

Technological Frontiers and Talent Wars: Navigating Intelligence Recruitment in the Digital Age

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Aaryan Amey Dhore

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

MC Forelle, Department of Engineering and Society

Introduction:

In the shadows of global affairs, a covert world operates, where intelligence agencies engage in a perpetual quest to recruit individuals possessing invaluable information and skills. This clandestine endeavor, shrouded in secrecy, has long been shaped by an understanding of human psychology and motivations. However, the rapid pace of technological advancement has disrupted traditional recruitment methods, forcing intelligence communities to evolve. From the meticulous vetting of prospective spies to the strategic deployment of emerging technologies, intelligence agencies navigate a landscape fraught with challenges and opportunities, where the consequences of success and failure extend far beyond classified operations.

This paper examines intelligence recruitment and operations, focusing on the methods, difficulties, and consequences involved. Using perspectives from psychology, technology, and organizational theory, we explore the secretive world of spies, case officers, and the agencies behind their activities.

I begin by surveying the foundational principles that underpin intelligence recruitment, drawing upon scholarly literature and historical precedents to elucidate the psychological frameworks and operational methodologies that shape the recruitment cycle. From the identification of prospective recruits to the cultivation of cover identities and the deployment of covert communication channels, I dissect the intricate strategies employed by intelligence agencies to navigate the espionage landscape.

Venturing further into the digital age, we confront the transformative impact of technology on intelligence agencies. We explore how the rise of social media platforms, facial recognition technologies, and AI-driven algorithms present both unprecedented opportunities and

daunting challenges. Through a critical analysis of contemporary developments and emerging trends, we unravel the intricate interplay between human actors and technological systems, exploring the implications for recruitment practices and operational effectiveness. Moreover, we examine the responses of intelligence agencies to the evolving recruitment landscape, from the outsourcing of operations to private firms to the implementation of innovative talent exchange programs and the establishment of research initiatives such as CIA Labs. Through an examination of government documents, scholarly literature, and firsthand accounts, we uncover the underlying motivations and implications of these strategic maneuvers, interrogating their efficacy in addressing recruitment challenges and sustaining competitive advantages.

Ultimately, this paper contends the active adoption and creation of technology enables agencies to recruit skilled individuals more easily. By synthesizing diverse perspectives and methodologies, we endeavor to provide a comprehensive understanding of the dynamic forces shaping intelligence recruitment and operations in the contemporary landscape.

Literature Review:

Intelligence agencies employ a meticulous process when recruiting spies, guided by a nuanced understanding of human behavior and motivation. There are two types of spies: individuals recruited in other countries to commit espionage and US officials sent to extract information. The majority of past research focused on recruiting individuals to commit espionage. Wilder (2017) suggests that self-interest often drives individuals towards clandestine activities. Entry into espionage typically hinges on three key elements: personal dysfunction, crisis, and opportunity. Individuals facing challenges such as relational strