utilized in these influence campaigns, with particular focus on how social media enabled Russian intelligence services to apply certain techniques to target specific segments of the American civilian populace in 2016. Suggestions for future research will conclude the study of Russia's use of social media to pursue its foreign intelligence goals.

The second chapter will explore Iran's use of the honey trap technique. After providing information to familiarize the reader with the honey trap technique and the modern world of Iranian cyber operations, this chapter will compare two case studies: the

Iranian regime's use of a real-life honey trap to lure prospective intelligence assets, in the form of defector Monica Witt, and Iranian intelligence's use of a digital honey trap, in the form of the digital persona Mia Ash. Comparative analysis considers the declining risks to intelligence officials themselves when employing digital honey traps versus employing human honey traps in more traditional HUMINT operations, thus the attractiveness of social media platforms that afford users anonymity for foreign intelligence services. This chapter will conclude with recommendations for future research into Iran's weaponization of social media.

The third chapter will explore what is arguably one of the most damaging intelligence activities conducted by Chinese intelligence: agent recruitment. First, this chapter will define relevant intelligence terms and provide historical insight into prototypical Chinese recruitment techniques. Next, this chapter will examine two agent recruitment operations conducted by Chinese intelligence services in before and after the rise of social media. The case of Chinese American Peter "Wen-Ho" Lee will serve as the first case study, and the case of former CIA case officer Kevin Mallory will serve as the second. Comparative analysis of these cases will show that social media significantly enhanced the recruitment process when Kevin Mallory was recruited through the professional networking site LinkedIn by enabling remote access to the target in a manner that was difficult for counterintelligence professionals immediately to detect. The case analysis will be followed by recommendations for future research of Chinese intelligence operations in social media.

The following three analytical chapters will address ways in which one of America's intelligence adversaries has enhanced a classical intelligence technique using

social media. Although this is a broad and complex issue, the case studies throughout the next three chapters have been chosen in order to properly highlight the most pertinent intelligence techniques that are characteristic of their respective nations.

Situation of the Paper Among Existing Intelligence Research

Intelligence and national security studies research is a field that has become international in scope and increasingly diverse in its scholarly approaches. Due to the covert nature of many intelligence activities, there are many barriers to conducting studies of intelligence operations for security studies scholars performing unclassified research.

While many barriers exist when it comes to publicly accessing classified intelligence, one subset of intelligence which should be mentioned when addressing intelligence operations in social media is the concept of open source intelligence (OSINT). When used by the Intelligence Community, OSINT is the collection of publicly available information which is synthesized and analyzed to contribute to finished intelligence products. OSINT has been a recognized subset of intelligence for some time, but in recent years, it has undergone several changes, mostly pertaining to the expansion of publicly available data and the ensuing need for a more concise definition of this intelligence practice.[13] As publicly available data sources have expanded, some researchers have argued that the methodologies behind OSINT collection require more concise refinement as well.[14] The collection of publicly available information from social media falls under the broad definition of OSINT. Much can be said about the intricacies

[13] Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, Santa Monica, CA: RAND Corporation, 2018, Accessed November 24, 2019, https://www.rand.org/pubs/research_reports/RR1964.html.
[14] Ibid.

of open source research and how it has changed intelligence collection practices. However, for the purposes of this paper, the following chapters of analysis will primarily analyze specific traits and characteristics of social media as a single OSINT collection vector.

Outside of OSINT, much of intelligence itself remains compartmented and distanced from academic and private sector researchers. In order to study this topic, the majority of intelligence researchers employ a historical or cultural approach. Researchers like Michael Warner,[15] Mark Phythian[16] and Christopher Andrew[17] have produced extensive overviews of entire intelligence services using these approaches. Some intelligence agencies, like Britain's MI-5, have granted seemingly unfettered access to their archives.[18] In other cases, archival research takes the form of an ethnographic postmortem of fallen intelligence regimes. Katherine Verdery's ethnographic research into Romania's former Securitate took advantage of the fall of Romania's Soviet-run security state and uncovered not merely the intelligence the Securitate had collected on her, but also files which revealed the inner-workings and social relations of Romania's intelligence service.[19]

Outside of legitimate access to intelligence archives, there are also instances where illegitimate access has increased the public's cultural knowledge and awareness of how intelligence agencies operate. Although defectors vary in their degrees of access and

---

[15] Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington, DC: Georgetown University Press, 2014).
[16] Mark Phythian, *Understanding the Intelligence Cycle* (Milton Park, Abingdon, Oxon: Routledge, 2013).
[17] Christopher M. Andrew, *The Secret World: A History of Intelligence* (New Haven: Yale University Press, 2018).
[18] Harold Leigh, "The Defence of the Realm: The Authorized History of MI5 by Christopher Andrew," *Guardian,* October 9, 2009, https://www.theguardian.com/books/2009/oct/10/defence-of-the-realm-mi5.
[19] Katherine Verdery, *Secrets and Truths: Ethnography In the Archive of Romania's Secret Police*, (Budapest: Central European University Press, 2014).

reliability, it cannot be denied that intelligence researchers greatly benefit from the firsthand accounts of foreign defectors. Figures such as Vasili Mitrokhin, Litvinenko and Sergei Tretyakov, have all published valuable archives of classified information which have benefited researchers as well as the United States as a whole, sometimes leading to the discovery of vast spy networks as was the case with Tretyakov's assistance in the expulsion of Russia's illegals.[20]

In addition to using historical and cultural approaches, some researchers approach the study of intelligence from a cross-disciplinary perspective. One cross-disciplinary approach to intelligence which some researchers have used is the examination of the psychology of spying and how this psychology has altered from a pre- to post-social media world.[21] Other researchers have used a cyber research approach to examine the broad ways in which technology plays a role in America's foreign intelligence collection.[22]

Additionally, some technology researchers are starting to focus their efforts on social media in particular and the legalities of its role as a platform for US foreign intelligence collection.[23] Notably, the vast majority of intelligence research which addresses social media's role has a very American-centric focus. This may be due to the fact that America's intelligence agencies are more widely known than others and also relatively transparent in terms of government oversight. The study of ethics in

---

[20] Fred Weir, "Kremlin official issues death threat in Russian spy scandal. Is the KGB coming back?" *CSMonitor*, November 12, 2010, https://www.csmonitor.com/World/Europe/2010/1112/Kremlin-official-issues-death-threat-in-Russian-spy-scandal.-Is-the-KGB-coming-back.

[21] Danielle A. Hayes, "The Trusted Insider: Motives, Behaviors, Fictions, and Digital Age Norms," *American Intelligence Journal* 35, no. 2 (July 2018): 17–25.

[22] Candace N. Stevens, "Technology in Foreign Intelligence Gathering," *American Intelligence Journal* 34, no. 1 (January 2017): 123–30.

[23] Steven C. Henricks, "Social Media, Publicly Available Information, and the Intelligence Community," *American Intelligence Journal* 34, no. 1 (January 2017): 21–31.

intelligence and particularly, the ethics of social media intelligence collection and its possible regulation has also entered the discussion in American intelligence studies literature.[24] However, as other nations detect what they believe to be interference in their elections and other domestic affairs, international publications of intelligence research with a social media focus is growing within this field of study.[25]

Regardless of which countries or agencies are studied, it is important that researchers continue to examine the central tenets of the intelligence profession through modern lenses. Namely, it is important for researchers to ask key questions regarding which quintessential aspects of this profession have changed and which practices have remained the same as intelligence operations have entered the digital sphere. Now that many spies have migrated their covert communications from secure landlines to encrypted messaging applications, it is important to examine which aspects of classical tradecraft inform today's intelligence practitioners. Although many Americans are now aware that Russia and other nations collect massive amounts of information using online sources and methods, precisely what foreign intelligence agencies do with this information and how they use classical human targeting techniques are topics which necessitate further discussion. From a cultural perspective, it is important that researchers consider which digital intelligence techniques are unique to the American experience, which techniques apply to other nations, and which techniques are universal.

In late 2016, the United States Senate attempted to make sense of a slew of seemingly related and absolutely disconcerting events, which appeared to be linked to a

[24] Nicole A. Softness, "Social Media and Intelligence: The Precedent and Future for Regulations," *American Intelligence Journal* 34, no. 1 (January 2017): 32–37.
[25] Carme Colomina, "La Desinformación de Nueva Generación: Cinco Escenarios Políticos y Geoestratégicos Ante El Fake," *Anuario Internacional CIDOB*, January 2019, 61.

coordinated digital intelligence operation which targeted the presidential election. In the search for answers on behalf of the American people, the Senate not only called upon America's top three intelligence services for help, they also called upon America's social media providers, whose CEOs were called to testify in congressional hearings.[26] It is doubtful that Zuckerberg was aware of all of the ramifications that would result from the social network he created in his college dorm room in the early 2000s, but there is no doubt that in the aftermath of the 2016 presidential election, Zuckerberg and the rest of America confronted several harsh realities about social media. Most notably, Americans confronted the dual reality that while social media has the power to bring all of the world's citizens together, the 'real world' includes all of the world's terrorists, traitors and spies.

Prior to the election of 2016, there was very little research which addressed social media's dual reality or even the possibility of adversarial intelligence services using social media as a weapon. Given the increasing number of covert operations that are conducted on social media and the relatively unproductive public discussion, it is clear that policymakers, citizens and academicians are still lacking clarity in certain areas, particularly in the technical aspects of these operations.[27] Apart from the technical aspects, the history of foreign intelligence services and their previous campaigns against American interests is something that is often glossed over or addressed in a sentence or two. This issue was highlighted in the July 2018 congressional response to the 2017

[26] Sheera Frenkel and Linda Qiu, "Fact Check: What Mark Zuckerberg Said About Facebook, Privacy, and Russia," *New York Times,* April 11, 2018, https://www.nytimes.com/2018/04/10/technology/ zuckerberg-elections-russia-data-privacy.html.
[27] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements." U.S. House of Representatives Permanent Select Committee on Intelligence. U.S. Senate. Accessed November 30, 2019. https://intelligence.house.gov/social-media-content/.

Intelligence Community Assessment (ICA).[28] Although Congress seemed to value and appreciate the US Intelligence Community's joint efforts to produce valuable unclassified materials, Congress noted that the historical narratives, terminology and language which informed the intelligence operations of 2016 was noticeably absent from the 2017 ICA.[29] Given the remaining interest in the historical context of intelligence operations, it is important that future research into intelligence operations in social media illuminates the longevity and continuity of intelligence through historical comparisons.

As the following chapters will show, there are numerous lessons from historical examples which can shed light on what is going on within social media's platforms. This paper will compare past and recent case studies which highlight how social media is used to update classical intelligence techniques that are favored by specific intelligence agencies. At the conclusion of the case studies, this paper will make recommendations for American intelligence researchers. These recommendations will combine this paper's research stemming from the history of intelligence with an updated analysis of the technological nuances of digital intelligence operations in the age of social media. Although not all of the public's questions will be answered in the following pages, this paper will demonstrate how intelligence operations were structured in the past, how intelligence operations have changed due to social media, and how, in many ways, intelligence operations have remained the same.

[28] U.S. Senate Select Committee on Intelligence, *Initial Findings on Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections*, 115th Cong., 2d sess., 2018.
[29] U.S. Senate Select Committee on Intelligence, *Initial Findings on Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections.*

CHAPTER 1
Russian Intelligence in Social Media

In 2015, the American Ambassador to Germany stated that the Russian disinformation machine was a $400 million dollar media campaign in over 100 countries.[30] One year later, the harsh reality of this statement confronted American citizens when it appeared that Russia was attempting to influence the 2016 US Presidential Election.[31] It began with reports that a server linked to the Democratic National Convention (DNC) had been hacked. Days after the hack, a trove of documents from the DNC server was published online.[32] Shortly thereafter, false online personas and groups began to emerge on various social media sites, seemingly out of nowhere. What appeared to be the common link amongst all of this activity was America's Cold War opponent, Russia. What was not discussed in the immediate aftermath of all of this activity, was whether this kind of malign influence had occurred before.

An examination of Russia's intelligence history reveals that 2016 was not the first time that Russia has directed its intelligence resources against an American presidential election. This essay will argue that Russia sought the same methodological doctrine and used the same active measures techniques against presidential elections in the Cold War and in 2016. However, the advent of cyber tools created more avenues of execution and enhanced the most recent Russian influence activities in 2016. In both eras, Russia sought

---

[30] John B. Emerson, "Exposing Russian Disinformation," News and Events, US Embassy and Consulates in Germany, accessed July 23, 2018, https://de.usembassy.gov/exposing-russian-disinformation/.
[31] US Department of Homeland Security, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* (Washington DC: DHS Press Office, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.
[32] Tom Hamburger and Karen Tumulty, "WikiLeaks releases thousands of documents about Clinton and internal deliberations," *Washington Post,* July 22, 2016, https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/.

to denigrate one American presidential candidate over another and to exploit internal social and political fissures in the United States. Beyond its tactical goals, Russia utilized several common techniques in the Cold War and in 2016. Although Russia uses a wide variety of covert influencing techniques, there are several which have been identified and assessed to be the most integral to the Russian intelligence apparatus. These techniques are part of what Russia calls 'active measures.' Several active measures techniques include the use of front groups, agents of influence, kompromat, and forgeries. In spite of continuing systemic change, analysis will show how the four techniques described above have defied regime change, persisted through bloody revolutions and been reinvigorated by digital innovation.

Analyzing these historic intelligence techniques is critical if American intelligence professionals do not want to repeat mistakes of the past. For this reason, this chapter will perform a critical comparison of Russia's historic and modern covert influence machinery. Apart from explaining common tactical goals, this paper will examine the continuity of Russian intelligence techniques. After examining Russia's historical covert influence techniques and defining key terms, this chapter will highlight the modern applicability of classical covert influence techniques by situating them within case studies. Case studies are one of the best ways to identify commonalities, highlight continuities and trace complex processes. This chapter will examine an American presidential election during the Cold War and the most recent American presidential election of 2016. In both of these elections, Russian covert influence played a key role in defining the Russian covert measures canon. Ensuing case study analysis will highlight

important concepts and provide recommendations for future researchers and intelligence practitioners.

Literature Review

Historical and interdisciplinary sources can greatly assist in the analysis of any political phenomenon. Active measures is a topic that has been addressed by historians, government researchers, cyber experts and perhaps most importantly, by Russian intelligence practitioners themselves. In order to properly situate the case studies, we will first examine the origins, definitions and central tenets of the Russian covert influencing method of active measures.

History of Active Measures

The Russian term *aktivinyye meropriyatiya,* or active measures, has no direct equivalent in the English language.[33] Clinical terms like "psychological warfare" and colloquial terms like "dirty tricks" have attempted to capture some of its meaning, but no single English word adequately situates 'active measures' within the Western intelligence lexicon.[34] While many definitions exist, researchers Shultz and Godson in their book *Dezinformatsiya: The Strategy of Soviet Disinformation* provide one of the most concise definitions, describing active measures as, "An array of overt and covert techniques for influencing events and behavior in and the actions of foreign countries."[35] Providing a more detailed definition is Soviet defector Vasili Mitrokhin*,* who defines active measures in his book *The KGB Lexicon* as, "Agent-operational measures aimed at exerting useful

[33] Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 224.
[34] Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View* (Washington: Pergamon-Brassey, 1985), 43.
[35] Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington: Pergamon-Brassey, 1984), 2.

influence on aspects of the political life of a target country which are of interest, its foreign policy, the solution of international problems, misleading the adversary, undermining and weakening his position, the disruption of his hostile plans, and the achievement of other aims."[36]

In terms of longevity, active measures have been an integral component of Russian statecraft for centuries. One hundred years before the Cold War began, the Czarist secret police (Okhrana) used a wide range of active measures to quell internal dissident groups and penetrate émigré dissident organizations in other countries.[37] Decades later, the Bolsheviks relied heavily upon a combination of propaganda and political influence techniques to advance their political agenda.[38] Shultz and Godson write that it was this unique combination of covert influence techniques that spurned a "logical outgrowth" of Soviet active measures techniques during the Cold War.[39] Regime after regime, dictator after dictator, the practice of active measures eventually became inextricable from Russia's intelligence culture.

The significant impact of active measures upon US-Soviet relations led Ronald Reagan to create the Active Measures Working Group (AMWG).[40] The group's task was to research active measures and suggest ways that America could counter its negative effects.[41] In a report from 1987, researchers from the AMWG delineated some of the most common techniques of active measures. Their list included the use of front groups,

---

[36] Vasili Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook,* (London: Routledge, 2002), 7.
[37] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Strategic Perspectives*, No. 11 (June 2012): 9.
[38] Shultz and Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, 17.
[39] Ibid.
[40] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications," 66-67.
[41] Ibid.

covert broadcasting, forgeries, agents of influence, manipulation, disinformation, forgeries, and overt propaganda.[42] Apart from these 'soft' measures, the AMWG noted that active measures could also extend into more violent activities, including covert actions toward incitement, targeted assassinations, and terrorism.[43] In one of their most seminal reports from 1987, the AMWG wrote that, "Active measures are distinct both from espionage and counterintelligence, and from traditional diplomatic and informational activities."[44] While espionage traditionally entails an intelligence officer covertly collecting information pertaining to foreign countries, active measures entails an officer or agent disseminating information (both overtly and covertly) in order to influence foreign countries, corporations and individuals.

In the Cold War, active measures were the responsibility of Service A within the First Chief Directorate of the *Komitet Gosudarstvennoy Bezopasnosti* (KGB).[45] Service A also coordinated operations with the International Department (ID) of the Soviet Communist Party Central Committee.[46] In a report from 1987, American intelligence analysts estimated that there were up to 15,000 KGB officers dedicated to "disinformation and psychological warfare efforts" (two practices that fall under active measures).[47] As for the day-to-day schedules of KGB employees, Vasili Mitrokhin reported that Line PR officers (KGB officers stationed in foreign residencies) were

[42] US Department of State, The Active Measures Working Group, *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987,* 1987, viii.
[43] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications," 66-67.
[44] The Active Measures Working Group, *Soviet Influence Activities*, viii.
[45] Max Holland, "The Propagation and Power of Communist Security Services Dezinformatsiya," *International Journal of Intelligence and Counterintelligence* 19, no. 6 (2009): 1-31, doi:10.1080/08850600500332342.
[46] The Active Measures Working Group, *Soviet Influence Activities*, viii.
[47] Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia And Europe: Implications for U.S. National Security,* 115th Cong., 2nd sess., 2018, S Rep. 115-21, 37.

required to devote twenty-five percent of their time to active measures.[48] In terms of financing these activities, the CIA estimated that the KGB spent $4 billion dollars a year in the 1980s on active measures (roughly $8.5 billion in today's dollars).[49]

It is important to note that while journalists and academicians within the Anglosphere still use the term 'active measures' its use has been deprecated in its native country and replaced by the term *meropriyatiya sodeistviya* ("support measures").[50] According to researchers from the International Centre for Defence and Security (ICDS) the public use of the newer term can be traced to a 1992 legal document.[51] However, in spite of the change in nomenclature, the ICDS researchers concluded that, "Support measures are the direct successors of active measures, and merely a new and politically correct term formulated after the fall of the Soviet Union."[52] For the purposes of analysis, the traditional term of 'active measures' will be used in order to avoid confusion and also as acknowledgment of the lack of current research on the later term.

Unique Characteristics of Russian Active Measures

Although the United States carries out psychological operations, these are usually included in the American definition of 'covert measures' which do not include the prototypical Russian overt practices of propaganda and state-sponsored media outlets.[53] Similarly, the French General Directorate for External Security (GDES) has an 'Action Division' which carries out some of what Americans would consider 'covert action' but

[48] Andrew and Mitrokhin, *The Sword and the Shield*, 224.
[49] Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy*, 37.
[50] Ivo Juurvee, "The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox," *Strategic Analysis* (April 2018): 1-8, The European Centre of Excellence for Countering Hybrid Threats, 2.
[51] Ibid., 3.
[52] Ibid.
[53] Frank L. Goldstein and Benjamin F. Findley, *Psychological Operations: Principles and Case Studies,* (Maxwell Air Force Base, Ala.: Air University Press, 1996), 5.

is more similar to the special military operations of Navy SEALs than the intelligence operations of James Bond.[54]

Apart from differences in terminology, there are various characteristics which distinguish Russia's active measures doctrine from the prototypical covert action doctrine of its western counterparts. Shultz and Godson wrote that one distinguishing characteristic is that "the means utilized in Soviet active measures are virtually unlimited" whereas Western intelligence services "are constrained by major cultural, political, and moral considerations."[55]

Another distinguishing characteristic is the question of when active measures or covert actions are applied, or more specifically, when each culture *feels* they should be applied. National security law expert M.E. Bowman writes that while Americans view covert action as an adjunct to war-time activities, any attempts to "surreptitiously influence (or change) another country during peacetime is difficult for us to countenance."[56] This doesn't mean that covert action isn't exercised during peacetime, but simply that its covert nature runs counter to American tenets of openness and transparency. Soviet tradition, however, provides a deep-rooted justification for the application of active measures in almost any context. As Leonard Schapiro explains, "The use of an overwhelming military presence and the maximum espionage and subversion presence are part of what has always been described in Soviet terminology as

[54] Gérald Sawicki, "Aux origines lointaines du "service action". Sabotage et opérations spéciales en cas de mobilisation et de guerre 1871-1914", *Revue Historique des Armées* Vol 13, Issue 268 (August 2012): 21.
[55] Shultz and Godson, *Dezinformatsiya: Active Measures in Soviet Strategy, 16.*
[56] M.E. Bowman, "Secrets in Plain View: Covert Action the U.S. Way," In *The Law of Military Operations: Liber Amicorum Professor Jack Grunawalt,* edited by Michael N Schmitt, (Newport, R.I.: Naval War College Press, 1998), 3.

'ideological struggle' which is repeatedly asserted as the necessary concomitant of 'peaceful coexistence'."[57]

Other distinguishing characteristics of the Russian active measures doctrine include its infallible secrecy and its tight concentration of decision-making power within the Russian intelligence apparatus. Although largely obfuscated from public view, American covert action has stringent statutory reporting requirements as stipulated by the Hughes-Ryan Amendment of 1974[58] and the Intelligence Authorization Act of 1991.[59] The Hughes-Ryan Amendment specifically requires the CIA to report all covert actions to no less than eight congressional committees (four in each house) which equates to roughly sixty congress members plus their staff.[60] This decentralized authority structure, coupled with American media practices, lends itself to a relatively transparent system compared to its Russian equivalent. In modern Russia, former Soviet spy Alexander Litvinenko has reported that when the KGB was dissolved and the Russian intelligence apparatus was no longer under the microscope of the Communist Party, the various security agencies began "operating in Russia absolutely independently and totally unchecked."[61]

Another distinguishing characteristic of the Russian active measures doctrine is the objective of using active measures to deceive, create confusion and internally demoralize targeted nations, largely through propaganda.[62] This contrasts with the stated

---

[57] Leonard Schapiro, "Totalitarianism in Foreign Policy," In *The Soviet Impact on World Politics*, edited by Kurt London, (New York, N.Y.: Hawthorn Books, 1974), 8.
[58] Foreign Assistance Act of 1974, Public Law 93-559, 93rd Cong., 2d sess. (December 30, 1974).
[59] Intelligence Authorization Act, Fiscal Year 1991, Public Law No: 102-88, 102nd Cong., 2d sess. (August 14, 1991).
[60] M.E. Bowman, "Secrets in Plain View: Covert Action the U.S. Way," 15.
[61] Alexander Litvinenko and Yuri Felshtinsky, *Blowing Up Russia: The Secret Plot to Bring Back KGB Terror* (New York: Encounter Books, 2007), xxi.
[62] Bittman, *The KGB and Soviet Disinformation,* 2.

ideals of America's covert propaganda efforts, which Loch K. Johnson writes as being painted more as "giving a helping hand" in order to promote equality and freedom.[63] One example of this covert helping hand was the American effort to support the Christian Democratic party in Italy after the Second World War.[64] The resultant outcomes of each side's covert operations can be politically and emotionally interpreted as positive or negative, but the intentions of each nation are notable for their contrasts.

Active Measures Techniques

Although the Russian active measures spectrum is wide, some techniques have received more public attention more often than others.[65] Four techniques are notable not only for their wide usage but also for their specific usage against American presidential elections. These include the techniques of agents of influence, front groups, kompromat, and forgery. Because these terms are likely unfamiliar to anyone outside the Intelligence Community, we will examine each one individually before analyzing their applications within specific case studies.

Agents of Influence

First, when defining agents of influence, it is important to distinguish agents of influence from traditional espionage agents, just as the AMWG distinguished active measures from more 'traditional' espionage activities. According to a 1992 report from the AMWG, "Agents of influence are foreigners who have been recruited by the KGB in

[63] Loch K. Johnson. "The Enduring Myths of Covert Action," *Virginia Policy Review* 7, no. 2 (Winter 2014): 61.
[64] Ibid.
[65] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* Vol. 15, Issue 1 (Winter 2015): 15.

order to be used to influence the opinions of foreign publics and governments."[66] While traditional espionage agents are tasked purely with collecting information regarding events that are happening around the world, agents of influence are tasked with a more active role in changing world events. However, in both cases, the agent's affiliation with a foreign intelligence agency remains secret. During the Cold War, agent of influence operations were some of the most difficult active measures operations to identify, since many agents of influence were perceived by their fellow countrymen as loyal patriots expressing opinions that were entirely their own.[67] Agents of influence were also often tasked to operate within their own social circles, but "for greater effect, they often [were] integrated with penetration of enemy groups."[68]

Front Groups

Another tool within the Russian active measures toolbox is the use of front groups. Front groups or front organizations are also used to exert influence over a nation, a group of persons or an individual, and they are often political in nature.[69] However, front groups can also purport to be philanthropic or social organizations. Regardless of their function, these groups are never publicly affiliated with the Russian government.[70] During the Cold War, some of the most prominent Soviet front organizations were the World Peace Council, the World Federation of Trade Unions, the International Union of

[66] US Department of State, United States Information Agency. 1992. *Soviet Active Measures in The 'Post-Cold War' Era 1988-1991: A Report Prepared at the Request of the United States House of Representatives Committee on Appropriations by the United States Information Agency.*
[67] Ibid.
[68] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications," 9.
[69] Shultz and Godson, D*ezinformatsiya: Active Measures in Soviet Strategy,* 107.
[70] Ibid., 106.

Students, the Christian Peace Conference and the International Association of Democratic Lawyers.[71]

Kompromat

In addition to the 'softer' measures of using agents and front groups there is the more aggressive technique of *kompromat* (or compromising information). When a Cold War operation required more offensive measures against a person or group of persons, the KGB often turned to the collection of kompromat to provide the mechanism towards a swift public downfall.[72] Sources of kompromat which KGB agents were encouraged to find included hidden pasts, private habits, or any character traits that could be considered socially deviant.[73] When no legitimate compromising material could be found, it was simply concocted and then published through whichever news outlet would accept it as true. Kompromat was and is such a deeply entrenched and common practice in Russian political warfare that today there is a website dedicated to cataloguing the salacious stories collected by political opponents called 'kompromat.ru.'[74]

Forgery

In order to present fabricated kompromat or any other lies that would benefit Russia's foreign interests, the Russian intelligence apparatus often turns to forgeries.[75] Forgeries can serve a myriad of purposes, but are usually directed towards one of two purposes: to fabricate denigrating 'evidence' against a singular target of active measures or to falsify official government documents that would suggest wrongdoing on the part of

[71] Shultz and Godson, D*ezinformatsiya: Active Measures in Soviet Strategy,* 26.
[72] Malcolm W. Nance, *The Plot to Hack America: How Putin's Cyberspies and Wikileaks Tried to Steal the 2016 Election* (New York, NY: Skyhorse Publishing, 2016), 48.
[73] Ibid.
[74] Ibid., 49.
[75] Bittman, *The KGB and Soviet Disinformation*, 90.

an entire nation.[76] The former type of forgery was often used to augment kompromat. The latter type was described by Ladislav Bittman as "slightly 'improved' copies of genuine government documents that were anonymously distributed among American, Western European, or Third World journalists" which were met with varying degrees of acceptance.[77]

The American Target of Active Measures

Although Russian active measures were directed against many countries during the Cold War, numerous Soviet defectors, including Vasili Mitrokhin and Sergey Kondrashev labeled the United States as the 'main enemy'[78] or the 'main target'[79] of the KGB's active measures campaigns, even at the peak of détente.[80] At a conference for senior KGB officers in January 1984, the goals of active measures were discussed, which mostly included frustrating American imperialism, discrediting America and exposing its weaknesses.[81] Exploiting internal fissures that tore at the social fabric of the United States was also viewed as one of the most effective ways to weaken the 'main enemy' from within.[82] Some of the most notable instances where active measures were used against the United States included KGB-created conspiracy theories surrounding President Kennedy's assassination[83] and the false origin story of the AIDS virus.[84] Over the course of the twentieth century, the KGB utilized active measures against a variety of

[76] Shultz and Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, 150.
[77] Bittman, *The KGB and Soviet Disinformation*, 218.
[78] Tennent H. Bagley, *Spymaster: Startling Cold War Revelations of a Soviet KGB Chief.* (New York: Skyhorse Publishing, 2015), 120.
[79] Andrew and Mitrokhin, *The Sword and the Shield,* 224.
[80] Christopher M. Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations From Lenin to Gorbachev* (New York, NY: HarperCollins Publishers, 1990), 539.
[81] Andrew and Mitrokhin, *The Sword and the Shield*, 224.
[82] Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy*, 36.
[83] Andrew and Mitrokhin, *The Sword and the Shield*, 246.
[84] Bagley, *Spymaster : Startling Cold War Revelations of a Soviet KGB Chief*, 120.

targets including Martin Luther King,[85] J. Edgar Hoover,[86] and numerous American political officials who supported anti-Soviet measures in the halls of Congress and abroad.

Active Measures and US Presidential Elections

In addition to undermining America's foreign policy and domestic society, the KGB viewed American presidential elections as fair game in the arena of active measures. However, depending upon the perceived level of American animosity, the KGB could be strategically reserved. Soviet Ambassador Anatoly Dobrynin wrote that while the Communist Politburo was always cognizant of the American presidential election for its effect on US-Soviet relations, the Politburo never intervened or expressed a preference publicly, since this might have more of a detrimental than positive after effect.[87] The KGB on the other hand, did attempt to influence American elections through various active measures campaigns, most of which had a low rate of success.

In 1960, Soviet influence on American elections took the form of gifts, caviar and a proposal for financial backing of two-time failed presidential candidate Adlai Stevenson.[88] Stevenson, known for his unapologetic stance against nuclear weapons testing, was viewed as highly amenable to Soviet interests.[89] When Stevenson was approached in January of 1960, he thanked Soviet Ambassador Mikhail Menshikov for the Soviet's appreciation of his views, but to Stevenson's inner circle and written in his

---

[85] Andrew and Mitrokhin, *The Sword and the Shield*, 236.
[86] Ibid., 234.
[87] Anatoly Dobrynin, *In Confidence: Moscow's Ambassador to America's Six Cold War Presidents (1962-1986)* (New York: Times Books, Random House, 1995), 176.
[88] John Bartlow Martin, *Adlai Stevenson and the World: The Life of Adlai Stevenson* (Garden City: Doubleday & Company, 1977), 473.
[89] Arthur E. Rowse and Harold Kellock, "Foreign Policy in National Elections," *Editorial Research Reports 1960,* vol. II (1960): 543-62.

memoirs, he called the approach "highly improper, indiscreet, and dangerous to all concerned."[90]

In 1968, Ambassador Dobrynin was tasked with approaching Democratic candidate Hubert Humphrey with an offer to subsidize his campaign in order to keep the anti-Soviet, anti-communist Nixon out of the White House.[91] Humphrey declined and to the chagrin of Soviet leadership, Nixon was elected.[92] However, Nixon's policy of détente proved to be far better than what Soviet leaders had anticipated. Their appeasement was cut short however, when Nixon was impeached for actions that Dobrynin considered to be "a fairly natural thing to do. Who cared if it was a breach of the Constitution?"[93]

In 1976, Dobrynin wrote in his diary that a different American politician came under the eye of the Politburo. Conservative Democrat Henry ("Scoop") Jackson had a political track record of opposing the Soviet Union, particularly on its Jewish emigration policies and he seemed poised to gain the Democratic presidential nomination.[94] Mark Kramer with *PONARS Eurasia* writes that after Jackson won the Massachusetts and New York primaries, the KGB officially launched an active measures campaign against him to prevent his entrée into the White House.[95] The campaign primarily revolved around using fabricated kompromat to paint Jackson as a closeted homosexual (a trend that continues into the twenty-first century with world leaders like France's Emmanuel Macron being

[90] Martin, *Adlai Stevenson and the World*, 473.
[91] Andrew and Mitrokhin, *The Sword and the Shield*, 239.
[92] Ibid.
[93] Ibid.
[94] Dobrynin, *In Confidence,* 334.
[95] Mark Kramer, "The Soviet Roots of Meddling in U.S. Politics," *PONARS Eurasia Policy Memo* No. 452, George Washington University (January 2017), 4.

targeted).[96] KGB agents went as far as to send forged FBI letters to various American newspapers and journalists with relevant 'evidence' of his sexual orientation.[97] The KGB was so determined to keep Jackson from entering the White House that even after he dropped out of the presidential race, they continued their disinformation campaign against him.[98]

Until his bid for presidential reelection in 1984, Ronald Reagan managed to avoid the most aggressive tactics on the KGB's active measures spectrum. However, when he got precariously close to securing the Republican nomination in 1976, Mitrokhin writes that the KGB began searching for kompromat on the California governor, who had never touted anything close to détente in any of his political speeches.[99] Reagan failed to win the 1976 Republican nomination and instead, the seemingly peaceable Jimmy Carter was sworn in as the next American president, but he was accompanied and guided by a hardline national security advisor, Zbigniew Brzezinski.[100]

In 1980, the KGB was "less involved" in attempting to influence the presidential election than four years earlier, since they were (in the words of Ambassador Dobrynin), "Fed up with Carter and uneasy about Reagan."[101] Without a great deal of voter support and no Soviet smear campaigns, Reagan managed to win the Republican nomination and the presidency. However, during Reagan's first term when he followed his campaign's anti-Soviet rhetoric with forceful executive action, he found himself back in the KGB's

---

[96] Shehab Khan, "Emmanuel Macron 'A Psychopath Who Hates France', Russian Media Says", *Independent*, 2017, https://www.independent.co.uk/news/world/europe/russian-media-emmanuel-macron-french-president-general-election-2017-gay-psychopath-hates-france-a7723531.html.
[97] Kramer, "The Soviet Roots of Meddling in U.S. Politics," 4.
[98] Ibid.
[99] Andrew and Mitrokhin, *The Sword and the Shield,* 242.
[100] Ibid.*,* 241.
[101] Ibid., 242.

crosshairs. On February 25, 1983, the Centre (KGB headquarters) announced it would be launching an aggressive, multi-channel active measures campaign to prevent Reagan's reelection which would mostly consist of searching for sources of kompromat and finding any and all means to share it.[102] Ultimately, Reagan won 49 out of 50 states, securing him an overwhelming 1984 election victory and demonstrating the limited reach of the KGB's influence machinery and the dwindling power of the Soviet Union. In terms of active measures campaigns, it would be the last attempt to influence American elections for years.

Modern Active Measures

In the 1990s under President Yeltsin, the KGB was dismantled like a house of cards with its cadre reshuffled into disparate agencies.[103] For years after the end of the Cold War, Yeltsin's government made the strategic decision to exploit regional conflict in order to exact influence, rather than devote Russia's precarious government funds towards massive external propaganda campaigns.[104] With Russia's intelligence services in missional limbo, on December 31, 1999 Yeltsin resigned amidst accusations of mismanagement and corruption.[105] Shortly after his resignation, the practice of active measures was almost immediately reinvigorated thanks to a sixteen-year KGB veteran who initially found himself as the acting prime minister and later the elected president of Russia.[106]

---

[102] Andrew and Gordievsky, *KGB: The Inside Story*, 589.
[103] Mark Galeotti, "Russian Intelligence is at (Political) War," *NATO Review*, May 11, 2017, https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/EN/index.htm.
[104] Fiona Hill and Pamela Jewett, "Back in the USSR": Russia's Intervention in the Internal Affairs of the Former Soviet Republics and the Implications for United States Policy Towards Russia," *Brookings* (January 1994): 86, Ethnic Conflict Project.
[105] Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy,* 10.
[106] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," 8.

The resurgence of Russian active measures cannot be discussed without discussing President Vladimir Putin. Since his successful bid for election in 2000, Putin has created what Olga Kryshtanovskaya and Stephen White call a 'militocracy' by saturating the Russian government with former state security employees, referred to as *siloviki*.[107] Putin's intricate realignment of power has mirrored the Cold War culture of his predecessors to such a degree, that some have called his regime a "neo-KGB state."[108]

Whether he is using active measures to attack democratic systems, weaken peaceful transatlantic alliances or exploit other countries' internal conflicts in order to provide Russia with more power and political advantages on the world stage, it appears that Putin has integrated KGB doctrine into Russia's modern intelligence practices.[109] One of the most effective ways that modern Russian intelligence agencies have accomplished this is by leveraging new cyber tools to attack enemy states during their election seasons.[110]

Numerous democracies have shown symptoms of what they believe stems from Russian interference in their electoral processes.[111] For our purposes of study, the most pivotal case of post-Cold War Russian electoral interference occurred in 2016 during the American presidential election. Although previous attempts to influence post-Cold War elections have been quiet operations of small-scale propaganda campaigns, the 2016 American presidential election showed an unprecedented demonstration of force which

---

[107] Olga Kryshtanovskaya and Stephen White, "Putin's Militocracy," *Post-Soviet Affairs* 19, no. 4 (2003): 292, doi:10.2747/1060-586x.19.4.289.
[108] "The Making of a Neo-KGB State", *Economist*, June 25, 2007, https://www.economist.com/briefing/2007/08/23/the-making-of-a-neo-kgb-state.
[109] Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy*, 9.
[110] Ibid., 37.
[111] Ibid., 113.

has shocked several other nations into bolstering the security surrounding their own electoral processes.

The inherently covert nature of active measures has always made it difficult for researchers (particularly those outside the intelligence community) to verify and make definitive judgments regarding their impact on current events. Additionally, the lack of post-Cold War defector accounts and Russian intelligence service handbooks limits the number of primary sources used for verification. In spite of these limitations, various intelligence assessments,[112] cyber security reports[113] and congressional testimony[114] have all corroborated the assessment that the 2016 U.S. presidential election was the latest and most devastating manifestation of Russian active measures directed against the United States. There is also little doubt that with the advent of cyber tools, the scope of active measures tactics has grown wider than it was during the Cold War.[115]

As modern instances of Russian intelligence influence are investigated by governments, more information is now available for comparative research. Several think tanks,[116] non-governmental organizations[117] and international organizations[118] are also dedicating fiscal and human capital towards the identification of Russian active measures

---

[112] US National Intelligence Council, Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections,* January 06, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[113] Dmitri Alperovitch, "Bears in The Midst: Intrusion into The Democratic National Committee," *CrowdStrike* (blog), June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
[114] *Hearing Before the United States Senate Committee on the Judiciary Subcommittee on Crime and Terrorism,* 115th Cong., (2017) (statement of Colin Stretch, General Counsel, Facebook).
[115] Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy*, 8.
[116] Christopher Paul, and Miriam Matthews, "Russia's "Firehose of Falsehood" Propaganda Model," *Perspectives* (July 2016):1-16, https://doi.org/10.7249/PE198.
[117] "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," *Freedom House,* November 2017, https://freedomhouse.org/report/freedom-net/freedom-net-2017.
[118] Keir Giles, "Handbook of Russian Information Warfare," *NATO Defense College Research Division*, (November 2016): 1-90, http://www.ndc.nato.int/news/news.php?icode=995.

tactics in the twenty-first century. However, there is still a pressing need for trend identification, quantitative analysis and modern theory development in the study of Russian active measures in a digital society.

Methodology

To test the theory that the same techniques of Russian active measures were used during the Cold War and are still being used today, we will examine two active measures campaigns as case studies. The case study method provides a framework for analyzing complex phenomena across a variety of fields, but it is particularly well-suited for process tracing. The cases to be studied are the active measures campaigns carried out against the targets of the 1984 and 2016 US presidential elections.

In terms of case selection criteria, the following attributes were reasons for case selection: data richness, resemblance of case background conditions, prototypicality of case background conditions, and intrinsic importance. First, the cases were selected due to their comparatively high coverage in academic research and government reporting. Although the research literature addresses other Cold War instances of Russian active measures used against the American political system, the lack of source diversity and the dearth of corroborative reporting eliminated additional cases from this examination. Second, the cases being studied had similar targets of active measures. That is, both active measures campaigns were directed towards the American presidential election process. Third, the cases were chosen for their prototypicality. They were prototypical both in terms of their antecedent conditions which consisted of the American electoral process and in the resulting active measures campaigns that exemplify central tenets of the Russian active measures doctrine. Lastly, the cases were selected for their intrinsic

importance and resemblance to current situations of policy concern. Foreign interference has been a prolonged topic of discussion within the American legislature and a high priority for the U.S. Intelligence Community ever since the 2016 election.[119] Although case studies of other nations might also benefit American political researchers, it was imperative in this paper that the selected cases address the current climate of concern regarding the 2016 American presidential election.

We will present the cases chronologically and use a narrative framework that is intended to illuminate the underlying goals and resulting active measures techniques employed in both cases. First, we will present the background and tactical goals for commencing the active measures campaign. We will then present the techniques that were observed in both instances. Lastly, we will address the election outcomes in both instances. This is not an examination of effectiveness or political impact. Rather, the comparative method of case study will allow us to assess whether common tactical goals and techniques were used in both eras. This analytical framework will not only lay the groundwork for our process analysis, but also for future analysis of Russian active measures campaigns in other democracies.

Case Study #1 The 1984 U.S. Presidential Election

Background

Our first case study concerns Ronald Reagan's 1984 US presidential race and the active measures enacted by the KGB that attempted to prevent his reelection. Although Soviet active measures were heightened and especially targeted against Reagan in 1984,

[119] Mike Eckel, "U.S. Senate Committee Backs Intelligence Findings on Russian Meddling," *Radio Free Europe*, 2018, https://www.rferl.org/a/senate-committee-russian-interference/29336790.html.

the KGB had been monitoring the career of the Californian politician for years prior to his reelection.

Reagan initially caught the attention of the KGB during the Republican primaries of 1975 .[120] Reagan's public rhetoric was so unabashedly anti-Soviet that the Centre believed that if he was elected president, he might be anti-Soviet enough to launch one of the nuclear weapons that the Americans were undoubtedly stockpiling.[121] To prepare for such a situation, the KGB initiated a series of soft active measures, mostly involving research and collection of kompromat, in 1976.[122] These efforts were stalled when Reagan lost the Republican nomination to incumbent Gerald Ford.[123]

Four years later, when it was presented with anti-Communist Reagan or Jimmy Carter's aggressively anti-Soviet National Security Advisor Zbigniew Brzezinski, the KGB was at an impasse.[124] In an uncharacteristic bout of reticence, Soviet leadership waited on the sidelines to see who would win the election. The KGB would later regret this decision, as Ronald Reagan would take on an even more aggressive stance against the Soviet Union than his democrat predecessor.[125]

After their strategic restraint from using active measures during the 1980 presidential election, the Centre's number one objective for the 1984 election was clear: prevent Ronald Reagan from being elected for a second term.[126] Vasili Mitrokhin assessed that it was likely the strong desire for discrediting Reagan's administration which led the chairman of the KGB to announce on April 12, 1982 that all foreign

[120] Andrew and Mitrokhin, *The Sword and the Shield*, 242.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Ibid.
[126] Ibid., 243.

intelligence officers now had to participate in active measures (even those not assigned to Service A).[127] Roughly a year later, on February 25, 1983, the Centre announced it would be launching an aggressive, multi-channel active measures campaign specifically against Ronald Reagan.[128]

Kompromat

The previously collected kompromat on Reagan that had lain dormant for years was approved to be disseminated through mass media channels. While any source of negative information can serve as kompromat, one of the issues which KGB focused on was the possibility that Reagan's father's alcoholism affected Reagan's current health.[129] Although Regan later commented in his memoirs about the strain of his father's alcoholism on his family, this was not viewed as a smoking indictment against the person of Ronald Reagan.[130] The Centre also assessed that Reagan possessed "weak intellectual capabilities," but this was not a central tenet of most of their anti-Regan materials.[131] Instead, they relied more strongly on amplifying his political aggression as they crafted articles that were published in Denmark, France and India.[132] All of their efforts were not futile, as some of the KGB's negative press gained some traction abroad, but ultimately it failed to take hold in the United States.[133]

Agents of Influence

To bolster the scraps of kompromat the KGB possessed on Reagan, the Centre called upon its three American residencies (embassies where KGB agents operated) in

[127] Andrew and Mitrokhin, *The Sword and the Shield*, 243.
[128] Andrew and Gordievsky, *KGB: The Inside Story*, 589.
[129] Andrew and Mitrokhin, *The Sword and the Shield*, 242.
[130] Ibid.
[131] Ibid.
[132] Ibid.
[133] Ibid.

Washington D.C., New York, and San Francisco. The American residencies were ordered to obtain contacts in both political party's headquarters and on the staffs of all possible presidential candidates.[134] For additional assurance, residencies outside the United States were required to send any agents they could who would be willing to assist.[135] The goal of acquiring these contacts and bringing in additional agents was to find any pertinent information on Reagan and procure personal channels for its dissemination.[136] Unfortunately, primary sources are lacking with regards to the efficacy of any agent of influence operations in 1980. However, the lack of reporting suggests that this requirement was either not fulfilled or bore little fruit since no agents of influence came forward and no reports regarding suspected Soviet agents were published by either campaign after the election.

Front Groups

In addition to kompromat and agents of influence, the KGB also used front groups in their attempt to hinder Regan's chances of reelection. The benefit of using front groups was that similar to Soviet agents of influence, their ties to the Centre were still obfuscated, but their geographic coverage and political influence could also provide clear advantages to any Soviet smear campaign.[137] As part of the active measures campaign against Reagan, the KGB ordered its front groups to spread the political slogan "Reagan means war!"[138] Though the slogan was not very popular, any modicum of anti-American sentiment expressed abroad was attributed by the KGB as a sign of success.[139] In spite of

[134] Andrew and Gordievsky, *KGB: The Inside Story*, 590.
[135] Ibid.
[136] Andrew and Mitrokhin, *The Sword and the Shield*, 243.
[137] Shultz and Godson, *Dezinformatsiya: Active Measures in Soviet Strategy,* 108-109.
[138] Christopher M. Andrew and Oleg Gordievsky, *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985* (London: Hodder and Stoughton, 1991), 97.
[139] Loch K. Johnson, *Strategic Intelligence* (Westport, Conn.: Praeger Security International, 2007), 52.

many Soviet front groups' recognition by reputable bodies such as the United Nations, UNESCO and the United Council of Churches, Soviet efforts in this campaign failed to influence the key demographic of American voters.[140] According to Reagan's biographer Edmund Morris, Reagan was successful in swaying the Soviet populace when he unabashedly labeled the Soviet Union as 'an evil empire' in his 'Crisis of Confidence' speech delivered on March 9, 1983.[141] Within twenty-four hours, Westerners in Moscow reported that a reaction of "self-disgust and self-acknowledgment" spread throughout Russian society against their own government.[142]

Forgery

When compromising information, personal influence and political slogans were ineffective, the dissemination of forged pieces of information was a common active measures tactic. In *Instructions from the Centre,* Christopher Andrew and Oleg Gordievsky note that Service A's forgeries against the Reagan administration were generally of two kinds: 'silent forgeries' shown in confidence to Third World leaders or not-so-silent forgeries that were intended to promote media campaigns.[143] During his first term, Reagan was the subject of repeated forgeries, one of the most notorious being a fabricated letter to the King of Spain, urging the European leader to quickly "remove the forces obstructing Spain's entry into NATO."[144] Copies of this letter were mailed to Spanish journalists as well as all delegates (except the Americans) attending the Madrid Conference on Security and Cooperation in Europe (CSCE).[145] The letter made reference

[140] Loch K. Johnson, *Strategic Intelligence* (Westport, Conn.: Praeger Security International, 2007), 52.
[141] Edmund Morris, *Dutch: A Memoir of Ronald Reagan* (New York: Modern Library, 1999), 474.
[142] Ibid.
[143] Andrew and Gordievsky, *Instructions from the Centre*, 97.
[144] Ibid.
[145] Ibid.

to a 'highly secret' memorandum which was also fabricated by the KGB and also circulated along with the letter.[146] Due to its crude presentation, the letter had negligible impact and several Spanish journalists publicly accused them of being of Soviet origin.[147]

Summary

The 1984 Election active measures campaign failed to detract from Reagan's popular appeal with American voters. Like several other Cold war active measures campaigns its perceived effectiveness was overinflated by KGB operatives. Christopher Andrew further notes that, "The limitations of KGB active measures were illustrated by the failure of a single Residency in a NATO country to popularise the principal slogan "Reagan means War!"[148] Reagan won 49 out of 50 states in the electoral college, which secured him a second term and additional resources towards his anti-Soviet policies.[149] By any standard, the 1984 election active measures campaign was not viewed as a success.

Case Study #2 The 2016 U.S. Presidential Election

Background

In 2016, more than thirty years after the 1984 US Presidential Election, America was going to the polls to elect a new commander in chief. During this election cycle, the three primary candidates were Republican Donald Trump, Democrat Hillary Clinton and third-party candidate Bernie Sanders. Like the active measures campaign during the 1984

[146] Andrew and Gordievsky, *Instructions from the Centre*, 99-100.
[147] Ibid.
[148] Ibid., 97.
[149] Anthony Bennett, *The Race for the White House from Reagan to Clinton: Reforming Old Systems, Building New Coalitions* (New York: Palgrave Macmillan, 2013), 78.

election, the active measures directed towards the 2016 election were planned well in advance of Election Day.

Kompromat

Just like in 1984, soft active measures in the form of kompromat collection began in September 2015, when the FBI contacted the Democratic National Committee (DNC) to inform them that one of their computers had been hacked by a Russian cyber actor.[150] In November 2015, the FBI contacted the DNC again, to report that one of their computers was now actively transmitting information back to Russia.[151] On June 14, 2016 the *Washington Post* reported that Russian hackers gained access to DNC servers which included documents pertaining to opposition research on Donald Trump.[152] A day later, an unknown blogger named Guccifer took credit for the hack, claiming to be a Romanian hacktivist who was unaffiliated with Russian intelligence.[153] A week later, Wikileaks published nearly 20,000 emails online that had been exfiltrated from the DNC server.[154]

Although cyber hacking can be used for a variety of criminal and intelligence gathering purposes, the deliberate targeting and pursuant publication of the personal emails and documents from the DNC server was labeled by many as a clear instance of

[150] "2016 Presidential Campaign Hacking Fast Facts," *CNN*, July 18, 2018, https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.
[151] Ibid.
[152] Ellen Nakashima, "Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump," June 14, 2016, *Washington Post,* https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?hpid=hp_rhp-banner-main_dnc-hackers-1145a-banner%3Ahomepage%2Fstory&utm_term=.e8bf3382d30a.
[153] Threat Connect Research Team, "Guccifer 2.0: The Man, The Myth, The Legend?", *ThreatConnect* (blog), July 20, 2016, https://www.threatconnect.com/blog/reassesing-guccifer-2-0-recent-claims/.
[154] "2016 Presidential Campaign Hacking Fast Facts."

kompromat.[155] In December 2016, it was discovered that several Republican party servers were also hacked and exfiltrated. However, these documents were never made public; a fact that supported a later U.S. Intelligence Community assessment that the Russian influence campaign sought to denigrate Hillary Clinton rather than Donald Trump.[156]

Agents of Influence

As a means to spread their collected kompromat, Russia employed several digital versions of classical agents of influence. According to the U.S. Intelligence Community Report *Russian Interference in the 2016 Election,* Russia integrated this technique into a longstanding messaging strategy, which historically involved a blend of agents of influence, cutouts and front organizations.[157] In 2016, this specifically entailed the use of "third-party intermediaries and paid social media users or "trolls."[158]

Unlike agents of influence used during the Cold War, most of these agents did not actually exist. The majority consisted of fake online personas created by the Internet Research Agency, a company owned by Yevgeny Prigozhin, who is one of Vladimir Putin's close friends.[159] Several news outlets have gotten interviews from former Internet Research Agency employees who have worked in Russia's notorious 'troll factories' where employees were instructed on how to pose as real Americans and then post and propagate social media content that is favorable to Russia's foreign and domestic

[155] Nance, *The Plot to Hack America*, 49.
[156] Jim Sciutto and Pamela Brown, "Russia Hacked GOP Groups, US Intel Believes," *CNN*, December 12, 2016, https://www.cnn.com/2016/12/12/politics/gop-russia-hacking-trump/.
[157] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, 2.
[158] Ibid.
[159] *United States v. Internet Research Agency LLC et. al.,* indictment, 19 (2018).

agenda.[160] While some personas claimed to be Americans like the Southern, right-wing Twitter personality Jenna Abrams, others claimed to be foreigners who were seeking the truth amidst the American election, like Guccifer 2.0.[161] In addition to the notable fake personalities, there were thousands of automated agents of influence, otherwise known as 'bots' created by the Internet Research Agency that were mostly deployed to tweet and retweet on the social media outlet Twitter. Research by the cyber security firm FireEye found that Russian bots successfully made one of Russia's fake hashtags ("#HillaryDown") listed as 'trending' on Twitter, meaning that it garnered enough public attention to be listed on the Twitter homepage.[162]

Front Groups

In addition to creating fake individuals, Russia utilized digital front groups as well. Most of the front groups were created on the popular social media platform of Facebook where they garnered tens of thousands of 'likes' until the group pages were removed by Facebook administrators.[163] In terms of their efficacy to influence the American electorate, two front groups on opposite ends of a civil rights issue both managed to physically rally their followers to protest against each other outside an Islamic center in Houston, Texas.[164] One front group called 'Heart of Texas' had 250,000 followers and a tagline of "Homeland of guns, barbeque and your heart."[165] The other

---

[160] Sam Matthew, "Revealed: How Russia's 'Troll Factory' Runs Thousands of Fake Twitter and Facebook Accounts to Flood Social Media with Pro-Putin Propaganda," *Daily Mail*, March 28, 2015, http://www.dailymail.co.uk/news/article-3015996/How-Russia-s-troll-factory-runsthousands-fake-Twitter-Facebook-accounts-flood-social-media-pro-Putinpropaganda.html.
[161] "Guccifer 2.0: The Man, The Myth, The Legend?"
[162] Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.
[163] Ryan Lucas, "How Russia Used Facebook To Organize 2 Sets of Protesters," *NPR*, November 1, 2017, https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters.
[164] Lucas, "How Russia Used Facebook To Organize 2 Sets of Protesters."
[165] Ibid.

group that Russia managed to mobilize was called 'United Muslims of America' and had 328,000 followers and a tagline of "I'm a Muslim, and I'm proud."[166]

Forgery

Cementing all of these methods together was a novel remediation of the method of forgery. Of the two forgery methods used against the Reagan Administration, which included silent forgeries sent to world leaders and forgeries intended for mass media, the 2016 forgeries more closely resemble the latter approach. In 2016, forgery was not used to paste together fake letters to be viewed by a single reader. Rather, it was used to create an air of legitimacy within social media, whose inherent data infrastructure renders information provenance and a writer's true identity next to impossible to discern.[167] In an indictment filed on February 16, 2018, Special Counsel Robert Mueller and his team stated that from at least April 2016 through November 2016 Russian actors purchased advertisements on Facebook using false personas.[168] They then began to produce, purchase, and post these fake advertisements on other social media sites which expressly advocated for Trump or expressly opposed Clinton.[169] Instead of the slogan "Reagan Means War!" there was a constant stream of hashtags that were attached to various social media posts. Some hashtags used included "#Hillary4Prison" and "#NeverHillary".[170] Over the course of the congressionally mandated review of fake Russian accounts after the election, Facebook's analysts found "approximately $100,000 in ad spending from June of 2015 to May of 2017 — associated with roughly 3,000 ads — that was connected

[166] Lucas, "How Russia Used Facebook To Organize 2 Sets of Protesters."
[167] Geoffrey Barbier, *Provenance Data in Social Media* (San Rafael: Morgan & Claypool), 2013, 8.
[168] *United States v. Internet Research Agency LLC et. al.*, indictment, 19 (2018).
[169] Ibid.
[170] Ibid.

to about 470 inauthentic accounts."[171] They also reported that the falsified accounts "appeared to focus on amplifying divisive social and political messages across the ideological spectrum — touching on topics from LGBT matters to race issues to immigration to gun rights."[172]

Summary

As news of alleged Russian interference continued to circulate, the outgoing President Barack Obama directed the Intelligence Community to perform a full review of what happened during the 2016 election process.[173] To the general public, it may have initially seemed as though Russia had only used covert influence against the 2016 presidential election.[174] However, after examining the 1984 and 2016 elections side by side, several commonalities are apparent between Russia's Cold War and modern approaches.

Case Study Analysis

From the two case studies above, several classical techniques emerge in common. Kompromat is one technique that Russia used to denigrate American presidential candidates. As seen in the case studies, the use of kompromat is similar in both cases, but the ability to acquire kompromat and the ability to deny attribution has been enhanced greatly by cyber hacking tools.[175]

---

[171] Alex Stamos, "An Update on Information Operations on Facebook," *Facebook* (blog), September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/.
[172] Ibid.
[173] Tal Kopan, Kevin Liptak and Jim Sciutto, "Obama Orders Review of Russian Election-Related Hacking," *CNN, December 9, 2016, https://www.cnn.com/2016/12/09/politics/obama-orders-review-into-russian-hacking-of-2016-election/index.html.*
[174] "Discussion with CIA Director Mike Pompeo," FDD National Security Summit (repr., Washington D.C.: Foundation for Defense of Democracies, 2017), http://www.defenddemocracy.org/events/fdds-national-security-summit/.
[175] Justin Key Canfil, "Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity," *Journal of International Affairs* 70, no. 1 (Winter 2016): 219.

Another technique is the use of front groups. Although the KGB was known to have front groups embedded all across America and most certainly in Washington throughout the Cold War, they were not always capable of delivering the compromising material requested by Moscow.[176] Cold War-era front groups were usually confined to physical groups of people, which required physical presence and an inevitable paper trail. The numerous fake Facebook groups created in 2016 however, came in and out of existence within the span of several months and without a single publicly available document to verify their origins.

A third technique, similar to that of front groups is the use of agents of influence. Although the KGB requested that its agents of influence gain contacts on the presidential campaign staffs in 1984, there has not been any evidence to suggest that this was successfully carried out. However, in 2016 when a young American girl named Jenna Abrams started publishing political charged tweets on Twitter shortly before the election, she garnered significant attention from politicians, journalists and the American public.[177] Abrams engaged in Twitter arguments with former U.S. ambassador to Russia and Russian propaganda expert Michael McFaul, she was retweeted by Mike Flynn Jr. and was also mentioned in stories featured in the *Washington Post* and *The New York Times*.[178]

Lastly, the technique of forgery was used in both cases to present false information that was advantageous to Russian interests. In the 1984 election, forgeries

[176] Bittman, *The KGB and Soviet Disinformation*, 3.
[177] Ben Collins and Joseph Cox, "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media And The World," *Daily Beast,* November 2, 2017, https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.
[178] Ibid.

took the physical form of official government letters. In the 2016 election, forgeries evolved to suit the digital medium and provided Russian front groups with the appearance of legitimacy within the social media sphere.

Conclusion

The Russian influence campaign of 2016 warrants not only a historical review of active measures used against American elections as we have done here, but also a forward-looking assessment. Although they appear to be the heir apparent of active measures, how are 'support measures' organized and assigned? Are cyber hackers the new spies? In what areas are old traditions abandoned and where are they stridently indoctrinated into the next generation?

This chapter is intended to shine light upon the continuum of active measures techniques that have been seen in the 1984 and 2016 U.S. presidential elections. The United States has had historical successes in exposing Russian forgeries,[179] identifying agents of influence[180] and countering the actions of Russia's international front groups.[181] However, with the fall of the Berlin Wall, much of the US Intelligence Community's awareness and vigilance against Russian covert influence was lost.

The 2016 Presidential Election reminded the US Intelligence Community and Congress of the reality of foreign interference in American electoral processes and it initiated a series of inquiries, investigations and public discourse. However, in spite of all of the new information that has come to light, in July 2018, the Select Senate Committee

---

[179] John M. Goshko, "For Forgery Specialist, A Case Close to Home," *Washington Post,* August 19, 1986, https://www.washingtonpost.com/archive/politics/1986/08/19/for-forgery-specialist-a-case-close-to-home/4b8db266-699c-4557-8f01-93db86500599/?utm_term=.8b82773c0db6.
[180] Waller, Michael J., *Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare* (Washington, DC: Institute of World Politics Press, 2009), 215.
[181] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications," 46.

on Intelligence found the 2017 US Joint Intelligence Assessment's coverage of "the historical context of Russian interference in U.S. domestic politics perfunctory."[182] In other words, policymakers appear to understand the recent findings from the 2016 active measures campaign, but feel there is a blatant lack of historical contextualization to assist in the government and the public's understanding of the modern Russian intelligence machinery.

While there are many insights that American citizens and policymakers can glean from the events of 2016 and the ensuing congressional research, one aspect stands out. This aspect is what former CIA Director Mike Pompeo called 'strategic understanding.' Developing a strategic understanding of Russian active measures techniques can help politicians, American voters and the Intelligence Community prepare for attempts to influence future elections. During the Cold War, numerous Soviet defectors pointed out the need for Western intelligence services (the United States, in particular) to reexamine and reevaluate Russian intelligence tactics and to weigh this against Russia's potential for political subversion.[183]

As evidenced by the Senate findings, there is a general need for public awareness of the history of active measures which synthesizes this history with the future, particularly with regards to cyberspace. Over thirty years before the 2016 US Presidential Election, Soviet defector Ladislav Bittman shared some prescient predictions in his book *The KGB and Soviet Disinformation : An Insider's View:*

---

[182] U.S. Senate Select Committee on Intelligence, *Initial Findings on Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections*, 2018.
[183] Anatoliy Golitsyn, *New Lies for Old: The Communist Strategy of Deception and Disinformation* (repr., New York: Dodd, Mead, 1984).

> Computers are another source of valuable operational data for the KGB. Their use for storing, processing and transferring sensitive data about individuals in private sectors, such as banking and medicine and state or federal revenue sectors, opens new fields for Communist intelligence services. KGB operatives in the United States are very interested in computer encoding research both military and civilian. Access to this magic key would enable the KGB to penetrate the privacy of almost every American without getting involved in risky and time-consuming operations. More important, the KGB would be able to pollute the computer system with disinformation about individuals or companies, seriously damage their lives and paralyze their operations. (209-210)[184]

The openness of the Internet benefits Americans just as much as it benefits America's enemies. Any American who engages in the digitized, interconnected world should be aware that while the collective spaces of the Internet are free and open, they are not always populated by genuine truth-tellers and allies. As hackers, terrorists and spies co-author history's current chapter of digital covert action, it is imperative that the world's citizens are made aware of Russia's historical attempts to undermine American institutions so that future targets of active measures will not be doomed to repeat mistakes of the past.

[184] Bittman, *The KGB and Soviet Disinformation,* 209-210.

CHAPTER 2
Iranian Intelligence in Social Media

The previous chapter of this paper examined Russia's historical and current covert influence campaigns and the effects of social media on their preferred covert influence tactics. With so much coverage devoted to Russia, many Americans are ignorant of the broad spectrum of operations conducted by one of America's most persistent adversaries in the digital realm: the nation of Iran. Over the past two decades, operating under the cloak of proxy actors and virtual private networks, Iran has built a reputation as a formidable cyber power. Within the US Intelligence Community Iran is known for launching brutal cyberattacks against American government entities, corporations, and individuals.

In recent years, Iran has started to favor the use of a specific classical espionage technique in its cyber operations. The digital revival of this technique has allowed Iran's malicious cyber actors to not only target computer systems and critical infrastructure, but also humans. The technique which Iran is incorporating into its cyber toolbox is the honey trap. Honey traps typically involve the use of an alluring intelligence officer who is used to entice unwitting adversaries into sharing secret information through the leveraging of a personal (and sometimes romantic) relationship. Today, the classic honey trap collection technique has become digitized and is quickly becoming a hallmark of Iran's intelligence collection strategy.

The Internet and social media have affected governments around the world in different ways. One way that these new technologies have affected governments is in the ability to digitize information. Formerly physical formats of classified documents are now generated, edited, and disseminated within networked digital environments, which

sometimes bleed over into various sectors of society. Apart from the digitization of classified documents, it is also becoming apparent that former physical manifestations of an intelligence officer's identity are now manifest in the form of bits and bytes, scattered across digital space, and waiting to be discovered by cyber-savvy adversaries. Nowhere is this more apparent than the Internet spaces of social networking sites.

Although many social networking sites have outed Russia for its malicious Internet activity, Iran is proving to be just as dangerous in social media. As this chapter's analysis will show, Iran's cyber actors are equally skilled at persuading social media users to believe false information, infiltrating secure computer systems, and causing damage that ranges from slightly detrimental to gravely damaging to US national security.[185] Because Iran's malicious use of social media is growing and is proving to be damaging to individuals, companies, and governments, it is a worthy topic of study for modern intelligence researchers.

Due to a current lack of knowledge regarding the threat of Iranian foreign intelligence operations in social media, this chapter will seek to provide an enhanced understanding of this issue in the form of case studies. The case study method is an effective approach for isolating process steps and highlighting pertinent details. This chapter will present two case studies where Iranian actors successfully engaged unwitting social media users and used digital honey traps to gain access to sensitive information. The first case illustrates Iran's self-generated use of a fake, but attractive-looking digital persona, which was used to gain persistent access to corporate computer networks. The second case illustrates a hybridized version of the honey trap, which incorporates both

[185] Donara Barojan, "Eight Takeaways from Iranian Information Operations," *AFCEA*, April 1, 2019, https://www.afcea.org/content/eight-takeaways-iranian-information-operations.

digital personas and a real human behind it, in the form of American defector to Iran, Monica Witt.

Ensuing analysis will compare the cases, highlight online security concerns for social media users and suggest lines of future research. Due to the national security threat posed by this malicious activity, it is imperative that social media users with access to sensitive or classified data are made aware of this threat and are equipped with the knowledge to defeat it. By critically examining Iran's preference for certain intelligence collection techniques in social media, US intelligence agencies, academic institutions and private individuals can better protect themselves and preserve national security in an increasingly digitized world.

Literature Review

In terms of research on traditional intelligence tradecraft and digital honey traps in social media, there is very little open source literature that addresses both of these topics in tandem. However, a great deal of research has been devoted to analyzing the topics of traditional honey traps, digital identity deception, and the targeting of individuals online (also known in cyber parlance as 'spear phishing'). A review of the current research within these areas will help to situate the following case studies and ensuing analysis.

Traditional Honey Traps

The Oxford Dictionary defines a honey trap as, "A stratagem in which an attractive person entices another person into revealing information or doing something unwise."[186] Within this broader definition there are varying approaches and methodologies employed by foreign intelligence agencies and resistance movements

[186] *Oxford Dictionary*, s.v. "Honey Trap," accessed May 25, 2019, https://en.oxforddictionaries.com/definition/honeytrap.

throughout history. Although the majority of human intelligence is gathered through the vector of rapport-based, real life relationships, the honey trap adds a specific layer of enticement that is highly tailored to the target. From the renown and eventual execution of seductress Mata Hari, to the lesser known cadre of East German male seducers known as "Romeo spies," the honey trap has historically been applied by various nations with varying degrees of success.[187]

Several authors have tangentially addressed the topic of honey traps as part of a historical examination of women in intelligence. This is likely due to the culturally ingrained association of females with the honey trap technique. Long before the Cold War and going back to ancient times, women have often been cast as the seducers within honey trap operations. The Biblical story of Sampson and Delilah lays out the archetypal honey trap scenario of an unwitting male who is smitten by a female tasked with obtaining secret information. This classical female honey trap archetype has been used over multiple centuries and in various cultures. The formalized honey trap operations that the world knows today were likely not developed until the hiring of female intelligence officers. It has been argued by some historians, that this formalized technique of intelligence gathering did not take hold until the First World War, when today's modern intelligence bureaucracies were in their infancy.[188] In both World War I and World War II, women were hired to play a critical role in intelligence gathering for both sides. Their success was largely due to their unsuspecting demeanors and their rapid grasp of spy tradecraft. After the two World Wars gave way to the Cold War, more complex and long-

[187] Markus Wolf, *Man Without a Face: The Autobiography of Communism's Greatest Spymaster* (New York: PublicAffairs, 1999), 136.
[188] Tammy M. Proctor, *Female Intelligence: Women and Espionage in the First World War* (New York: New York University Press, 2003), 2.

term honey trap operations were directed against male, female, heterosexual, and homosexual targets.[189]

One of the most notorious agencies to employ honey traps was Russia's KGB, which used male agents (called 'uncles') to manage either female prostitutes or female KGB employees (both referred to as 'swallows'). The 'uncles' were tasked with instructing 'swallows' on the best methods for seducing male targets and obtaining high quality foreign intelligence. These activities could range from rifling through the contents of an American intelligence officer's suitcase or obtaining secret information regarding the United States' future plans for NATO.[190] Although the CIA has publicly denied using honey traps, its British counterpart, MI-6 regularly used honey traps during the Cold War. At the Eve Club on Regent Street in London, a cadre of women were hired to lure unsuspecting Soviet diplomats and businessmen into divulging state secrets.[191] Today, classical honey traps remain a viable intelligence gathering option, though many intelligence agencies continue to deny using this method. However, some of the most recent honey trap accusations have been leveled against the Chinese intelligence services.[192]

Iranian Intelligence: From Political to Digital Revolution

Although non-state sponsored groups can form loose intelligence agencies, it can be difficult to build an efficient intelligence bureaucracy without the backing of a

---

[189] Phillip Knightley, "The History of the Honey Trap," *Foreign Policy,* March 12, 2010, https://foreignpolicy.com/2010/03/12/the-history-of-the-honey-trap/.
[190] Richard Tahair, *The Encyclopedia of Cold War Espionage, Spies, and Secret Operations,* (Westport: Greenwood Press: 2004), 127.
[191] Ibid., 128.
[192] David Chazan, "French Spy Facing Charges 'was snared by Chinese honeytrap," *Telegraph*, May 27, 2018, https://www.telegraph.co.uk/news/2018/05/27/french-spy-snared-chinese-honeytrap-faces-treason-charges/.

national government. When governments are in turmoil, intelligence agencies often have to make very hard choices with the goal of self-preservation. After years of political upheaval and a consolidation of various government agencies, in August 1983, Iran's Ministry of Intelligence and Security (MOIS) was created in order to set new intelligence priorities and streamline Iran's fractured intelligence community. After its initial formation, MOIS was charged with collecting intelligence on Iran's foreign and domestic enemies and carrying out various covert missions in support of the Iranian regime. Today, the Iranian Revolutionary Guard Corps (IRGC) (responsible for military intelligence) and the Quds force (responsible for intelligence collection abroad) also serve as supplemental intelligence collection agencies which work in tandem with MOIS.[193] The IRGC is also known for supporting foreign client organizations via the Quds Force. These foreign client organizations also serve as proxies for carrying out foreign operations and expanding Iranian influence in the Middle East region.[194]

In terms of its HUMINT operations, Iran's focus is largely turned towards the United States and its neighboring countries.[195] Iran also listed the nation of Iraq amongst its intelligence enemies after the US-led invasion in 2003, as well as several other Shi'a-majority countries and countries with unpopular Sunni rulers.[196] Similar to many other intelligence agencies, Iran uses diplomatic cover for a lot of its intelligence officers. Iran has also been known to be somewhat haphazard in its tradecraft, with many of its diplomatic officers being exposed over the years. Lately, Iran has also directed its

[193] Library of Congress - Federal Research Division, "Iran's Ministry of Intelligence and Security: A Profile," December 2012, 15, https://fas.org/irp/world/iran/mois-loc.pdf.
[194] Udit Banerjea, "Revolutionary Intelligence: The Expanding Intelligence Role of the Iranian Revolutionary Guard Corps." *Journal of Strategic Security* 8, no. 3 (Fall 2015): 100.
[195] Library of Congress - Federal Research Division, "Iran's Ministry of Intelligence and Security: A Profile," 33.
[196] Ibid.

HUMINT operations towards Latin America, where it exploits networks of Shi'a individuals to report on Iranian interests in the Southern Hemisphere.[197]

Apart from its HUMINT operations, Iran has been slowly building its cyber capabilities not only within its military cadre, but also within its intelligence cadre. The impetus for this can be traced back to 2010, when the Stuxnet virus shook Iranian centrifuges. This caused Iran to devote government funding to the creation of a Supreme Council of Cyberspace (*Shora-ye Ali-ye Fazo-ye Majazl*), which would eventually coordinate all of Iran's cyber programs, bolster its national defenses, and supplement its intelligence collection efforts.[198] That same year, Iran also established a Cyber Defense Command (*Gharargah-e Defa-e Saiberi*) that was tasked with defending Iranian critical infrastructure.[199] Ever since 2010, Iran has continually enhanced its cyber resources.

The most critical aspect of Iran's cyber program for the purposes of this paper, is its encroachment into the traditional sphere of HUMINT operations. As more Iranian intelligence operations are analyzed and brought under public scrutiny, it is clear that Iran is demonstrating an increasing preference for combining modern cyber tools with specific techniques of traditional HUMINT tradecraft. Listed among these techniques is the honey trap, which will be explored more in-depth in the case studies to follow. Although Iran's malicious cyber activity has been seen in malicious email campaigns and computer network exploitation, it is becoming more and more prevalent within the human-centric platform of social media.

---

[197] Library of Congress - Federal Research Division, "Iran's Ministry of Intelligence and Security: A Profile," 33.
[198] Carl Anthony Wege, "Iranian Counterintelligence," *International Journal of Intelligence and CounterIntelligence* 32, no. 2 (April 3, 2019): 283. doi:10.1080/08850607.2019.1565274.
[199] Ibid., 282.

Identity Deception and Social Media

Deception, as defined by Buller and Bulgoon's Interpersonal Deception Theory, is "a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver."[200] In a digital context, several theories have emerged to explain how deception, and particularly identity deception, is perpetuated in social media.

Several studies on identity deception online have highlighted the role of the truth bias and the halo effect as contributors to the success of online identity deception.[201] The truth bias is the assumption that everyone is telling the truth.[202] This bias diminishes social media users' ability to detect when someone is lying about their identity. The halo effect stems from classical psychology and involves the formation of positive judgments about individuals based upon positive first impressions.[203] In digital media, the halo effect has been studied in reference to social norm violations. In one study, an individual's early violation of a powerful social norm tainted a group's positive view of the individual, in spite of the individual's pro-social and norm-abiding actions after their initial violation.[204]

---

[200] David B. Buller and Judee K. Burgoon, "Interpersonal Deception Theory," *Communication Theory* 6, Issue 3, (August 1, 1996): 203–242, https://doi-org.proxy1.library.jhu.edu/10.1111/j.1468-2885.1996.tb00127.x

[201] Catherine Friend and Nicola Fox Hamilton, "Deception Detection: The Relationship of Levels of Trust and Perspective Taking in Real-Time Online and Offline Communication Environments," *CyberPsychology, Behavior & Social Networking* 19, no. 9 (September 2016): 532–37. doi:10.1089/cyber.2015.0643.

[202] Charles F. Bond and Bella M. DePaulo, "Accuracy of Deception Judgments," *Personality and Social Psychology Review* 10, no. 3 (August 2006): 214–34, doi:10.1207/s15327957pspr1003_2.

[203] Harold H. Kelley, "The Warm-Cold Variable in First Impressions of Persons," *Journal of Personality* 18, no. 4 (June 1950): 431. doi:10.1111/j.1467-6494.1950.tb01260.x.

[204] Hwanseok Song, Jonathon P. Schuldt, Poppy L. McLeod, Rhiannon L. Crain, and Janis L. Dickinson, "Group Norm Violations in an Online Environmental Social Network: Effects on Impression Formation and Intergroup Judgments," *Group Processes & Intergroup Relations* 21, no. 3 (April 2018): 422–37. doi:10.1177/1368430217733118.

In addition to the truth bias and the halo effect, social disinhibition is another phenomenon related to digital environments that has been discussed in cyber psychology literature.[205] Dubbed 'the online disinhibition effect,' by researcher John Suler, this effect is believed to be aided by several components of digital interpersonal engagement. Suler writes about six factors which interact and contribute to the online disinhibition effect. Three of the primary factors include dissociative anonymity, invisibility, and what Suler calls 'communicative asynchronicity.'[206] Early research on computer mediated communication (CMC) found that people are more revealing about themselves in digital environments than in face-to-face communication.[207]

Scholars have generally distinguished between two types of deception; one type concerns providers of information, and the other concerns the nature of the information provided.[208] While several modern researchers have studied the latter type of deception by examining social media users' propensity to communicate deceptive information, fewer researchers have probed how social media affects the way in which identity deception is carried out.

Several researchers have contrasted different media with rates of deception (comparing telephonic, email, and instant messaging with face-to-face interactions).[209]

---

[205] John Suler, "The Online Disinhibition Effect," *CyberPsychology & Behavior* 7, no. 3 (June 2004): 321–26. doi:10.1089/1094931041291295.
[206] Ibid.
[207] L. Crystal Jiang, Natalya N. Bazarova, and Jeffrey T. Hancock, "From Perception to Behavior: Disclosure Reciprocity and the Intensification of Intimacy in Computer-Mediated Communication," *Communication Research* 40, no. 1 (February 2013): 125–43. doi:10.1177/0093650211405313.
[208] Yolanda Gil and Donovan Artz, "Towards content trust of web resources," *Web Semantics: Science, Services and Agents on the World Wide Web 5, no. 4 (2007): 227-239.*
[209] Jeffrey T. Hancock, Jennifer Thom-Santelli, and Thompson Ritchie, "Deception and design: the impact of communication technology on lying behavior," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04)* (2004) 129-134, accessed September 30, 2019, doi: 10.1145/985692.985709.

Both truth and deception are more difficult to detect in CMC than in face-to-face interactions, due to the lack of physical and visual source cues. This commonly leaves CMC users left with interpreting textual and content cues. Additionally, researchers have found that the types of lies that people tell in face-to-face interactions differ between the types of lies perpetuated in CMC. In face-to-face interactions, people tell more lies of omission, whereas in CMC, they tell more lies of commission (aka bald faced lies).[210] Some of the specific techniques used to perpetuate deception in social media include "bluffs, mimicry (such as mimicking a website), fakery (such as establishing a fake website), white lies, evasions, exaggeration, webpage redirections (such as misleading someone to a false profile page), and concealment (such as withholding information from one's profile)."[211]

Detecting Identity Deception and Social Media

Research into identity deception detection in social media has largely focused on automated or technical means of deception detection.[212] Through the use of artificial intelligence (AI) and machine learning, several researchers are probing the possibilities of textual analysis in the detection of false identities. Through the use of supervised learning models, some researchers have sought to unravel fake identities through the analysis of social media text messages.[213] In some studies, the application of AI to fake identity

[210] Lyn M. Van Swol, Michael T. Braun, and Miranda R. Kolb, "Deception, Detection, Demeanor, and Truth Bias in Face-to-Face and Computer-Mediated Communication," *Communication Research* 42, no. 8 (December 2015): 1116–42, doi:10.1177/0093650213485785.
[211] Michail Tsikerdekis and Sheralie Zeadally, "Online Deception in Social Media," *Communications of the ACM* 57, no. 9 (September 2014): 76, doi:10.1145/2629612.
[212] Estee van der Walt, J.H.P. Eloff and Jacomine Grobler, "Cyber-security: Identity deception detection on social media platforms," *Computers & Security* 78, (June 2018): 76-89. doi:10.1016/j.cose.2018.05.015.
[213] Eric A. Cruet, "Detecting Deception in Text Message Streams: Analyzing Linguistic-Based Cues and Readability Metrics Using Supervised Learning Models," *Journal of New Communications Research* 5, no. 2 (October 2013): 30–56.

detection has proven to have a success rate of 99 percent.[214] However, the vast majority of this research has been in reference to spam or bot-generated accounts and not accounts that are manually operated by humans purporting to be other humans.[215]

Specific methods of humans detecting lies in social media have been proposed. Some of the methods include detecting inconsistencies in the gender and expected background color of the person's account.[216] Other methods include searching for statistical inconsistencies in geo-location and update times.[217]

As human involvement in social media increases, universal feelings of trust, hope, and social acceptance tend to cloud critical judgment and result in much lower deception detection rates. Outside of digital interfaces, humans are notoriously bad at detecting interpersonal deception, with detection rates slightly better than random chance or 50 percent accuracy.[218] Within social media, the risks for deception are compounded, since digital personas can be quickly generated across numerous social media platforms.

Although there has not been a lot of research using adult subjects, digital researchers have used child subjects with parental consent in controlled identity deception studies. In one study, children ages 12-18 were asked to identify the age and gender of a stranger in a chatroom.[219] The main findings in this study were that only 16

---

[214] Zaher Yamak, Julien Saunier, and Laurent Vercouter. "Automatic Detection of Multiple Account Deception in Social Media," *Web Intelligence (2405-6456)* 15, no. 3 (July 2017): 219–31. doi:10.3233/WEB-170363.
[215] Richard J. Oentaryo, Arinto Murdopo, Philips K. Prasetyo, and Ee-Peng Lim, "On profiling bots in social media. Proceedings of the international conference on social informatics," *Social Informatics* (October 2016): 92-109.
[216] Jalal Alowibdi, et. al., "Deception Detection in Twitter," *Social Network Analysis and Mining* 5 (2015): 1-16. doi: 10.1007/s13278-015-0273-1.
[217] Ibid.
[218] Bond and DePaulo, "Accuracy of Deception Judgments," 230.
[219] Corinne May-Chahal, "Young People Struggle to Identify Who They Are Talking to Online," *British Journal of School Nursing* 10, no. 1 (February 2015): 39–40.

percent of child subjects were correct in guessing age, and only 10 percent were correct in guessing gender. Although the detection rates increased amongst older subjects, the highest detection rates were 22 percent (for guessing age) and 16 percent (for guessing gender) amongst year 11 and year 12 students. When asked how they evaluated the veracity of users' online identities, the child subjects said that content (e.g. what the user talked about) played a key role in their decision-making process.

Spear Phishing

One particularly pointed form of online identity deception is the act of spear phishing. Although spear phishing takes many shapes and forms, Stephen Northcutt with SANS Technology Institute defines it as, "A pinpoint attack against some subset of people (users of a website or product, employees of a company, members of an organization) to attempt to undermine that company or organization. It isolates a specific group of people, as opposed to spamming the world, and attempts to get them to do something to gain access to proprietary data or company systems. It will often look real and appear to come from a legitimate member of the organization. For instance, a spear phish may appear to come from an executive of the company asking for login IDs and passwords."[220]

Like spam emails, the malicious act of phishing (i.e. the targeting of many individuals in order to gain elevated access to information) has existed since the early days of the Internet in the 1990s.[221] Spear phishing, however, is a more recent

[220] Stephen Northcutt, "Spear Phishing," *SANS Technology Institute,* Security Laboratory: Methods of Attack Series*,* last modified May 9, 2007, https://www.sans.edu/cyber-research/security-laboratory/article/spear-phish.
[221] "A Brief History of Spear Phishing," *Infosec Institute,* last modified September 4, 2015, https://resources.infosecinstitute.com/a-brief-history-of-spear-phishing/#gref.

phenomenon. In contrast to general phishing, spear phishing requires more time and effort, but with potentially higher payloads. As time has progressed, both petty criminals and nation states have seen the efficacy of spear phishing in obtaining money, blackmail materials, and classified information. Although email remains the preferred method of spear phishing worldwide, the use of social media as a spear phishing platform is gaining ground.

In August 2018, a United States intelligence official publicly declared that China was waging a "super aggressive" campaign to target LinkedIn users with access to confidential material.[222] A year earlier, an unsealed affidavit was published, detailing the online recruitment of a former top-secret clearance holder, Kevin Mallory. The affidavit reveals that Mallory was contacted through LinkedIn by someone who he believed to be a Chinese headhunter. After messaging back and forth, Mallory eventually travelled to China and brought several US government documents with him which were classified at the top-secret level. The FBI indicted Mallory on one count of 8 U.S.C. § 1001 (Making Materially False Statements) and one count of 18 U.S.C. § 794 (Gathering or Delivering Defense Information to Aid a Foreign Government).[223]

Like Russia's election interference campaign, China's LinkedIn spear phishing efforts are merely a small fragment of today's foreign intelligence activity within social media. While it may be impossible to capture all of the nuances within this expanding digital environment of intelligence collection, focusing on one nation and one tactic is helpful for studying trends and making future predictions. In this chapter, background,

[222] Hannah Kuchler, "LinkedIn battles China's effort to recruit spies in US," *Financial Times,* August 31, 2018, https://www.ft.com/content/dccfd78e-ad32-11e8-94bd-cba20d67390c.
[223] "United States of America v. Kevin Patrick Mallory," United States Department of Justice, Office of Public Affairs, June 21, 2017, https://www.justice.gov/opa/press-release/file/975671/download.

analysis and recommendations will focus on the nation of Iran and the concept of digital honey traps.

Methodology

As a way to analyze how Iranian state-sponsored cyber groups use digital honey traps in social media, this chapter will examine two recent cases. The method of case study presents an ideal format to examine complex processes and isolate important aspects of theoretical concepts. Given the complexities of honey traps, social media technology, and modern cyber operations, the method of case study is the best approach for introducing this topic into broader discussions.

The first case to be studied involves a fake LinkedIn persona named 'Mia Ash,' an Iranian cyber group, and several unwitting LinkedIn members who were infected with spyware after engaging with an alluring, but ultimately fake persona. The second case study involves an American defector, a string of unwitting American clearance holders, and a private Facebook network that allowed a false persona into its inner circle.

In terms of case selection criteria, the following attributes were reasons for case selection: data richness, prototypicality of case background conditions, and intrinsic importance. First, these cases were selected due to their comparatively high coverage in international cyber security discourse and journalistic reporting. Although other cases of cyber espionage and cyberattacks have been covered in public outlets, many of these other cases lack in-depth analysis of the tactics, techniques, and procedures used, as well as corroborative reporting, which is why they were not selected. Second, these cases were chosen for their pointed use of the digital honey trap within a social media context. Lastly, these cases were selected for their intrinsic importance and relevance to current

areas of policy concern. Foreign intelligence interference via social media has been a prolonged topic of discussion within the American legislature and a high priority for the US Intelligence Community ever since the 2016 presidential election.[224] Because the digital honey trap is an evolving foreign intelligence threat in the sphere of digital covert activity, examining several recent cases will provide a substantive benefit to American policymakers and citizens.

This chapter will examine these cases using a narrative framework that is intended to illuminate the underlying mechanics of digital honey traps when they are used as a foreign intelligence tool. First, a review of the background conditions of the cases will introduce readers to the digital environment of modern intelligence targets. Next, the cases will show how vectors of contact have changed in the digital age. In addition to contact vectors, the cases will illuminate social media techniques that bolstered the mechanics of the campaign's deception. Lastly, the cases will present the damage of digital honey trap campaigns. After examining the case studies, this chapter will explore ways that the digital honey trap threat is evolving and provide recommendations for future research.

This case study analysis is not a comprehensive overview of Iran's intelligence programs. Rather, it is an examination of a single intelligence collection vector that is being deployed by Iran, and likely by other foreign intelligence adversaries. Through the analytical lens of case study analysis, this chapter will not only provide after-action analysis for the case studies in question, it will also lay the groundwork for future inquiries into digital honey trap operations by other intelligence agencies.

[224] Eckel, "U.S. Senate Committee Backs Intelligence Findings on Russian Meddling."

Case Study #1: Mia Ash, OilRig, and PupyRAT

In 2016, Dell's SecureWorks Counter Threat Unit detected some malicious cyber activity that resembled the tactics, techniques, and procedures used by a well-known Iranian cyber threat group, known as OilRig.[225] This activity was logged and noted, but no significant connections to specific actors were made during this time.

Then, in 2017, a LinkedIn profile belonging to a female with the username Mia Ash appeared. The profile began sending invitations to connect with a select group of men online. Ash claimed to be a twenty-something photographer based out of London who displayed a particular affinity for Middle Eastern, tech-savvy men working in the oil and gas refinery industries. To keep up digital appearances, Ash had a legitimate-looking resume, several filtered profile photos as well as regular posts and updates to her social media accounts. To an unassuming LinkedIn user, Ash's profile containing over 500 connections appeared to be unassuming, if not well-connected, judging by the polished look of her profile. In addition to her robust LinkedIn profile, Ash also had social media profiles on Facebook, Blogger, WhatsApp, and the artistic online social networking site, DeviantArt.

On the surface, Ash seemed like a friendly and adventurous young woman with a penchant for high-ranking Middle Eastern executives in the oil refinery and technology industries. Her modus operandi was simple. Ash would initiate contact by sending an innocent message to a CEO or vice president via LinkedIn's messaging application, then

[225] The hacker group OilRig has also been referred to as "COBALT GYPSY" and "Twisted Kitten." In addition to Secureworks's Iranian attribution, the cybersecurity firm CrowdStrike has also attributed the group as being an Iranian state-sponsored hacker group.

Ash would request that her new friend move their correspondence to a different social media platform, typically Facebook Messenger or an email provider.

While Ash was luring high-value targets in social media, around February 2017, Dell SecureWorks Counter Threat Unit detected some additional malicious cyber activity that resembled the tactics, techniques, and procedures used by the well-known Iranian cyber threat group, OilRig. A slew of corporate victimized computers appeared to have been compromised via malicious macros embedded in Microsoft Excel spreadsheets, sent via email attachment. Before any attribution or forensic assessments could be made, SecureWorks still needed to determine an initial attack vector and find the source of all of this damage.

In February 2017, a team of SecureWorks cyber investigators was deployed to a Middle Eastern company to diagnose an attempted spyware infection. During their deployment, it was discovered that one of the company's employees had been communicating with the Mia Ash LinkedIn persona for over a month.[226] According to victim statements, an employee of the victimized company began an online relationship with Ash on LinkedIn. Ash had approached the employee with photography questions, then moved the relationship to Facebook and other nodes of electronic contact.[227]

At one point during their communications, Ash asked the employee to download a 'photography survey', in the form of a Microsoft Excel spreadsheet. Moreover, Ash insisted that the employee open the survey on his work computer, otherwise, she told him, the survey would not work properly. Unfortunately, upon opening the file, the

[226] Andy Greenburg, "Meet Mia Ash, the Fake Woman Iranian Hackers Used to Lure Victims," *Wired,* July 27, 2017, https://www.wired.com/story/iran-hackers-social-engineering-mia-ash/.
[227] Ibid.

employee unleashed a vicious remote access trojan (RAT) known as 'PupyRAT,' which immediately gained administrator privileges across the corporate computer network and started exfiltrating sensitive digital records to a remote server.[228]

After months of analyzing the PupyRAT activity and performing cyber forensic analysis, SecureWorks attributed Mia Ash, the remote spyware and the malicious activity to the Iranian advanced persistent threat group OilRig.

Case Study #2: The Secret Facebook Network of Bella Wood

On February 8, 2019, a seven-count indictment against former AFOSI Special Agent Monica Witt was filed in the District of Columbia.[229] In addition to unveiling a slew of espionage charges levied against Witt, the unsealed indictment also unveiled a previously unknown digital honey trap campaign directed against US Air Force employees with access to specialized programs. The targets included "current or former Special Agents, counterintelligence analysts and other USIC employees who were coworkers or colleagues" of Witt.

The story of Witt's eventual defection to Iran began years before her alleged violations of US law. In February 2012, Witt traveled to Iran for the purpose of attending a "Hollywoodism" conference, sponsored by the IRGC and aimed at condemning America's lax moral standards. Shortly thereafter, Witt was seen in online videos, where she openly shared her status as a US veteran, her anti-American views and a public

[228] Greenburg, "Meet Mia Ash, the Fake Woman Iranian Hackers Used to Lure Victims."
[229] "Former U.S. Counterintelligence Agent Charged with Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues," Department of Justice, Office of Public Affairs, February 13, 2019, https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber.

statement about a recent conversion to Islam. Based on the evidence of the case, FBI officials later stated that Witt's defection appeared to be ideological in nature.[230]

Between 2012 and 2013, Witt was in contact with the IRGC and someone identified as "Individual A" in the indictment.[231] Through snippets of FBI-collected communications, Witt appeared to be eager to assist Iran and was ultimately given several opportunities to do so, largely through the vector of social media.

Around July and August 2013, Witt began conducting Facebook searches for former AFOSI counterintelligence colleagues. On August 28, 2013, Witt officially defected to Iran and from then on, Witt conducted Facebook queries for US government employees using fictitious Facebook accounts registered to multiple fake personas. Between January 2014 and May 2015, Witt "created 'target packages' for use by Iran against USG Agents, including USIC counterintelligence officers." Furthermore, around the same time, Witt disclosed the true name of a US government agent, as well as the fact that he or she conducted counterintelligence activities.

While Witt was performing social engineering research and building social media-derived target packages, in January 5, 2015, a group of Iranian cyber actors created an email account, bella.wood87@yahoo.com as well as an associated Facebook account with the username "Bella Wood." Shortly after the account was created, the Iranian cyber actors used it to send a Facebook friend request to a US government employee (referred to in the indictment as "USG Agent 2") who was currently deployed

---

[230] Ryan Lucas, "Ex-Air Force Counterintelligence Agent Charged with Giving Secrets to Iran," *NPR*, February 13, 2019, https://www.npr.org/2019/02/13/694234985/ex-air-force-counterintelligence-officer-charged-with-giving-secrets-to-iran/ (accessed May 25, 2019).

[231] "Former U.S. Counterintelligence Agent Charged with Espionage on Behalf of Iran; Four Iranians Charged with a Cyber Campaign Targeting Her Former Colleagues," Department of Justice, Office of Public Affairs, February 13, 2019, https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber.

to Kabul, Afghanistan with US Central Command (CENTCOM) Joint Intelligence Unit.[232] During this deployment, USG Agent 2 used a US Department of Defense computer to access Facebook. Around January 9, 2015, several Iranian cyber actors sent an email to USG Agent 2 with a spoofed link that purportedly directed USG Agent 2 to a "pretty card." The spoofed link actually led to a server which was controlled by the Iranian cyber actors. The email itself also used covert tracking software to confirm that USG Agent 2 was reading the email from a US Department of Defense computer network located in Kabul, Afghanistan. On January 9, 2015, bella.wood87@yahoo.com emailed USG Agent 2 again, using the following text: "I'll send you a file including my photos but u should deactivate your anti virus to open it because i designed my photos with a photo album software, I hope you enjoy the photos i designed for the new year, they should be opened in your computer honey." The links to the purported photos would have also directed USG Agent 2 to a server controlled by Iranian cyber actors.

Around the same time frame, Iranian cyber actors created a fake Facebook account using the true name of an individual noted in the indictment as "USG Agent 3." This was done using real photos and information that was gleaned from a legitimate Facebook account maintained by USG Agent 3. Using their newly created fake Facebook account, the Iranian cyber actors sent a Facebook friend request to an individual known as USG Agent 1, who accepted it. Within roughly twenty-four hours, the fake Facebook account sent USG Agent 1 a message with what appeared to be a .jpg image file, but was in fact, a .zip file containing malware that would have given the Iranian cyber actors "covert, persistent access on USG Agent 1's computer and any associated network."

[232] "Former U.S. Counterintelligence Agent Charged with Espionage on Behalf of Iran."

Around March 10, 2015, the Iranian cyber actors were able to persuade a Facebook user known as "USG Agent 5" to not only accept a friend request, but also to vouch for the fake Facebook account and add the fake account to a private Facebook group comprised mostly of USG Agents. In accomplishing this, the Iranian cyber actors gained multiple lines of access to personal and intimate information regarding US government employees. In May 2015, the same fake Facebook account sent separate messages to four other US government employees containing links that seemed to lead to international news articles, but in reality, led to pages controlled by the Iranian cyber actors.

Although the public will likely never know the full extent of the damage caused by Witt, former intelligence officials have described it as "severe", given Witt's former top-secret security clearance, her alleged violations of national defense statutes, and the suspicion that she revealed the names of double agents run by the United States.[233]

Case Study Analysis

In classical espionage, honey traps are men and women groomed to attract the attention of unsuspecting intelligence targets, but in the case of the KGB 'swallows,' these honey traps were sometimes blackmailed themselves into working as agents of the state. This coerced handling dynamic often created problems for KGB handlers of swallows. In the digital realm, where honey traps are nothing but computer code, Iranian handlers do not simply wield more control over their digital 'swallows' and have far fewer risks of defection, they also possess the collective wealth of the world's knowledge

[233] Alan Blinder, Julie Turkewitz, and Adam Goldman, "Isolated and Adrift, an American Woman Turned Toward Iran," *New York Times,* February 16, 2019, https://www.nytimes.com/2019/02/16/us/monica-witt-iran.html.

at their fingertips. These may be some of the reasons why the fake persona of Mia Ash was labeled by SecureWorks as one of the more sophisticated honey trap personas in recent history.

However, in spite of her successes, Ash wasn't perfect.

Like many fake social media profiles, the digital pieces which comprised Ash's profile were not crafted by Iranian intelligence officers. Rather, they were pilfered from across the Internet. Although the Ash persona was likely rooted in extensive research before it was deployed, the following analysis will show that it did not have the same human element as the honey trap set by Monica Witt.

Rather than being her own entity, the Mia Ash persona was a digital pastiche of publicly available jpeg and plaintext files which were stolen from the digital lives of others. Several of Ash's profile pictures and photograph uploads to her Blogger account were stolen from a Romanian woman with the DeviantArt moniker 'Bittersweetvenom.'[234] Additionally, Ash's LinkedIn resume bullets appear to have been copied almost word for word from an American female's LinkedIn profile.[235] From an intellectual property standpoint, Ash's entire persona was one huge violation of copyright law, which no one caught until her victims recognized the serious damage she had caused to national security.

As part of their published analysis, the SecureWorks researchers noted several specific social network anomalies, which assisted them in their attribution of the Mia Ash persona to the Iranian threat group. First, all of Ash's non-photography connections were

[234] "The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets," *Secureworks,* July 27, 2017, https://www.secureworks.com/research/the-curious-case-of-mia-ash.
[235] Ibid.

located in Bangladesh, India, Iraq, Iran, Israel, Saudi Arabia, and the United States, and they all worked for technology, oil/gas, healthcare, aerospace and consulting organizations. This conflagration of Iranian intelligence targets that formed the bulk of Ash's connections was one of the first indications to SecureWorks that Mia Ash had ulterior motives that seemed in sync with the OilRig Iranian cyber threat group.

Second, apart from the geographic and topical interests which aligned with known OilRig targets, SecureWorks also noted that all of Ash's connections were "mid-level employees in technical (mechanical and computer) or project management roles with job titles such as technical support engineer, software developer, and system support."[236] To a trained cyber analyst, the people in these roles carried elevated access within corporate networks, which would have given a cyber threat actor better access to a targeted environment.

Third, all of Ash's connections appeared to align with broader Iranian government "ideological, political and military intelligence objectives" which are likely not held by single female photographers looking to make friends on the Internet[237]

Regardless of the indicators of Iranian intelligence involvement in the Ash persona, the sophisticated fake social network aided by the knowledge and research of defector Monica Witt demonstrates a dangerous escalation of Iran's intelligence operations in social media.

In the case of Monica Witt's 'Bella Wood' persona and her multiple fictitious Facebook accounts, this multifaceted honey trap was greatly bolstered by the real-life experience of American defector and honey trap hybrid, Monica Witt.

---

[236] "The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets."
[237] Ibid.

Although Witt's indictment avoids naming specific individuals or delving into much detail on the content of the communications between Witt's fake personas and her targets, it does communicate a relative ease with which Witt infiltrated the unwitting network of former colleagues and current US government agents.

Like the Ash persona, Witt used photos from someone else's real social media page, but Witt had the benefit of being able to draw from her personal knowledge of the targets. This allowed her to craft non-alerting content and messages, which allowed her to secure positive responses to her surreptitious 'friend' requests.

Additionally, as someone with experience using, querying and manipulating the social media platform of Facebook, Witt was well-equipped to infiltrate its disparate social networks, including a private Facebook group of US government employees. In the FBI's indictment of Witt, the FBI agent details the multiple rounds of research conducted by Witt in Facebook's open search portal. Witt's research and rapport-building skills were so good, that she was able to penetrate a private Facebook group, allowing her enhanced access to a cache of information and a pre-vetted group of potential agents.

Compared to the Mia Ash persona, the case of Monica Witt demonstrates that although HUMINT collection is becoming increasingly digitized, the invaluable inclusion of the human factor will likely make digital honey traps even more sophisticated and effective, particularly if there are passionate, ideologically driven defectors involved. When a foreign intelligence service is crafting a simple mass-marketing covert influence campaign, much of the tedium can be eradicated by using AI, carefully crafted algorithms and computational propaganda. However, when it comes to targeting high value individuals (like Witt's former AFOSI counterintelligence colleagues), the Monica Witt

case demonstrates the power that comes from having a living, breathing human on the other side of the screen, who can navigate social media's nuances and breathe an air of authenticity into malicious online personas.

Today, Witt is believed to be residing in Iran, where she is effectively shielded from extradition to the United States. No matter where she resides, social media continuously allows this former US clearance holder to do more damage to US national security interests than she ever could have prior to social media. By connecting her with handlers and Iranian cyber experts, social media allows distance-directed honey traps like Witt to operate with reckless abandon, until their activities are detected by modern cyber tools and repaid with appropriate forms of retaliation from the US intelligence community.

Conclusion

According to the *IBM Security Services 2014 Cyber Security Intelligence Index* over 95 percent of all incidents investigated by IBM recognized "human error" as a contributing factor.[238] In the sphere of modern intelligence, where the Internet has vastly increased the size of the global attack surface, slight human errors of judgment can morph into irreversible national security disasters. As the analysis above demonstrates, Iran's intelligence services are proving to be innovative and relentless in their efforts to access sensitive information. Beneath social media's shining surface, it is important to remember that all it takes is one instant of human error for America's enemies to gain access to troves of top-secret information.

238 "IBM Security Services 2014 Cyber Security Intelligence Index," *IBM*, June 2014, https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

This chapter analyzed classical intelligence techniques which Iranian intelligence has revived within social media. Private cyber security firms have performed valuable post-incident analysis of the intricacies of Iranian digital honey traps. However, from the human intelligence angle, protracted and ongoing research in this area is lacking. The two case studies analyzed in this chapter present a small sliver of the totality of Iranian digital honey trap campaigns. Further research is required in order to assess the broader footprint of Iranian intelligence collection techniques in social media.

In terms of mitigation, up until now, social media providers have performed a limited number of preventative actions to protect against identity deception. This has largely involved the closing of fake 'bot' accounts which violate terms of use agreements. Given the scope and sensitive nature of concerted foreign intelligence campaigns, more effort should be dedicated towards developing standard methodologies for detecting foreign intelligence actors in social networking sites.[239] Although the initial implications of identity deception might seem insignificant, the long-term costs of successful honey traps and other malign intelligence operations can be devastating. The spillage of state secrets and the pillaging of sensitive technologies are just some of the initial payoffs that foreign intelligence agencies gain from the types of operations analyzed in this chapter.

As new challenges arise and the tactics of foreign cyber adversaries evolve, continuing research into this area can unmask malicious activity, connect common threads that attribute bad cyber actors, and develop additional counterintelligence measures. By heeding the lessons gleaned from these case studies and from future research, American intelligence practitioners can be better equipped to face the

239 Tsikerdekis and Zeadally, "Online Deception in Social Media," 78.

challenges of socially networked adversaries in the digital age.

CHAPTER 3
Chinese Intelligence in Social Media

Thus far, this paper has examined two of America's intelligence adversaries and has analyzed the ways in which social media enhances classical intelligence techniques favored by those adversaries. This chapter will examine how social media has enhanced Chinese agent recruitment.

China is unique among America's foreign intelligence adversaries for many reasons. Chinese intelligence has been known to recruit primarily ethnic Chinese as agents.[240] It has also been known to adopt a broader view of what many other agencies would label "intelligence." Lastly, in contrast to many Western intelligence officers who make it obvious when they have recruited someone and entered into a confidential relationship, the Chinese will rarely label these valuable intelligence relationships as such. Instead, Chinese intelligence officers will classify the relationship as social or professional, even though to highly trained Western eyes, there are clear intelligence-gathering dimensions.

One of the most striking aspects of Chinese intelligence is its 'grains of sand' or 'vacuum' approach to collection.[241] This approach is described in a metaphor that circulated through the FBI's Counterintelligence Division for years and has become synonymous with America's number one Asian intelligence adversary. As explained by former FBI analyst Paul Moore, "If a beach was an espionage target, the Russians would send in a sub, frogmen would steal ashore in the dark of night and with great secrecy

---

[240] Paul D. Moore, "How China Plays the Ethnic Card," *Los Angeles Times,* June 24, 1999, https://www.latimes.com/archives/la-xpm-1999-jun-24-me-49832-story.html.
[241] David Wise, *Tiger Trap: America's Secret Spy War with China,* (Boston: Houghton Mifflin Harcourt, 2011), 10-11.

collect several buckets of sand and take them back to Moscow. The US would target the beach with satellites and produce reams of data. The Chinese would send in a thousand tourists, each assigned to collect a single grain of sand. When they returned, they would be asked to shake out their towels. And they would end up knowing more about the sand than anyone else."[242]

This incredibly thorough yet cautious approach to intelligence is one of the hallmarks of Chinese human intelligence. In terms of its efficacy, this has historically been up for debate. For decades, the feasibility of processing, sorting and making general sense of such large volumes of information was unrealistic. Today, with the advent of machine learning, supercomputers and artificial intelligence, a collection technique that was once considered excessive and ineffective by other intelligence agencies, is now a productive reality. As China's and the rest of the world's records become digitized, the intelligence field moves semantically closer to embodying the grains of sand metaphor. Nowhere is this more evident than in the realm of social media.

While China has historically preferred to spot, assess, recruit, and meet its intelligence agents on Chinese soil, the twenty-first century has provided an additional vector for human agent recruitment in the form of social media. Within social media's digital environment, covert relationships thrive, encrypted communications are the norm and no virtual customs officials exist to question whether a digital citizen has sent classified materials across borders. In particular, professional networking sites like LinkedIn are proving to be well-suited venue for Chinese agent recruitment.

[242] Wise, *Tiger Trap: America's Secret Spy War with China*, 10-11.

Since entering the digital sphere of social media, China has become a highly aggressive online intelligence adversary. China has accomplished this by first leveraging the most innocuous of online social relationships in order to increase its foreign intelligence repository. Second, China has simultaneously imposed rigid domestic social media regulations based on its conception of 'Internet sovereignty' which exist to the detriment of Western democratic nations and China's own citizens.[243]

In the following pages, this paper will argue that social media offers a more seamless, discreet and effective vector for Chinese agent recruitment. Applying the case study method, this chapter will present a case of pre-social media Chinese agent recruitment and a case of post-social media Chinese agent recruitment, the latter conducted through the professional networking site *LinkedIn.* Following the presentation of the case studies, ensuing analysis will highlight critical aspects of this modern phenomenon and propose suggestions for future research. What the case studies and ensuing analysis will show is that China's social media-enabled agent recruitment should be of particular concern for the US Intelligence Community because of the ways in which it expedites and conceals the early phases of agent recruitment.

Literature Review

The HUMINT Recruitment Cycle

Human intelligence or HUMINT has often been called "the world's second oldest profession."[244] Although diverse opinions argue over what precisely constitutes

---

[243] Warren Strobel and Jonathan Landay, "Exclusive: U.S. accuses China of 'super aggressive' spy campaign on LinkedIn," *Reuters,* August 31, 2018, https://www.reuters.com/article/us-linkedin-china-espionage-exclusive/exclusive-us-accuses-china-of-super-aggressive-spy-campaign-on-linkedin-idUSKCN1LG15Y.

[244] Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* Sixth edition, (Los Angeles: CQ Press, 2015), 127.

"intelligence" there is wide consensus regarding the steps of the process of human agent recruitment. This is also known as the 'agent acquisition cycle' which various intelligence agencies employ.[245] The five steps to this cycle include the following: targeting or spotting, assessing, recruiting, handling, and termination.[246] Targeting is the initial identification of individuals who are believed to have access to intelligence. Assessing is the research and decision-making process that seeks to narrow the field of potential human assets. Recruiting is the critical step in which an intelligence officer 'pitches' the potential human asset, and the formal confidential relationship begins. Handling is the ongoing relationship between the recruited agent and his or her handler, where intelligence is provided to the handler, often in exchange for money, goods, or other benefits. Termination is the dissolution of the confidential relationship for any number of reasons, whether it is the endangerment of the human asset, a lack of productivity by the asset or a change in an agency's intelligence requirements.[247] As intelligence officers move forward in their careers and relocate around the world, they may also 'turnover' assets to fellow intelligence officers in order to continue the stream of intelligence, if termination is unnecessary.

Traditional Chinese Agent Recruitment

As many sinologists and historians will attest, China has a long history tied to the world's second oldest profession, dating back to at least the fifth century B.C.E. In Tsun Zhou's *The Art of War*, the final chapter of the famed military strategist deals exclusively with espionage.[248] According to Tsun Zhou, spies come in five different garden varieties

[245] Lowenthal, *Intelligence: From Secrets to Policy,* 128.
[246] Ibid.
[247] Ibid.
[248] Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis: Naval Institute Press, 1994), 3.

and can be used for action, information-gathering, deception operations and many other tasks in order to serve the state or secure military successes.[249]

Over the centuries, as China's military and foreign policy objectives have shifted, its intelligence apparatus and operational methodologies have also shifted. Prior to establishing diplomatic relations with the United States in 1979, the opportunities for Chinese espionage were few and far between and almost exclusively carried out by Chinese nationals who were tasked by their own government and then sent overseas.[250] In fact, prior to 2009, the only Chinese espionage case to reach prosecution was that of Larry Wu-Tai Chin, who was a CIA translator with the Foreign Broadcast Information Service (FBIS).[251] Recruited in the 1940s, Chin was paid hundreds of thousands of dollars over four decades and handled according to Western intelligence service tradecraft standards.[252] Chin was recruited while working for the U.S. Army Liaison Office in Fuzhou and continued to spy past his army retirement date. Over his lifetime, Chin provided Chinese intelligence with interrogation transcripts of Chinese prisoners during the Korean War, the identities of CIA employees, as well as scores of classified CIA and FBIS documents.[253] Chin's Ministry of Public Security handlers typically met him in Hong Kong or the mainland, but also provided him with a courier who would meet Chin at a mall in Toronto to retrieve any pertinent documents he had for his handlers.[254] Chin signaled that he was ready to meet with his handlers by sending letters

---

[249] Michael Warner, "The Divine Skein: Sun Tzu on Intelligence," *Intelligence & National Security* 21, no. 4 (August 2006): 488. doi:10.1080/02684520600885624.
[250] Dan Stober and Ian Hoffman, *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage* (New York, NY: Simon & Schuster, 2001), 129.
[251] Peter L. Mattis, "Assessing Western Perspectives on Chinese Intelligence," *International Journal of Intelligence & Counterintelligence* 25, no. 4 (2012): 684. doi:10.1080/08850607.2012.678745.
[252] Ibid., 685.
[253] Mattis, "Assessing Western Perspectives on Chinese Intelligence," 685.
[254] Ibid.

to addresses in Hong Kong or Guangzhou. Some sources reported that the Chinese had an exigency plan to exfiltrate Chin out of the United States using an intelligence officer disguised as a priest who lived in New York.[255]

With its vast territory and deeply entrenched belief in state sovereignty, China has rarely sent its officers abroad to perform recruitments in place. The exception to this would be when the Chinese Communist Party (CCP) sent officers abroad during the years leading up to 1949, when the People's Republic of China (PRC) was founded.[256] Following 1949, and after severing its ties with the Soviet Union, Chinese intelligence entered an isolationist phase that has continued to this day. While China progressed through several decades of limited diplomatic engagement, Chinese intelligence adapted its ethnocentric human recruitment methodology accordingly. Operating under varying kinds of isolationist restrictions, Chinese intelligence began to adapt its operational tactics in order to reduce the amount of contact between case officers and agents.[257]

From the mid to late twentieth century, Chinese intelligence also added another technique to their HUMINT toolbox: grooming and 'seeding' agents by convincing them to apply to sensitive positions within the United States government.[258] A classic example of this was the case of naturalized U.S. citizen Chi Mak. After immigrating to Hong Kong, Chi began providing the Chinese with plans of U.S. warships and visitor lists of U.S. naval commanders visiting the port city. In the 1970s, Chi immigrated to the United States, where he earned his citizenship in 1985.[259] In 1996, Chi gained a security

[255] Mattis, "Assessing Western Perspectives on Chinese Intelligence," 685.
[256] Ibid.
[257] Ibid.
[258] Ibid.
[259] Ibid., 688.

clearance through his work at Power Paragon, a subsidiary of L-3 Communications. For over forty years, Chi provided intelligence to the Chinese and assisted in the handling of other U.S.-based assets.[260] Before getting arrested in 2005, Chi provided intelligence on the Quiet Electronic Drive, which powered the new U.S. Navy Virginia-class submarines and similar sensitive technologies.[261]

According to China expert Peter Mattis, today's Chinese intelligence apparatus is comprised of several institutions, including the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the Second Department of the People's Liberation Army General Staff Department (2PLA), or the Liaison Office of the General Political Department.[262] China's MSS still gathers a vast amount of HUMINT by co-opting high numbers of ethnic Chinese residing within the PRC or abroad, although non-ethnic Chinese have also been co-opted.

In order to spot and assess individuals who may be open to recruitment, the Chinese have traditionally relied on open source material gleaned from American businesses, technical societies, and universities.[263] Although it is not classified, the value of open source intelligence or "OSINT" should never be underestimated, particularly when it is analyzed and synthesized by a veritable adversary. Compared to the high-risk, extraterritorial recruitment operations of Western intelligence agencies, the Chinese prefer to exert a high degree of control over the recruitment environment, as evidenced by their preference to recruit human assets within the PRC. This preference, noted by Chinese intelligence scholar Nicholas Eftimiades, is summarized below:

---

[260] Mattis, "Assessing Western Perspectives on Chinese Intelligence," 688.
[261] Ibid.
[262] Ibid., 684.
[263] Eftimiades, *Chinese Intelligence Operations,* 36.

> The MSS prefers to recruit agents in China. Recruiting foreign nationals on one's own soil tends to be a secure and cost-effective method of conducting espionage. The primary benefits are the safe environment for the case officer and the lack of ramifications should the prospective agent decline the recruitment pitch... A secondary benefit of recruiting espionage agents in one's own country is that governments need not incur the cost of maintaining case officers and their families overseas. In addition, this method is generally considered safe vis-a-vis foreign counterintelligence concerns.[264]

In order to lure foreign nationals to Chinese soil, common forms of cover include invitations for industry experts, government officials and academics to visit China on a lecture circuit or a lengthy, multi-day job interview. These clandestine "job interviews" may comprise of professional meetings, a slew of social events and often a great deal of alcohol. All of this is thrown at Chinese HUMINT targets in the hopes that this combination will wear down the target and make them more amenable to revealing private or personal matters.[265] At a certain point during this carefully constructed rigmarole, the invitee is offered the opportunity to continue their relationship with the cover entity (often a Chinese university, MSS-affiliated research institution or state-sponsored company) and provide them with more materials than was originally agreed upon. Quite often, this request is for classified materials. If the semi-professional relationship treads into covert territory and an actual recruitment takes place, then the agent will sign an agreement, conferring them a sum of money and promising their

[264] Eftimiades, *Chinese Intelligence Operations*, 57.
[265] Ibid., 59.

Chinese handlers their continued "cooperation" at a later date. Once co-optees or agents have been recruited in China they are then sent back to the United States with taskings to collect intelligence on science, technology or classified material of interest to the PRC.[266] Like the controlled recruitment environment, source handling amongst Chinese intelligence is often restricted to face-to-face meetings on Chinese soil, typically when the human asset claims they are visiting the PRC on business or for pleasure. This type of cover can often be maintained for decades without coming to the attention of American counterintelligence, as China has often had a special interest in sensitive science and technology targets, working in both the public and private sector.[267]

While many of the world's most active intelligence agencies rely upon a steady flow of cash in order to motivate their assets, China's ethnically homogenous cadre of human assets is often initially motivated by a sense of cultural and social obligation.[268] This is further enabled by China's social pressure cooker process of recruitment with its heavy emphasis on 'mutual understanding' and cultural exchange. For non-ethnic Chinese who are recruited, they are often fluent Mandarin speakers with an excellent grasp of the language and a deep understanding and fondness for the culture. These multifaceted layers of motivation further blur the relationship lines between social, professional and clandestine categories.

Chinese Agent Recruitment 2.0: Covert Recruitment in Social Media

LinkedIn was founded as a professional networking site in 2003 and as of 2019 has more than 660 million users in 200 countries worldwide.[269] In an increasingly

[266] Eftimiades, *Chinese Intelligence Operations*, 27.
[267] Lowenthal, *Intelligence: From Secrets to Policy*, 456.
[268] Stober and Hoffman, *A Convenient Spy,* 131.
[269] "About LinkedIn," *LinkedIn,* accessed December 6, 2019, https://about.linkedin.com/.

fractured and politicized Internet, LinkedIn stands out for its multicultural appeal. In contrast to the strict exclusion of many western social media sites like Facebook and Twitter, LinkedIn has been allowed to operate in many digitally sovereign nations like China, Iran and even North Korea.[270] While this may seem advantageous from a global economic standpoint, several recent uses of LinkedIn by adversarial cyber powers tell a cautionary tale. Although the full extent of the involvement of foreign intelligence agencies on LinkedIn has not been reported, there have been several journalistic outlets which have reported on numerous incidents in recent years.

On July 24, 2015, the United Kingdom's domestic intelligence agency, MI-5 sent an email that served as a "Security Service Espionage Alert."[271] Among the key findings and warnings in the email was the note that "hostile foreign intelligence services are increasingly using LinkedIn to find, connect with and begin cultivation and recruitment of current and former HMG [Her Majesty's Government] employees."[272]

In December 2017, the German domestic intelligence agency Bundesamt für Verfassungsschutz (BfV) reported that Chinese Intelligence had created a network of fake LinkedIn profiles that had contacted over 10,000 German citizens.[273] The BfV publicly shared some of these profiles with the news outlet Reuters, which upon review,

[270] Nicola Smith and Harriet Alexander, "LinkedIn becomes social media of choice for North Korea's elite," *Telegraph,* October 26, 2018, https://www.telegraph.co.uk/news/2018/10/26/linkedin-becomes-social-media-choice-north-koreas-elite/.
[271] Ian Drury and David Williams, "Foreign spies on LinkedIn trying to recruit civil servants by 'befriending' them before stealing British secrets," *Daily Mail,* August 9, 2015, https://www.dailymail.co.uk/news/article-3191733/Foreign-spies-LinkedIn-trying-recruit-civil-servants-befriending-stealing-British-secrets.html.
[272] Ibid.
[273] Thomas Escritt, "German intelligence unmasks alleged covert Chinese social media profiles," *Reuters,* December 10, 2017, https://www.reuters.com/article/us-germany-security-china/german-intelligence-unmasks-alleged-covert-chinese-social-media-profiles-idUSKBN1E40CA.

reported that some of these profiles had "senior diplomats and politicians from several European countries" amongst their connections.[274]

In October 2018, the French newspaper *Le Figaro*, received a leaked jointly written report from the French DGSI and DGSE (France's domestic and foreign intelligence agencies, respectively). The document reported that French state employees had been guilty of "culpable naivety" with respect to Chinese intelligence agents seeking them out through LinkedIn.[275] Purportedly, thousands of French government employees had been approached by Chinese avatars, causing French intelligence to alter its security posture in June 2017 and to respond to attacks 'blow for blow' from that point onward.[276]

In August 2018, a United States intelligence official publicly declared that China was waging a "super aggressive" campaign to target LinkedIn users with access to confidential material.[277] United States intelligence officials have said that Russia, Iran, North Korea and other nations also use LinkedIn and similar platforms for agent recruitment but that "China is the most prolific and poses the biggest threat."[278]

Methodology

To analyze how Chinese intelligence agent recruitment has evolved in social media, this chapter will examine two cases: one, where an American citizen was recruited in a pre-social media context and another case where an American was recruited in a post-social media context. Specifically, this chapter will highlight differences in the spotting, assessing and recruitment phases. The method of case study presents an ideal

[274] Escritt, "German intelligence unmasks alleged covert Chinese social media profiles."
[275] Henry Samuel, "Chinese spies fooled 'hundreds' of civil servants and executives, France reveals," *Telegraph,* October 23, 2018, https://www.telegraph.co.uk/news/2018/10/23/chinese-online-spies-fool-hundreds-totally-unprepared-top-french/.
[276] Ibid.
[277] Kuchler, "LinkedIn battles China's effort to recruit spies in US."
[278] Strobel and Landay, "Exclusive: U.S. accuses China of 'super aggressive' spy campaign on LinkedIn."

format to examine complex processes and isolate important aspects of theoretical concepts. Given the various stages of agent recruitment, the uniqueness of the Chinese approach, and the complications of social media, the case study method is the most optimal for examining this topic and bringing it into the broader research discussion.

The first case to be studied is that of Peter Lee, a naturalized American citizen from Taiwan, whose frequent business trips to China's mainland resulted in a textbook Chinese agent recruitment. The second case study is that of Kevin Mallory, a former CIA case officer, whose life circumstances led him to paste his resume into LinkedIn and respond to a Chinese 'job recruiter' who eventually persuaded Mallory that it was in his best interests to hand over classified documents to Chinese Intelligence in exchange for money.

In terms of case selection criteria, the following attributes were reasons for case selection: data richness, prototypicality of case background conditions, and intrinsic importance. First, these cases were selected due to their comparatively high coverage in journalistic and official government reporting. Although other cases of Chinese espionage and American agent recruitment have received coverage in public outlets, many of these other cases do not have primary source documents or the same level of detail and corroboration, which is why they were not selected. Second, the following cases were chosen for their prototypical representation of China's approach to agent recruitment within and outside of social media. Lastly, these cases were selected for their intrinsic importance and relevance to the current Chinese espionage threat. Although covert influence via social media has been a prolonged topic of discussion amongst the American public, the covert recruitment of human sources in social media is equally if

not more concerning. Because intelligence agent recruitment via social media is a new threat in the modern counterintelligence sphere, examining these cases will provide a substantive benefit to American intelligence practitioners and policymakers.

This chapter will examine these cases using a narrative framework that is intended to illuminate the underlying mechanics of classical and digital agent recruitment. First, this chapter will present the narratives of the cases. Next, this chapter will examine how the initial vectors of contact have changed and what the implications are for modern American intelligence officers. After examining initial vectors of contact, this chapter will highlight aspects of social media that enhance the process of agent recruitment. Lastly, ensuing analysis will explore ways in which this threat is evolving and then provide recommendations for future research.

The ensuing analysis does not attempt to provide a comprehensive overview of China's entire intelligence program. Rather, it is an examination of a single intelligence collection vector that is being deployed by China, and likely by other foreign intelligence adversaries. Through the analytical lens of case study analysis, this chapter will not only analyze the case studies in question, it will also lay the groundwork for future inquiries into digital agent recruitments carried out by other foreign intelligence adversaries.

Case Study #1: Peter Lee: Thinker, Translator, Scientist, Spy

On the surface, Peter Hoong-Yee Lee would likely not be cast as the male lead of a Hollywood spy thriller. As a quiet and unassuming scientist, Lee had no military or espionage training, but was a highly skilled researcher who excelled in the field of inertial confinement fusion (ICF) of nuclear weapons.[279] Lee's father had been a general

[279] Stober and Hoffman, *A Convenient Spy,* 135.

in the Chinese Nationalist Army that was eventually driven out by Mao Zedong.[280] Having grown up in Taiwan, Lee attended the National Taiwan University and then later moved to the United States, where he became a naturalized citizen in 1975.[281] After graduation, Lee obtained an ICF research contract with Lawrence Livermore National Laboratory (Livermore) through TRW Inc. in California.[282] Lee's aptitude for nuclear research soon earned him a position as the head of a laser research team at Livermore. In 1980, Lee returned to China, acting as a translator for a team of Livermore scientists. During this stay, a Chinese scientist came to Lee's hotel room one night. Although he didn't share many details, Lee did mention the meeting to a coworker. The coworker, aware of the company's security policy, promptly reported the impromptu meeting to Livermore security when they returned to the United States.[283] Notably, Lee failed to report the incident to security and began a decades-long overtly social and covertly intelligence-based exchange with China that would lead to an FBI investigation and eventual prosecution.

Along with his wife this time, Lee quickly returned to China after this initial visit, spending five weeks in December 1981 and January 1982 working at the Shanghai Institute of Optics and Lasers. Seeing the deplorable conditions of the Chinese lab in comparison to what the United States had, Lee sought to improve the conditions in China. A fellow scientist who assisted in the later investigation of Lee said that while Lee was in Shanghai, "he fell in love with the history and the art, the mystique."[284] On one of these

[280] Stober and Hoffman, *A Convenient Spy,* 135.
[281] Public Broadcasting Service. "Four Chinese Espionage Investigations." PBS.org. https://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/four.html (accessed May 12, 2019).
[282] Stober and Hoffman, *A Convenient Spy,* 135.
[283] Ibid.
[284] Ibid., 136.

early trips to China, Lee met Chen Neng Kuan, who was an explosives researcher who served as a host for China's high value American intelligence targets, which would at one point include Los Alamos Laboratory director Harold Agnew. After meeting Chen, Lee began a sixteen-year relationship with Chinese intelligence, captured in correspondence with Chinese scientists which consisted of over six hundred phone calls, letters, and emails.[285]

In 1984, Lee began working at Los Alamos Laboratory as he continued his regular visits to the Chinese mainland. In 1985, on a solo trip to a nuclear weapons research center in Mianyang, Lee was visited in his hotel room again, this time by Chen. Calmly and deftly, Chen began asking Lee a series of questions that delved into classified information.[286] Lee was initially hesitant, but after Chen emphasized the deplorable conditions of China's nuclear research facilities and how Lee could simply nod 'yes' or 'no,' to his questions, Lee relented and began answering first with nods and then with full sentences. The next day, Lee was taken to another hotel room, this time filled with Chinese weapons scientists who asked similarly sensitive questions for hours, which were promptly answered by Lee.[287]

If the relationship had teetered between professional and clandestine before, in the second hotel room, surrounded by such a great cloud of witnesses, there was no question that China had effectively converted Lee from an eager acquaintance to a fully-fledged spy.

---

[285] Stober and Hoffman, *A Convenient Spy,* 136.
[286] Ibid.
[287] Ibid., 136-137.

Around 1985, the FBI opened an espionage investigation and received approval for electronic surveillance of Lee.[288] For years, nothing substantive materialized, but in 1997, after returning home from China, Lee's wife discovered an FBI microphone in a ceiling vent while she was dusting. The FBI was now aware that their covert recordings were compromised, so they requested to interview Lee in a Santa Barbara hotel. Eventually, Lee admitted to sharing national defense information with China for more than a decade. Lee also stated that his motivations stemmed largely from a desire to please his father, from personal insecurity, and from what Lee's attorney called "scientific enthusiasm."[289] Although government inquiries later questioned the FBI and Department of Justice's prosecution of Peter Lee, his agent recruitment process serves as a prototypical example of China's HUMINT modus operandi.[290]

Case Study #2: Kevin Mallory: Former Case Officer Seeking Current Employment

A case study illustrating China's evolved agent recruitment techniques is the successful recruitment of Kevin Mallory. In 2017, it was discovered that Mallory, a former CIA case officer and fluent Mandarin speaker, had been spotted, assessed, and ultimately recruited by Chinese Intelligence via the professional networking site LinkedIn.[291]

Prior to his recruitment, Mallory held officer positions at the Central Intelligence Agency (CIA) and the Defense Intelligence Agency (DIA), both of which granted him

---

[288] Stober and Hoffman, *A Convenient Spy*, 137.
[289] Ibid., 139.
[290] *The Peter Lee Case: Hearings before the Subcommittee on Administrative Oversight and the Courts of the Committee on the Judiciary, United States Senate, One Hundred Sixth Congress, Second Session, March 29, April 5, and April 12, 2000,* Washington: U.S. G.P.O., 2001.
[291] David Shortell, "Trial begins for former CIA officer accused of spying for China," *CNN Politics*, May 30, 2018, https://www.cnn.com/2018/05/30/politics/cia-officer-spying-trial-china/index.html.

top-secret security clearances.[292] Mallory left government employment in 2012, and by 2017, he was purportedly behind on his mortgage payments, making him financially vulnerable and a prime target for a benefits-based recruitment.[293]

China's contact with Mallory was initiated via LinkedIn in February 2017 by someone who Mallory said appeared to be a headhunter (later revealed to be an individual by the name of Michael Yang) offering him a job as a consultant for a Chinese think tank.[294] An FBI affidavit listed the think tank as the Shanghai Academy of Social Sciences ("SASS").[295] Also included in the same affidavit was the FBI's assessment that "the Shanghai State Security Bureau ("SSSB"), a sub-component of the Ministry of State Security ("MSS"), has a close relationship with SASS and uses SASS employees as spotters and assessors. The FBI has further assessed that SSSB intelligence officers have also used SASS affiliation as cover identities."[296]

Several LinkedIn messages later, Yang, still posing as a headhunter, arranged a phone call with Mallory and an employee of the think tank.[297] Mallory made two trips to China in 2017 and at one point, agreed to meet with three men in a hotel room. Once inside the hotel suite in Shanghai, Mallory was questioned about the Trump administration's foreign policy, probed for details on the THAAD missile system, and

---

[292] "Former CIA Officer Sentenced to Prison for Espionage," U.S. Department of Justice, May 17, 2019, https://www.justice.gov/opa/pr/former-cia-officer-sentenced-prison-espionage.
[293] Ibid.
[294] Ibid.
[295] U.S. Department of Justice, *United States v. Kevin Patrick Mallory,* Stephen Green. Case No.: 1:17-MJ-288, Alexandria: U.S. Eastern District Court, 2017. https://www.justice.gov/opa/press-release/file/975671/download (November, 28, 2018).
[296] *United States v. Kevin Patrick Mallory.*
[297] "US accuses China of running aggressive LinkedIn spying program," *Reuters,* September 1, 2018, https://www.pri.org/stories/2018-09-01/us-accuses-china-running-aggressive-linkedin-spying-program (accessed May 26 2019).

asked about the United States' posture towards the South China Sea.[298] On the second of his two trips to China in the Spring of 2017, Mallory was given a specially configured Samsung Galaxy phone with an encrypted chat application which he used to communicate with Yang.[299] The FBI was able to recover these conversations and uncover details of the source-handler relationship between Mallory and Yang. Yang appeared to press Mallory for more information that could be of use, while emphasizing his focus on Mallory's safety. Mallory, on the other hand, seemed to be pressing Yang for higher financial compensation, given the risk he was running by providing these documents.[300] Additional FBI forensic analysis of the phone and its contents revealed that Mallory had completed all of the required steps for transmitting at least five classified government documents, one of which contained personally identifiable information of US government human sources. At least two of the documents were transmitted and communications between Mallory and Yang about these two documents were later captured off of the device.

Mallory surmised that his Chinese contacts were intelligence officers, but nevertheless, he persisted in providing them with what was determined by an FBI investigation to be classified documents. At his trial, it was revealed that Mallory had sent Yang at least two documents, including one which outlined a proposed DIA undercover operation.[301]

---

[298] Shortell, "Trial begins for former CIA officer accused of spying for China."
[299] Rachel Weiner, "Former CIA officer Kevin Mallory found guilty of selling secrets to China," *Chicago Tribune*, June 8, 2018, https://www.chicagotribune.com/nation-world/ct-cia-kevin-mallory-guilty-secrets-china-20180608-story.html.
[300] Ibid.
[301] Weiner, "Former CIA officer Kevin Mallory found guilty of selling secrets to China."

Although many of the details of the proposed operation were redacted, court testimony indicated that the operation would have involved Mallory using non-official cover at a company with a presence in China, but whose owners (labeled in court as "the Johnsons") were already cooperating with the U.S. government. Mallory's objective would have been to gather intelligence on science and technology. Court witness Robert Ambrose who oversaw undercover operations at the DIA testified that a modified version of this plan did go forward. However, in 2011, Mallory was let go from the DIA after he shared details of the proposed operation with a private intelligence contractor. Court records show that the Johnsons communicated with Mallory via LinkedIn in 2017, sharing that they no longer had business in China.[302] Hugh Michael Higgins, another former DIA employee who oversaw operations, said that this communication as the Johnsons' former handler was a major breach.[303]

Mallory was arrested upon his second return from Shanghai when customs agents found $16,500 of undeclared cash on his person.[304]

A total amount of $25,000 was reportedly what Mallory received in exchange for providing classified documents.[305] At his espionage trial in 2018, jurors saw these documents, in addition to other classified documents pertaining to defense intelligence operations and CIA intelligence analysis regarding another country's intelligence capabilities which Mallory had loaded onto SD cards.[306] Trial evidence included video footage of Mallory scanning top-secret and secret documents at a FedEx store and then

[302] Weiner, "Former CIA officer Kevin Mallory found guilty of selling secrets to China."
[303] Ibid.
[304] Maya Kosoff, "China Has Been Using LinkedIn to Recruit Potential U.S. Spies," *Vanity Fair,* August 31, 2018, https://www.vanityfair.com/news/2018/08/china-has-been-using-linkedin-to-recruit-potential-us-spies.
[305] Shortell, "Trial begins for former CIA officer accused of spying for China."
[306] Weiner, "Former CIA officer Kevin Mallory found guilty of selling secrets to China."

loading the documents onto SD cards. Court records also detailed Mallory's precarious financial situation, demonstrating how he had $12,205.32 past due on his mortgage payments, a credit card debt of $30,000, and a balance of more than $200,000 on a home equity line of credit.[307]

In June 2018, Mallory was found guilty of conspiracy to deliver, attempted delivery, actual delivery of national defense information to aid a foreign government and making materially false statements.[308] In May 2019, Mallory was sentenced to twenty years in prison followed by five years of supervised release.[309]

Case Study Analysis

As illustrated by both cases, China's spotting and assessing phases of agent recruitment often begin as innocent encounters, bereft of what many foreign intelligence agencies would deem sophisticated tradecraft. There are no dead drops, no high-speed surveillance and no cocktail parties; simply one professional reaching out to another, with a tacit expectation of a deeper relationship. Likewise, the Chinese intelligence recruitment and handling phases take place along the same relational spectrum of business or research with a sprinkling of positive cultural exchange. However, there are several key facets of social media's technology that have significantly altered this process and are worth exploring more deeply.

Spotting in Social Media

---

[307] Kevin Dilanian, "How a $230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China," *NBC News,* April 4, 2019, https://www.nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691.
[308] "Former CIA Officer Sentenced to Prison for Espionage," U.S. Department of Justice, Office of Public Affairs, May 17, 2019, https://www.justice.gov/opa/pr/former-cia-officer-sentenced-prison-espionage.
[309] Ibid.

Like many intelligence targets, the target of the first case study, Peter Lee, was most likely a target of opportunity. Once any initial reticence on his part was eradicated, the Chinese took advantage of his cooperation and invited him time and time again back to China, pulling him deeper into a mutually beneficial exchange of financial gifts for intelligence. Like many intelligence targets, Lee was not likely not verified as an intelligence target upon his first, second, or third visit to the foreign intelligence service's country. Intelligence recruitments and approaches always carry a degree of risk and uncertainty, even when they occur in one's home country. To this day, China receives many ethnic Chinese like Lee as visitors, who may be potential intelligence targets, but unlike the Cold War, today's technology enables nations like China to perform much of their spotting beforehand. Prior to the advent of social media, spotting a particular target on the world's professional stage was a far more difficult task.

As evidenced by the Mallory case, the spotting phase of agent recruitment is made infinitely easier with the advent of social media and the richly detailed profiles that accompany it. On LinkedIn, users are given reminders of the percentage of completeness of their profiles. LinkedIn provides positive feedback to users who opt to share a wide range of personal information and provides negative feedback (in the form of pop-ups and email reminders) to users who decline to share such details. LinkedIn is particularly cognizant of users who choose to omit a profile picture and will routinely ask users for the reasoning behind this omittance. For the modern Chinese intelligence officer, LinkedIn's digital culture of encouraged openness provides a highly accessible data set of potential intelligence targets.

Assessing in Social Media

Similar to spotting through social media, assessing targets is far easier in social media, as sites like LinkedIn allow users to search profiles based upon a wide variety of characteristics, enabling would-be handlers to sort and filter profiles based on desired skill sets and professional experience. Additionally, LinkedIn allows users to export profiles in various file formats, furthering the portability and ease of information sorting afforded by social media.

While Chinese operatives likely assessed Lee over the course of several carefully orchestrated visits to the Chinese mainland, it requires far fewer resources to assess a modern-day target like Mallory.

Recruiting in Social Media

Although it is not the only professional networking site, LinkedIn stands alone in terms of market share. Because LinkedIn is engineered for legitimate job recruiters, it takes very little effort for any individual to find someone who possesses a very specific set of skills and experience. Within the digital confines of LinkedIn, there also lies a high degree of privacy, making it ideal for employees who want to clandestinely seek additional job opportunities, or defect to a foreign nation.

In contrast to the overt, hotel room approach used by Chinese intelligence against Peter Lee, the approach of Mallory was more private, more innocuous, and more routine than someone claiming to have job opportunities entering Mallory's bedroom. The paradoxical intimacy and distance afforded in social media makes contact from strangers seem normal and likewise, more innocent than the physical approaches of the Cold War.

Additionally, the air of legitimacy afforded by LinkedIn presents unique challenges for monitoring espionage, deception operations, and human recruitment

efforts. Unlike the legions of faceless bots generated by Russia's Internet Research Agency, the legions of Chinese HUMINT recruiters are flesh and blood. They have backstories, legends, and outside lives that any social network's algorithms would not immediately label as a threat to its users. Because the modern Chinese agent recruitment threat is a complex hybrid of traditional HUMINT techniques and modern affordances of the digital sphere, it presents an ongoing challenge for Western intelligence agencies.

Conclusion

From this examination of Chinese agent recruitment in social media, it is clear that China's modern cyber operations are not focused solely on probing America's critical infrastructure and stealing its intellectual property. In terms of cyber tools, as this chapter has shown, the relatively 'soft' vector of social media appears to be a valuable new vector for intelligence recruitments, and as such, it should not be overlooked as a serious counterintelligence concern. As more and more Chinese intelligence officers infiltrate social media networks, it is critical that researchers from the public and private sectors are aware of the historical driving forces behind these events. This chapter intended to illuminate the history behind China's increasingly aggressive actions to recruit current and former U.S. intelligence officers. The recent prosecution and sentencing of Kevin Mallory demonstrate America's ability to investigate espionage. However, more efforts could be put towards the prevention of this form of Chinese recruitment before it starts.

One notable aspect of this problem, which differentiates its solution from that of Cold War espionage, is that much of the pertinent data that can assist intelligence analysts, academic researchers and policymakers, is currently held by private companies.

Because of this fact, future lines of research should be approached with public and private sector cooperation. With input from both intelligence professionals and private sector stakeholders, social media developers can build robust platforms that can detect or prevent foreign interference. As the *9/11 Commission Report* demonstrated, successful defense of the nation is not secured through bureaucratic stove-piping, but the concerted collaboration of public and private sector professionals.[310]

Future research into this area should continue to monitor developments in the tradecraft of Chinese recruitment efforts in social media, paying particular attention to the tactics, techniques and procedures which mirror those that China has used for centuries. If private and public sector experts possess a more holistic understanding of how the Chinese intelligence threat has historically evolved, then media analysts can better spot and assess future threats of Chinese agent recruitment for the benefit of policymakers, analysts, and U.S. security officials.

[310] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004).

Conclusion

The United States has often been able to anticipate future threats posed by foreign intelligence agencies. For much of American history, astronomical defense budgets and a robust intelligence bureaucracy have supplied the necessary technological and workforce advantages to accomplish this. With the advent of social media however, there has been an expansion of the intelligence playing field. With all the world's terrorists, spies and criminals gathered on the Internet, the possibilities for covert influence, data theft and espionage grows by the day. Information that was formerly confined to encrypted cables and invisible ink now travels at the speed of light through social media networks on a daily basis. Yet, much of social media's affordances have not altered the central goals, covert techniques and classical tradecraft of foreign intelligence agencies.

This paper sought to find out which classical intelligence techniques are used by America's most prominent intelligence adversaries in the sphere of social media. As discussed in the previous three chapters, the nations of Russia, Iran and China have all demonstrated a willingness and capability to revive specific intelligence techniques and direct these techniques against the United States through the vector of social media. This chapter will highlight key findings and conclusions from the previous chapters, make recommendations for addressing the issues discussed in this paper, and then make suggestions for future research on this topic.

Key Findings and Conclusions

As explored in Chapter 1, Russia has proven to be one of the most brazen US intelligence adversaries in the twenty-first century. However, in spite of its brazenness and lengthy history of engagement, Russian intelligence has had a mixed record of

operational success. Even at the height of the Cold War, Soviet attempts to influence American elections were often hindered by the limited technological tools available to propagate covert influence materials. In 1984, the KGB launched one of its most ambitious covert influence campaigns to date, in an effort to kick incumbent president Ronald Reagan out of the White House. The KGB did this by producing scores of inflammatory pamphlets and ephemera and by specifically tasking all of its officers with carrying out 'active measures.' As evidenced by Reagan's sweeping reelection victory, this KGB covert influence operation failed to achieve its stated goals and left Ronald Reagan unscathed in the eyes of American voters.

Though not every mission was a success, all throughout the Cold War the Soviet Union made it no secret that the United States was its number one intelligence enemy, and many researchers argue that this threat prioritization still stands.[311] While America may always be Russia's number one enemy, during the immediate period following the Cold War, Russia's intelligence agencies underwent years of internal political and bureaucratic reorganization, which put many of their intelligence operations on a temporary hiatus. After President Putin took office, Russia slowly rebuilt its intricate intelligence networks and recently extended these networks into the realm of social media.

This paper found that within the realm of social media Russia has revived the classical intelligence techniques of kompromat, forgeries, front groups and agents of influence and directed these techniques towards American presidential elections. While

[311] Seth G. Jones, "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare," *Center for Strategic and International Studies*, October 1, 2018, https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

the core tenets of these techniques remain, two critical aspects of Russia's covert influence toolbox have been enhanced through social media.

First, Russia's ability to obfuscate its involvement in spreading digital forgeries has improved. Influencing from the shadows has always been where Russia's spies have felt most at home. While most countries wait to attack their adversaries when they can see the whites of their eyes, Russia is notorious for attacking its enemies from a distance and then denying any and all involvement in the malicious activity.[312] Russia's inherent tendency and social media's ability to hide one's identity have only enhanced Russia's modern effectiveness in the intelligence realm. Secondly, social media has worsened Americans' ability to discern the truth in modernity's digital mire of misinformation. As many communications studies have shown, several aspects of human information processing become stunted when humans interact with digital media. Without the aid of source cues such as nonverbal body language and direct eye contact, many social media users make decisions based purely in emotion when it comes to deciphering digital content. On the whole, the only conclusion that can be drawn at this point in time, is that constant vigilance is required by every government, social media provider and digital citizen in order to constantly untangle the socially disruptive wires held together by falsely concocted kompromat, front groups, forgeries, and agents of influence.

In Chapter 2, this paper explored the expanding cyber operations of Iran and how social media plays no small part in acquiring and manipulating targets for Iranian honey trap operations. Following the launch of Stuxnet in 2010, Iran's cyber and intelligence

[312] Vladimir Soldatkin and Andrew Osborn, "Putin to Britain: Let's forget about the Skripal poisoning," *Reuters,* June 6, 2019, https://www.reuters.com/article/us-russia-forum-putin-britain/putin-to-britain-lets-forget-about-the-skripal-poisoning-idUSKCN1T71OU?il=0.

forces awakened to the digital age and bolstered their cyber defensive and offensive resources. In the *2019 Worldwide Threat Assessment of the US Intelligence Community* the US Director of National Intelligence writes that Iran is now a veritable opponent within the fifth domain of cyber operations and specifically, that Iran also "uses social media platforms to target US and allied audiences."[313]

While several of Iran's cyber operations are worthy of study, this paper found that Iran's deployment of honey traps in social media should be of grave concern to US intelligence. In early 2017, Iranian intelligence operations unleashed a demure yet deadly force multiplier in the form of digital persona, Mia Ash. Claiming to be a single, female photographer based in London, Mia Ash was a classic example of a honey trap made digital. While she appeared friendly to her victims, she was nothing more than a series of pillaged online profiles pasted together by Iranian intelligence operatives in order to lure unassuming victims in the oil, gas and aerospace industries and infect their computer systems with remote access malware. Simultaneously, the components of another Iranian honey trap operation were coalescing. In 2012, as US Air Force employee and Iranian defector Monica Witt attended anti-American conferences in Tehran she was being lured into her own Iranian trap when she refused to heed repeated warnings from the FBI that Iranian intelligence was targeting her. In or around 2013, Witt officially defected and became a spy for Iran and began years of valuable service to Iranian intelligence. Using her knowledge of former colleagues, Witt assumed various false identities in social media networks, quietly assessing and delivering digital targets into the hands of her Iranian

[313] Office of the Director of National Intelligence, *2019 Worldwide Threat Assessment of the US Intelligence Community,* Washington, D.C.: GPO, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed October 19, 2019)

handlers. After generating this initial contact, Witt's co-conspirators sent malicious links and attachments which downloaded malware onto the machines of Witt's social media contacts, which logged their keystrokes and maintained persistent access to their computer and associated network.

After closely examining the intelligence techniques used in the case studies of Iran's 'Mia Ash' persona and Iran's use of American defector Monica Witt, it is clear that Iran is incorporating the traditional honey trap technique into its computer network exploitation operations (CNE). While CNE operations may involve multi-phase execution and millions of lines of code, Chapter 2's analysis shows that Iran's initial vector of cyberattack relies on more traditional and human-centric vectors which mirror the mechanisms of the Soviet Union's 'swallows' and 'Romeo spies.'

Although Iran's digital honey trap operations do not directly target nearly as many individuals as Russia's one-hundred-million-views Facebook campaigns, Iran has damaged US national security and obtained intelligence successes by focusing its efforts on select groups of high-value targets. Not every nation has the workforce and funding of Russia or China. What Iran lacks in numbers of officers, it provides in the persistence of its cyber operators and in the careful cultivation of its human sources, like Monica Witt.

In the case of Mia Ash, though her identity was ultimately dismantled, she left a path of destruction in her wake. With no mechanisms built within social media's platforms to prove or disprove her true existence, she coached various targets into downloading malicious attachments which gave persistent computer access to Iran's cyber cadre. One of the key benefits to using a purely digital persona like Ash, is the fact that once her identity was burned, her digital footprint could be quickly erased, and a new

persona could be launched within seconds. No lives or livelihoods of female intelligence operatives were lost in the process which allows Iran to continue pilfering the Internet for lonely hearts and lucrative secrets.

When Monica Witt first visited Iran and expressed an overt interest in its culture, Iranian intelligence officers wasted no time in training and developing her as a human source. Their investment proved to be invaluable when Witt began accepting taskings from Iran and turning on her former US Air Force colleagues. The Witt case study demonstrates that modern social media honey traps are not confined to purely digital personas. The Monica Witt case is a perfect example of a hybrid honey trap operation in which an American defector serves as the controller behind any number of real or fake digital personas. Through hybrid honey traps such as Witt, America's adversaries are constantly reinventing their social media operations, derailing US national security and threatening America's most vital human assets.

Chapter 3 explored Chinese intelligence operations in social media. Specifically, this chapter explored China's use of the intelligence technique of agent recruitment and how both personal desperation and financial struggles can lead both ethnic Chinese and Americans to divulge secrets to Chinese Intelligence. Instead of leveraging friendly or purely social relationships (like Iran's Mia Ash and Bella Wood personas) the Chinese often leverage professional relationships. Over time, these professional relationships morph into a covert relationship which ultimately leads Chinese assets to violate non-disclosure agreements and pass valuable US intelligence onto their Chinese handlers.

Prior to social media, the Chinese targeted Peter 'Wen-Ho' Lee and used his scientific research as a grappling hook into his professional life. By offering Lee

professional research opportunities and speaking engagements, the Chinese lured Lee to China's mainland, where they exercised a high degree of control over his personal loyalties and persuaded him to help China in its race to beat the Americans in scientific innovation. This recruitment was bolstered by Lee's cultural and familial ties to China, but ultimately succeeded through the strong establishment of professional rapport through consecutive physical meetings and an intelligence recruitment in-person.

Kevin Mallory, on the other hand, was a former CIA case officer and financially plagued individual who was targeted through the online resume repository and professional networking site, LinkedIn. If Mallory had any initial hesitation, this was quickly quashed as the relationship moved from the digital world to the real one. However, even after meeting his handler in-person, the digital tradecraft between Mallory and his Chinese intelligence contacts continued when Mallory was assigned a specially configured phone which was likely encrypted in some form, so as to keep any further communications secret. Due to lapses in tradecraft, Mallory's phone and its contents were discovered by the FBI. The phone, along with a slew of secret conversations between an asset and his handlers were ultimately uncovered and added to the pile of evidence against Mallory. What is most notable about the Mallory and Lee cases, is the speed with which the clandestine relationship developed in both cases. While Lee appears to have been developed for roughly five years, between 1980 and 1985 before agreeing to work for China in a covert capacity, Mallory's recruitment progressed more quickly and with far fewer trips across oceans.

As seen in the case studies, the valuable vector of social media has proven to be highly effective when it comes to covertly targeting and approaching Americans

individually, in small groups, and in swaths upwards of hundreds of millions. China often prefers to target people individually after sifting through their background and creating the perfect opportunity to get them to agree to a second meeting and ultimately, to agree to provide sensitive information. Iran often targets victims who work with sensitive technologies, going after IT managers or other individuals who may fall prey to alluring online personas who steal victim's data or gain access to their networks. Russia possesses what is arguably the broadest target set. America's Eurasian adversary seeks to influence entire populations in order to ideologically rip apart America's citizens and cause divisions which distract Americans from recognizing who the true enemy is.

Apart from the differences in techniques which exist amongst America's intelligence adversaries, there are several aspects of social media which benefit them all. Namely, the covert, instantaneous and overexposed, yet simultaneously private nature of social media seems to broadly benefit intelligence operations as a whole. Although physical approaches of intelligence targets will likely continue within the diplomatic circuit, at professional conferences and anywhere else a valued target may be found, social media has created a less risky venue for intelligence agencies to initially approach and engage with human targets.

While civilians may use social media to conceal communications from a spouse, a supervisor or any number of social acquaintances, all of America's intelligence adversaries use social media tools to conceal their true identities from their targets and to hide their intelligence affiliation. They also use social media's encryption and automatic delete features to facilitate secure communication with targets as in the case of Kevin Mallory. Even if the content of communications is uncovered, the exact location of guilty

interlocutors has never been easier to hide or misattribute. Through the use of non-static IP addresses and virtual private networks, fake digital personas can hide in a sea of privately held big data which often requires specialized technical expertise to decipher.

Apart from the concealment advantages of social media as an intelligence operations platform, another value of this platform lies in its instantaneous dissemination capabilities. Through direct messaging applications, information can be passed across international borders within seconds. Meaningful relationships between digital honey traps and their targets can blossom without either party ever driving, flying or walking to meet each other. A million illicit messages can traverse the Internet without ever being seen by another soul.

The final aspect of social media which makes it ideal for carrying out long-term intelligence operations is the fact that privacy in social media is an ill-defined concept with only patchwork regulation across the world. Many companies vow to keep customer information private, yet many fail to elaborate regarding what their internal privacy practices entail. Because intelligence agencies benefit from large budgets and technological experts, they can easily gain unauthorized access to vast troves of private information about individuals. Information which was formerly shared with a small subset of physically proximate individuals is now readily shared with social media providers and then pilfered by foreign intelligence agencies. Given the diverse forms of information safe-guarding within social media, this has sometimes resulted in significant data breaches and cases of espionage, like the recent case of two former Twitter employees charged with probing Twitter's internal records for information on Saudi

dissidents and thousands of Twitter users on behalf of Saudi Arabia.[314] The often unregulated and easily penetrable aspects of privacy in social media makes targeting individuals far easier, as their pattern of life and personal preferences are readily accessible by intelligence officers.

General Recommendations

The threat of intelligence operations in social media presents a persistent problem for American citizens, the US Intelligence Community and social media providers, the latter of whom are often reluctant to take action out of fear of alienating their customers. Although the current state of affairs in social media can seem like a harsh reality, there are steps which the US Intelligence Community and social media providers can take, in order to create a safer, more secure digital world. Four recommendations for mitigating the threat of foreign intelligence in social media include: educating Americans on the threat, implementing security by design protocols in social media platforms, creating identity verification mechanisms, and improving private and public sector information sharing.

First, in order to fight forgeries, social media companies, nonprofit organizations and the US government can all produce public service announcements (PSAs) to better educate Americans in digital literacy and specifically, the importance of verifying information provenance in social media. Apart from emphasizing the need to verify information, PSAs could also educate Americans on verifying identities of people they connect with through social media. This could help victims determine agents of influence

[314] Robert Burnson, "Two Ex-Twitter Employees Charged With Spying on Users for Saudis," *Bloomberg*, November 6, 2019, https://www.bloomberg.com/news/articles/2019-11-06/two-ex-twitter-employees-charged-in-saudi-government-spy-plot.

and expose front groups. In terms of countering kompromat, PSAs could urge Americans to be careful regarding what they post publicly. Additionally, since many kompromat operations involve false information, PSAs should encourage social media users to think before reposting or retweeting information which not be true.

Second, apart from educating social media users, social media and information technology providers can try to implement 'security by design,' which Facebook implemented to some extent after the 2016 US Presidential Election.[315] Security by design is a proactive approach to infrastructure security — one that does not rely on reactive third party security tools which only respond to individual incidents, but rather, builds security into infrastructure from the ground up.[316] Public and private sector cooperation in this matter could assist social media developers with identifying digital indicators of foreign intelligence activity on their platforms and could assist the public sector by providing a streamlined early warning system for suspected covert influence campaigns before they persist for months undetected.

Third, better identity verification mechanisms should be put in place within social media. Before any technical solutions are developed, it is important for intelligence professionals, CEOs and citizens to note that the success of most of the intelligence operations discussed in this paper can be attributed to the lack of consistent and reliable identity verification mechanisms in social media. All social media users should make an effort to verify their online contacts, but when heightened security awareness is sacrificed

[315] James Langford, "Facebook has made fundamental changes since 2016 election, Sandberg says," *Washington Examiner,* January 21, 2019, https://www.washingtonexaminer.com/business/facebook-has-made-fundamental-changes-since-2016-election-sandberg-says.
[316] "What is Security by Design?" *LogicWorks* (blog)*,* January 25, 2017, https://www.logicworks.com/blog/2017/01/what-is-security-by-design/.

for convenience or expediency, social media users will likely not take the time to perform extensive background research of newly developed online contacts. If the victims of the Mia Ash operation had means to verify or corroborate the Mia Ash identity within the platforms in which she was operating then the malware unleashed by Mia Ash could have been contained. It is particularly imperative that public and private sector executives are aware of any and all tools which can assist in verifying the identities within their social media circles. As these types of individuals are the most likely to be targeted for proprietary or closely held information, executive briefings on digital verification mechanism could help to curb the number of successful online approaches of top executives and clearance holders.

Fourth, it is important that US intelligence leaders address the lack of information sharing and overall communication between private sector stakeholders and the Intelligence Community. Hurdles to public-private sector cooperation abound in a variety of fields, but particularly within the field of intelligence. This is because espionage and counterintelligence investigations are often highly classified, compartmentalized and closely guarded by those who work these types of cases, and often for good reason. unfortunately, over-classification within the US government can also present information sharing hurdles which has been one of many critiques put forth by many leading researchers.[317] These kinds of hurdles make public and private sector information sharing difficult but not insurmountable. Ways in which the public sector can facilitate information sharing is through publishing of unclassified white papers, granting

[317] Herbert Lin, "A Proposal to Reduce Government Overclassification of Information Related to National Security," *Journal of National Security Law & Policy* 7, no. 3 (September 2014): 443–63.

clearances to qualified private sector partners and de-classifying as much material as is practicable.

However, successful sharing of information and collaboration in this field requires actions from both sides. The private sector can assist by funding projects which seek to detect deception operations in social media. Technology researchers in corporate America and American universities are perpetually making strides in artificial intelligence (AI) and machine learning algorithms that are designed to detect certain patterns of behavior. Research which combines the fields of intelligence studies and AI could assist the Intelligence Community in identifying potential espionage cases in real time and real social networks.

A blatant hurdle to this kind of data collection and information sharing is the potential for privacy violations. Social media currently exists in a patchwork of privatized corporations, each with their own user agreements and privacy policies. Although the 2016 US Presidential Election called attention to the lack of defenses against foreign interference, many Americans are often wary of corporate interference and over-collection of private data. Therefore, this kind of data sharing would have to be carefully scrutinized for First and Fourth Amendment considerations, as well as politicization concerns.

Recommendations for Future Research

Although this paper provides historical and cultural context regarding the digital intelligence operations of America's top intelligence adversaries, there are several lines of research which were not addressed and should be considered by future researchers. The first research recommendation of this paper is to broaden the cultural lens of

intelligence studies and analyze lesser known intelligence agencies in mainstream research. Just as history has informed this paper about classical intelligence techniques, history also has a lot to say about hidden intelligence alliances, with Russia's Cold War assistance to Cuba and its former Soviet states being a prime example. Many current, but lesser known intelligence agencies are likely working with some or all of the agencies examined in the chapters above, but there is little research which attempts to make this kind of advanced attribution.

Smaller intelligence adversaries certainly take action against the United States, but the lack of public attention on these lesser known adversaries has created a dearth of research regarding the nuances of their operations. North Korea and Israel are two examples of nations whose cyber operations are legion, yet they often remain hidden from the public eye. Additionally, in 2017, Cyber security firm FireEye officially designated APT32 aka 'Ocean Lotus Group' for executing intrusions into private sector companies, foreign governments, dissidents, and journalists.[318] APT32 is a Vietnamese advanced persistent threat (APT) group whose socially engineered malware and espionage operations had been on the cyber firm's radar since 2014 and whose activities continue to disrupt global politics and economics.[319]

Intelligence studies has often been limited in terms of its cultural focus, with a great deal of research devoted to what some researchers have called the 'Anglosphere.'[320] This has historically led to a severe lack of source diversity and richness. This paper

[318] Geary, "Rise of the Rest: APT Groups No Longer from Just China and Russia."
[319] Nick Carr, "Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations," *FireEye* (blog), May 14, 2017, https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.
[320] Philip H. J. Davies and Kristian Gustafson, *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere,* (Washington, DC: Georgetown University Press, 2013).

addressed this issue from an American perspective and highlighted three of America's top intelligence adversaries. However, the United States is not the only country whose elections and national resources have been targeted for exploitation and Americans are not the only citizens who use social media. Germany, France and the UK have all experienced what their national security experts believe was foreign influence through social media. By examining the social media operations directed towards other nations, American researchers can learn from America's allies and better understand foreign intelligence operations in social media from a global perspective.

The second research recommendation of this paper is to address this topic from a technical standpoint and examine which intelligence tactics, techniques and procedures are platform specific. In other words, which forms of intelligence gathering take place on specific social media platforms? LinkedIn is a somewhat obvious platform for human agent recruitment since its stated purpose is for job recruitment. Among other, less well-known social media sites, it would be valuable to explore the human recruitment aspects of each platform and how these platforms are specifically leveraged to perform specific types of intelligence collection. Every social media site claims to specialize in certain forms of human connection within digital media. Some sites, like Twitter are more text-driven, while other sites like Instagram are geared more towards photo and video sharing. Future research could analyze the most popular social media sites from an intelligence perspective and report on the specific ways in which its users may be exploited by foreign intelligence adversaries.

This kind of platform-specific research is already ongoing within the private sector. FireEye's report on APT29 (HAMMERTOSS) explores how this Russian state-

sponsored cyber group capitalizes on Twitter's source code and a custom algorithm to generate random Twitter handles every day, which seek out specific high-value targets on the social media platform to inject command and control (CNC) malware.[321] CNET has characterized this HAMMERTOSS as "essentially a first class spy" whose Twitter-enabled malware "mimics normal computer user behavior the entire time it's compromising files on a victim's machine. It can even time itself to the victim's work schedule."[322] According to FireEye, other malicious tools that specifically weaponize Twitter, include: MiniDuke, a Windows-based backdoor that is a suspected Russian tool, the Sninfs botnet, and Flashback, which is a Mac-based backdoor.[323] This form of platform-specific intelligence analysis is valuable to coders, intelligence professionals and all users of social media. Future research could expand threat analysis to other platforms and then publish results regarding the threats other platforms are most likely to face.

The third research recommendation of this paper is to probe the interdisciplinary depths of deception research. Although deception theory has greatly expanded since the onset of computer mediated communication, much of social media territory remains to be explored. Future intelligence studies could include human psychology and communications research to conduct studies on topics such as the effects of introducing more robust visual source cues in social media, which hitherto have been sorely lacking in this digital communications medium. Analyzing whether source cues aid in online

---

[321] "HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group," *FireEye*, July 2015, https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf.
[322] Laura Hautala, "Extra sneaky Hammertoss malware acts just like you on your computer," *CNET*, July 29, 2015, https://www.cnet.com/news/hammertoss-extra-sneaky-malware-acts-just-like-you/.
[323] "HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group."

deception detection could help social media providers in implementing better security measures for their users and in creating a more trustworthy online experience. Some intelligence researchers are taking cues from the history of honey pots and 'sexpionage' and are synthesizing intelligence and sexuality studies, to explore how online sexual behaviors affect modern intelligence operations.

Much of modern intelligence collection still revolves around the collection of human intelligence, which should not be forgotten when analyzing comprehensive data sets provided by social media analytics tools. For this reason, it is imperative that future intelligence research acknowledges the human factor in its varying approaches.

The Future Without Change

If research and public discussion continues to label the threat of intelligence operations in social media purely as a modern technological challenge, then future elections, state secrets and economic proprietary information will continue to be stolen. From the research presented in this paper, is clear that foreign intelligence agencies are using social media not merely as an open source platform for collection, but as a meeting venue for initial introductions to intelligence targets. In this sense, social media has been used to supplement, rather than replace classical venues of intelligence activity. Although OSINT continues to expand the base of the intelligence analyst's data sources, social media is particularly potent for its human factor and the direct human contact which occurs on its platforms.

This paper's analysis of specific classical intelligence techniques that have been revived in social media demonstrates a small portion of the tradecraft paradigm shift which is taking place within the intelligence profession. What once required large sums

of money, a lifetime of cultural knowledge and highly trained intelligence officers is now accomplished through encryption algorithms, data servers and digital bots. Although many private sector and academic researchers are well versed in the modern technologies behind today's intelligence operations in social media, there are few cyber experts who also possess a deep understanding the histories, cultures and motivations of America's intelligence adversaries. Because intelligence operations in social media are causing some of the most damaging incidents in recent American history, it is imperative that all researchers synthesize historical insights, current technology and forward-looking analysis to better understand and combat this issue.

Bibliography

"2016 Presidential Campaign Hacking Fast Facts." *CNN*. July 18, 2018. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

"About LinkedIn," *LinkedIn,* https://about.linkedin.com/. (accessed December 6, 2019).

Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections: The Quarterly Journal* 15, Issue 1 (Winter 2015): 5-31.

Alowibdi, Jalal et. al. "Deception Detection in Twitter." *Social Network Analysis and Mining* 5 (2015): 1-16. doi: 10.1007/s13278-015-0273-1.

Alperovitch, Dmitri. "Bears in The Midst: Intrusion into The Democratic National Committee," *CrowdStrike* (blog). June 15, 2016. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Andrew, Christopher M. *The Secret World: A History of Intelligence.* New Haven: Yale University Press, 2018.

Andrew, Christopher M., and Oleg Gordievsky. *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985*. London: Hodder and Stoughton, 1991.

_____. *KGB: The Inside Story of Its Foreign Operations From Lenin to Gorbachev.* New York, NY: HarperCollins Publishers, 1990.

Andrew, Christopher M., and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB.* New York: Basic Books, 1999.

Bagley, Tennent H. *Spymaster: Startling Cold War Revelations of a Soviet KGB Chief.* New York: Skyhorse Publishing, 2015.

Banerjea, Udit. "Revolutionary Intelligence: The Expanding Intelligence Role of the Iranian Revolutionary Guard Corps." *Journal of Strategic Security* 8, no. 3 (Fall 2015): 93-106.

Barbier, Geoffrey. *Provenance Data in Social Media*. San Rafael, Calif: Morgan & Claypool, 2013.

Barojan, Donara. "Eight Takeaways from Iranian Information Operations." *AFCEA*. April 1, 2019. https://www.afcea.org/content/eight-takeaways-iranian-information-operations.

Bennett, Anthony. *The Race for the White House from Reagan to Clinton: Reforming Old Systems, Building New Coalitions.* New York: Palgrave Macmillan, 2013.

Bittman, Ladislav. *The KGB and Soviet Disinformation: An Insider's View*. Washington: Pergamon-Brassey, 1985.

Blinder, Alan, Julie Turkewitz, and Adam Goldman. "Isolated and Adrift, an American Woman Turned Toward Iran." *New York Times.* February 16, 2019. https://www.nytimes.com/2019/02/16/us/monica-witt-iran.html.

Bond, Charles F. and Bella M. DePaulo. "Accuracy of Deception Judgments." *Personality and Social Psychology Review* 10, No. 3: 214-234.

Bowman, M.E. "Secrets in Plain View: Covert Action the U.S. Way." In *The Law of Military Operations: Liber Amicorum Professor Jack Grunawalt,* edited by Michael N Schmitt, 1-16. Newport, R.I.: Naval War College Press, 1998.

Burnson, Robert. "Two Ex-Twitter Employees Charged With Spying on Users for Saudis." *Bloomberg*. November 6, 2019. https://www.bloomberg.com/news/articles/2019-11-06/two-ex-twitter-employees-charged-in-saudi-government-spy-plot.

"A Brief History of Spear Phishing." *Infosec Institute.* September 4, 2015. (accessed January 8, 2019). https://resources.infosecinstitute.com/a-brief-history-of-spear-phishing/#gref.

Buller, David B. and Judee K. Burgoon. "Interpersonal Deception Theory." *Communication Theory* 6, Issue 3, (August 1, 1996): 203–242, doi:10.1111/j.1468-2885.1996.tb00127.x

Canfil, Justin Key. "Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity." *Journal Of International Affairs* 70, no. 1 (Winter 2016): 217-226.

Carr, Nick. "Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations." *FireEye* (blog). May 14, 2017. https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

Chazan, David. "French Spy Facing Charges 'was snared by Chinese honeytrap." *Telegraph*. May 27, 2018. https://www.telegraph.co.uk/news/2018/05/27/french-spy-snared-chinese-honeytrap-faces-treason-charges/ (accessed May 25, 2019).

Collins, Ben and Joseph Cox. "Jenna Abrams, Russia's Clown Troll Princess, Duped The Mainstream Media and The World." *The Daily Beast,* November 2, 2017. https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.

Colomina, Carme. “La Desinformación de Nueva Generación: Cinco Escenarios Políticos y Geoestratégicos Ante El Fake.” *Anuario Internacional CIDOB*. January 2019, 61.

Cruet, Eric A. “Detecting Deception in Text Message Streams: Analyzing Linguistic-Based Cues and Readability Metrics Using Supervised Learning Models.” *Journal of New Communications Research* 5, no. 2 (October 2013): 30–56.

“The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets.” *SecureWorks.* July 27, 2017. https://www.secureworks.com/research/the-curious-case-of-mia-ash.

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

Dilanian, Kevin. “How a $230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China.” *NBC News.* April 4, 2019. https://www.nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691.

"Discussion with CIA Director Mike Pompeo." *FDD National Security Summit* (repr., Washington D.C.: Foundation for Defense of Democracies, 2017). http://www.defenddemocracy.org/events/fdds-national-security-summit/.

Dobrynin, Anatoly. *In Confidence: Moscow's Ambassador to America's Six Cold War Presidents (1962-1986)*. New York: Times Books, Random House, 1995.

Drury, Ian and David Williams. “Foreign spies on LinkedIn trying to recruit civil servants by 'befriending' them before stealing British secrets.” *Daily Mail.* August 9, 2015. https://www.dailymail.co.uk/news/article-3191733/Foreign-spies-LinkedIn-trying-recruit-civil-servants-befriending-stealing-British-secrets.html.

Eckel, Mike. "U.S. Senate Committee Backs Intelligence Findings on Russian Meddling." *Radio Free Europe.* 2018. https://www.rferl.org/a/senate-committee-russian-interference/29336790.html.

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

Emerson, John B. "Exposing Russian Disinformation.” Speech, Berlin, June 25, 2015. US Embassy and Consulates in Germany. https://de.usembassy.gov/exposing-russian-disinformation/.

“Enhancing Engagement Efforts to Stay Ahead of the Threat.” FBI. February 2, 2017. https://www.fbi.gov/news/stories/office-of-private-sector.

Escritt, Thomas. “German intelligence unmasks alleged covert Chinese social media profiles.” *Reuters.* December 10, 2017. https://www.reuters.com/article/us-germany-security-china/german-intelligence-unmasks-alleged-covert-chinese-social-media-profiles-idUSKBN1E40CA.

“Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements.” U.S. House of Representatives Permanent Select Committee on Intelligence. U.S. Senate. Accessed November 30, 2019. https://intelligence.house.gov/social-media-content/.

“Former CIA Officer Sentenced to Prison for Espionage,” U.S. Department of Justice, May 17, 2019, https://www.justice.gov/opa/pr/former-cia-officer-sentenced-prison-espionage.

“Former U.S. Counterintelligence Agent Charged with Espionage on Behalf of Iran; Four Iranians Charged with a Cyber Campaign Targeting Her Former Colleagues.” Department of Justice. Office of Public Affairs. February 13, 2019. https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber.

"Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy." *Freedom House* (November 2017): 1-48. https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Frenkel, Sheera and Linda Qiu. “Fact Check: What Mark Zuckerberg Said About Facebook, Privacy, and Russia.” *New York Times.* April 11, 2018. https://www.nytimes.com/2018/04/10/technology/ zuckerberg-elections-russia-data-privacy.html.

Friend, Catherine and Nicola Fox Hamilton. “Deception Detection: The Relationship of Levels of Trust and Perspective Taking in Real-Time Online and Offline Communication Environments.” *CyberPsychology, Behavior & Social Networking* 19, no. 9 (September 2016): 532–37. doi:10.1089/cyber.2015.0643.

Galeotti, Mark. "Russian Intelligence is at (Political) War." *NATO Review*. May 11, 2017. https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/EN/index.htm.

Geary, Sarah. “Rise of the Rest: APT Groups No Longer from Just China and Russia.” *FireEye.* April 26, 2018.https://www.fireeye.com/blog/executive-perspective/2018/04/rise-of-the-rest-apt-groups-no-longer-from-just-china-and-russia.html.

Gil, Yolanda and Donovan Artz. “Towards content trust of web resources.” *Web Semantics: Science, Services and Agents on the World Wide Web 5, no. 4 (2007): 227-239.*

Giles, Keir. "Handbook of Russian Information Warfare." *NATO Defense College Research Division*, (November 2016): 1-90. http://www.ndc.nato.int/news/news.php?icode=995.

Goldstein, Frank L., and Benjamin F. Findley, *Psychological Operations: Principles and Case Studies.* Maxwell Air Force Base, Ala.: Air University Press, 1996.

Golitsyn, Anatoliy. *New Lies for Old: The Communist Strategy of Deception And Disinformation*. New York: Dodd, Mead, 1984.

Goshko, John M. "For Forgery Specialist, A Case Close to Home." *The Washington Post*. August 19, 1986. https://www.washingtonpost.com/archive/politics/1986/08/19/for-forgery-specialist-a-case-close-to-home/4b8db266-699c-4557-8f01-93db86500599/?utm_term=.8b82773c0db6.

Greenburg, Andy. "Meet Mia Ash, the Fake Woman Iranian Hackers Used to Lure Victims." *Wired.* July 27, 2017. https://www.wired.com/story/iran-hackers-social-engineering-mia-ash/.

Hamburger, Tom and Karen Tumulty. "WikiLeaks releases thousands of documents about Clinton and internal deliberations." *Washington Post*. July 22, 2016. https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/.

"HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group," *FireEye*, July 2015, https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf.

Hancock, Jeffrey T., Jennifer Thom-Santelli, and Thompson Ritchie. "Deception and design: the impact of communication technology on lying behavior," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04)* (2004) 129-134, accessed September 30, 2019, doi: 10.1145/985692.985709.

Hautala, Laura. "Extra sneaky Hammertoss malware acts just like you on your computer." *CNET*. July 29, 2015. https://www.cnet.com/news/hammertoss-extra-sneaky-malware-acts-just-like-you/.

Hayes, Danielle A. "The Trusted Insider: Motives, Behaviors, Fictions, and Digital Age Norms." *American Intelligence Journal* 35, no. 2 (July 2018): 17–25.

Henricks, Steven C. "Social Media, Publicly Available Information, and the Intelligence Community." *American Intelligence Journal* 34, no. 1 (January 2017): 21–31.

Hill, Fiona and Pamela Jewett. "Back in the USSR ": Russia's Intervention in the Internal Affairs of the Former Soviet Republics and the Implications for United States Policy Towards Russia." *Brookings*. (January 1994): 1-90, Ethnic Conflict Project.

Holland, Max. "The Propagation and Power of Communist Security Services Dezinformatsiya." *International Journal of Intelligence and CounterIntelligence 19, no. 6* (2009): 1-31. doi:10.1080/08850600500332342.

"IBM Security Services 2014 Cyber Security Intelligence Index." *IBM*. June 2014. https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

Insikt Group. "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion." *RecordedFuture.* March 6, 2019. https://www.recordedfuture.com/china-social-media-operations/.

Jiang, L. Crystal, Natalya N. Bazarova, and Jeffrey T. Hancock. "From Perception to Behavior: Disclosure Reciprocity and the Intensification of Intimacy in Computer-Mediated Communication." *Communication Research* 40, no. 1 (February 2013): 125–43. doi:10.1177/0093650211405313.

Johnson, Derek B. "DHS plans to step up cyber agreements with private companies." *Federal Computer Week*. December 21, 2017. https://fcw.com/articles/2017/12/21/section9-dhs-cyber-johnson.aspx.

Johnson, Loch K. "The Enduring Myths of Covert Action," *Virginia Policy Review* 7, no. 2 (Winter 2014): 52-64.

_____. *Strategic Intelligence*. Westport, CT: Praeger Security International, 2007.

Jones, Seth G. "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare." *Center for Strategic and International Studies*. October 1, 2018. https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

Juurvee, Ivo. "The Resurrection of 'Active Measures': Intelligence Services as a Part of Russia's Influencing Toolbox." *Strategic Analysis* (April 2018): 1-8, The European Centre of Excellence for Countering Hybrid Threats.

Kelley, Harold H. "The Warm-Cold Variable in First Impressions of Persons." *Journal of Personality* 18, no. 4 (June 1950): 431. doi:10.1111/j.1467-6494.1950.tb01260.x.

Khan, Shehab. "Emmanuel Macron 'A Psychopath Who Hates France', Russian Media Says." *Independent*. 2017. https://www.independent.co.uk/news/world/europe/russian-media-emmanuel-macron-french-president-general-election-2017-gay-psychopath-hates-france-a7723531.html.

Knightley, Phillip. "The History of the Honey Trap." *Foreign Policy.* March 12, 2010. https://foreignpolicy.com/2010/03/12/the-history-of-the-honey-trap/ (accessed May 25, 2019).

Kopan, Tal, Kevin Liptak and Jim Sciutto. "Obama Orders Review of Russian Election-Related Hacking." *CNN.* December 9, 2016. https://www.cnn.com/2016/12/09/politics/obama-orders-review-into-russian-hacking-of-2016-election/index.html.

Kosoff, Maya. "China Has Been Using LinkedIn to Recruit Potential U.S. Spies." *Vanity Fair.* August 31, 2018. https://www.vanityfair.com/news/2018/08/china-has-been-using-linkedin-to-recruit-potential-us-spies.

Kramer, Mark. "The Soviet Roots of Meddling in U.S. Politics," *PONARS Eurasia Policy Memo* No. 452, George Washington University (January 2017).

Kryshtanovskaya, Olga and Stephen White. "Putin's Militocracy." *Post-Soviet Affairs* 19, no. 4 (2003): 289-306, doi:10.2747/1060-586x.19.4.289.

Kuchler, Hannah. "LinkedIn battles China's effort to recruit spies in US." *Financial Times.* August 31, 2018. https://www.ft.com/content/dccfd78e-ad32-11e8-94bd-cba20d67390c.

Langford, James. "Facebook has made fundamental changes since 2016 election, Sandberg says." *Washington Examiner.* January 21, 2019. https://www.washingtonexaminer.com/business/facebook-has-made-fundamental-changes-since-2016-election-sandberg-says.

Leigh, Harold. "The Defence of the Realm: The Authorized History of MI5 by Christopher Andrew." *Guardian*. October 9, 2009. https://www.theguardian.com/books/2009/oct/10/defence-of-the-realm-mi5.

Lin, Herbert. "A Proposal to Reduce Government Overclassification of Information Related to National Security." *Journal of National Security Law & Policy 7*, no. 3 (September 2014): 443–63.

Litvinenko, Alexander and Yuri Felshtinsky. *Blowing Up Russia: The Secret Plot to Bring Back KGB Terror*. New York: Encounter Books, 2007.

Lowenthal, Mark M., *Intelligence: From Secrets to Policy, Sixth edition.* Los Angeles: CQ Press, 2015.

Lucas, Ryan. “Ex-Air Force Counterintelligence Agent Charged with Giving Secrets to Iran.” *NPR*. February 13, 2019. https://www.npr.org/2019/02/13/694234985/ex-air-force-counterintelligence-officer-charged-with-giving-secrets-to-iran/ (accessed May 25, 2019).

_____. "How Russia Used Facebook To Organize 2 Sets of Protesters." *NPR*, November 1, 2017. https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters.

Lynch, Justin. “Cyber Command wants to partner with private sector to stop hacks.” *Fifth Domain.* July 21, 2018. https://www.fifthdomain.com/dod/cybercom/2018/07/31/cyber-command-wants-to-partner-with-private-sector-to-stop-hacks/.

"The Making of a Neo-KGB State." *The Economist*. June 25, 2007. https://www.economist.com/briefing/2007/08/23/the-making-of-a-neo-kgb-state.

Martin, John Bartlow. *Adlai Stevenson and the World: The Life of Adlai Stevenson*. Garden City: Doubleday & Company, 1977.

Matthew, Sam. “Revealed: How Russia’s ‘Troll Factory’ Runs Thousands of Fake Twitter and Facebook Accounts to Flood Social Media with Pro-Putin Propaganda.” *Daily Mail*. March 28, 2015. http://www.dailymail.co.uk/news/article-3015996/How-Russia-s-troll-factory-runsthousands-fake-Twitter-Facebook-accounts-flood-social-media-pro-Putinpropaganda.html.

Mattis, Peter L. “Assessing Western Perspectives on Chinese Intelligence.” *International Journal of Intelligence & Counterintelligence* 25, no. 4 (2012): 684. doi:10.1080/08850607.2012.678745.

May-Chahal, Corinne. “Young People Struggle to Identify Who They Are Talking to Online.” *British Journal of School Nursing* 10, no. 1 (February 2015): 39–40.

Meyers, Adam. “Meet the Advanced Persistent Threats: List of Cyber Threat Actors.” *FireEye*. February 24, 2019. https://www.crowdstrike.com/blog/meet-the-adversaries/.

Mitrokhin, Vasili. *KGB Lexicon: The Soviet Intelligence Officer’s Handbook.* London: Routledge, 2002.

Moore, Paul D. “How China Plays the Ethnic Card.” *Los Angeles Times.,* June 24, 1999. https://www.latimes.com/archives/la-xpm-1999-jun-24-me-49832-story.html.

Morris, Edmund. *Dutch: A Memoir of Ronald Reagan.* New York: Modern Library, 1999.

Nakashima, Ellen. “Russian Government hackers penetrated DNC, stole opposition research on Trump.” June 14, 2016. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?noredirect=on&utm_term=.012baaef8d83.

Nance, Malcolm W. *The Plot to Hack America: How Putin's Cyberspies and Wikileaks Tried to Steal the 2016 Election.* New York, NY: Skyhorse Publishing, 2016.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York: Norton, 2004.

Northcutt, Stephen. “Spear Phishing.” *SANS Technology Institute.* Security Laboratory: Methods of Attack Series. May 9, 2007. https://www.sans.edu/cyber-research/security-laboratory/article/spear-phish.

Oentaryo, Richard J., Arinto Murdopo, Philips K. Prasetyo, and Ee-Peng Lim. “On profiling bots in social media. Proceedings of the international conference on social informatics.” *Social Informatics* (October 2016): 92-109.

Paul, Christopher and Miriam Matthews. "Russia's "Firehose of Falsehood" Propaganda Model." *Perspectives* (July 2016):1-16, https://doi.org/10.7249/PE198.

Phythian, Mark. *Understanding the Intelligence Cycle.* Milton Park, Abingdon, Oxon: Routledge, 2013.

Proctor, Tammy M. *Female Intelligence: Women and Espionage in the First World War.* New York: New York University Press, 2003.

Public Broadcasting Service. “Four Chinese Espionage Investigations.” PBS.org. https://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/four.html (accessed May 12, 2019).

Revelli, Alice and Lee Foster. “Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests.” *FireEye.* May 28, 2019. https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html.

Rowse, Arthur E., and Harold Kellock. "Foreign Policy in National Elections." *Editorial Research Reports 1960*, vol. II (1960): 543-62.

Samuel, Henry. “Chinese spies fooled 'hundreds' of civil servants and executives, France reveals.” *Telegraph.* October 23, 2018. https://www.telegraph.co.uk/news/2018/10/23/chinese-online-spies-fool-hundreds-totally-unprepared-top-french/.

Sawicki, Gérald. "Aux origines lointaines du “service action”. Sabotage et opérations spéciales en cas de mobilisation et de guerre 1871-1914", *Revue Historique des Armées* 13, Issue 268 (August 2012): 12-22.

Schapiro, Leonard. “Totalitarianism in Foreign Policy.” In *The Soviet Impact on World Politics*, by Kurt London, 3-21. Bristol: Hawthorn Books, 1974.

Schoen, Fletcher and Christopher J. Lamb. “Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference.” *Strategic Perspectives,* No. 11 (June 2012): 1-155.

Sciutto, Jim and Pamela Brown. "Russia Hacked GOP Groups, US Intel Believes." *CNN*. December 12, 2016. https://www.cnn.com/2016/12/12/politics/gop-russia-hacking-trump/.

Shane, Scott. “The Fake Americans Russia Created to Influence the Election.” *New York Times*. September 7, 2017. https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

Shortell, David. “Trial begins for former CIA officer accused of spying for China.” *CNN Politics*. May 30, 2018.https://www.cnn.com/2018/05/30/politics/cia-officer-spying-trial-china/index.html.

Shultz, Richard H. and Roy Godson. *Dezinformatsia: Active Measures in Soviet Strategy.* Washington: Pergamon-Brassey, 1984.

Smith, Nicola and Harriet Alexander. “LinkedIn becomes social media of choice for North Korea's elite.” *Telegraph,* October 26, 2018, https://www.telegraph.co.uk/news/2018/10/26/linkedin-becomes-social-media-choice-north-koreas-elite/.

Softness, Nicole A. “Social Media and Intelligence: The Precedent and Future for Regulations.” *American Intelligence Journal* 34, no. 1 (January 2017): 32–37.

Soldatkin, Vladimir and Andrew Osborn. “Putin to Britain: Let's forget about the Skripal poisoning.” *Reuters.* June 6, 2019. https://www.reuters.com/article/us-russia-forum-putin-britain/putin-to-britain-lets-forget-about-the-skripal-poisoning-idUSKCN1T71OU?il=0.

Song, Hwanseok, Jonathon P. Schuldt, Poppy L. McLeod, Rhiannon L. Crain, and Janis L. Dickinson. “Group Norm Violations in an Online Environmental Social Network: Effects on Impression Formation and Intergroup Judgments.” *Group Processes & Intergroup Relations* 21, no. 3 (April 2018): 422–37. doi:10.1177/1368430217733118.

Stamos, Alex. “An Update on Information Operations on Facebook.” *Facebook* (blog). September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/.

Stevens, Candace N. “Technology in Foreign Intelligence Gathering.” *American Intelligence Journal* 34, no. 1 (January 2017): 123–30.

Stober, Dan, and Ian Hoffman. *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage*. New York, NY: Simon & Schuster, 2001.

Strobel, Warren and Jonathan Landay. “Exclusive: U.S. accuses China of 'super aggressive' spy campaign on LinkedIn.” *Reuters.* August 31, 2018. https://www.reuters.com/article/us-linkedin-china-espionage-exclusive/exclusive-us-accuses-china-of-super-aggressive-spy-campaign-on-linkedin-idUSKCN1LG15Y.

Suler, John. “The Online Disinhibition Effect.” *CyberPsychology & Behavior* 7, no. 3 (June 2004): 321–26. doi:10.1089/1094931041291295.

Tahair, Richard. *The Encyclopedia of Cold War Espionage, Spies, and Secret Operations*. Westport: Greenwood Press, 2004.

Tanner, Murray Scot. “Beijing’s New National Intelligence Law: From Defense to Offense.” *Lawfare*. 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

Threat Connect Research Team. "Guccifer 2.0: The Man, The Myth, The Legend?" *ThreatConnect* (blog). July 20, 2016. https://www.threatconnect.com/blog/reassesing-guccifer-2-0-recent-claims/.

Tsikerdekis, Michail and Sheralie Zeadally. “Online Deception in Social Media.” *Communications of the ACM* 57, no. 9 (September 2014): 72-80, doi:10.1145/2629612.

"US accuses China of running aggressive LinkedIn spying program," *Reuters,* September 1, 2018, https://www.pri.org/stories/2018-09-01/us-accuses-china-running-aggressive-linkedin-spying-program.

US Congress, Senate. Initial Findings on Intelligence Community Assessment: *Assessing Russian Activities and Intentions in Recent U.S. Elections*, 115th Cong., 2d sess., 2018, https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.

US Congress, Senate. Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security. 115th Cong., 2nd sess., 2018. S. Prt. 115-21. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

US Department of Homeland Security. *Joint Statement from the Department Of Homeland Security and Office of the lligence on Election Security* (Washington DC: DHS Press Office, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

US Department of State. The Active Measures Working Group. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987.* 1987. 1-89.

US Department of State. United States Information Agency. *Soviet Active Measures in The 'Post-Cold War' Era 1988-1991: A Report Prepared at the Request of the United States House of Representatives Committee on Appropriations by the United States Information Agency.* 1992.

US National Intelligence Council. Office of the Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent US Elections.* January 06, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

van der Walt, Estee, J.H.P. Eloff and Jacomine Grobler. "Cyber-security: Identity deception detection on social media platforms." *Computers & Security* 78, (June 2018): 76-89. doi:10.1016/j.cose.2018.05.015.

Van Swol, Lyn M., Michael T. Braun, and Miranda R. Kolb. "Deception, Detection, Demeanor, and Truth Bias in Face-to-Face and Computer-Mediated Communication." *Communication Research* 42, no. 8 (December 2015): 1116–42. doi:10.1177/0093650213485785.

Verdery, Katherine. *Secrets and Truths: Ethnography In the Archive of Romania's Secret fs Police*. Budapest: Central European University Press, 2014.

Waller, Michael J. *Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare.* Washington, DC: Institute of World Politics Press, 2009.

Warner, Michael. "The Divine Skein: Sun Tzu on Intelligence." *Intelligence & National Security* 21, no. 4 (August 2006): 483–92. doi:10.1080/02684520600885624.

Warner, Michael. *The Rise and Fall of Intelligence: An International Security History.* Washington, DC: Georgetown University Press, 2014.

Wege, Carl Anthony. "Iranian Counterintelligence." *International Journal of Intelligence and CounterIntelligence* 32, no. 2 (April 3, 2019): 272-294. doi:10.1080/08850607.2019.1565274.

Weiner, Rachel. "Former CIA officer Kevin Mallory found guilty of selling secrets to China." *Chicago Tribune*. June 8, 2018. https://www.chicagotribune.com/nation-world/ct-cia-kevin-mallory-guilty-secrets-china-20180608-story.html.

Weir, Fred. "Kremlin official issues death threat in Russian spy scandal. Is the KGB coming back?" *CSMonitor*. November 12, 2010. https://www.csmonitor.com/World/Europe/2010/1112/Kremlin-official-issues-death-threat-in-Russian-spy-scandal.-Is-the-KGB-coming-back.

Williams, Heather J., and Ilana Blum. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica, CA: RAND Corporation. 2018. Accessed November 24, 2019. https://www.rand.org/pubs/research_reports/RR1964.html.

Wise, David. *Tiger Trap: America's Secret Spy War with China.* Boston: Houghton Mifflin Harcourt, 2011.

Wolf, Markus. *Man Without a Face: The Autobiography of Communism's Greatest Spymaster.* New York: PublicAffairs, 1999.

"Wray Stresses Private Sector-FBI Collaboration Against Cyberthreats," *Meritalk*, March 6, 2019, https://www.meritalk.com/articles/wray-stresses-private-sector-fbi-collaboration-against-cyberthreats/.

Yamak, Zaher, Julien Saunier, and Laurent Vercouter. "Automatic Detection of Multiple Account Deception in Social Media." *Web Intelligence (2405-6456)* 15, no. 3 (July 2017): 219–31. doi:10.3233/WEB-170363.

About the Author

Sarah Ogar works in U.S. national security. In her professional and academic pursuits, she seeks to increase her knowledge and experience of countering America's adversaries by surrounding herself with people who are smarter than she is. An Ann Arbor native, she holds a B.A. in English Literature from the University of Michigan. This work marks the completion of a Master of Arts in Government from Johns Hopkins University. She currently resides in California. In her free time, she enjoys traveling, hiking and volunteering with charities that empower women everywhere to reach their full potential.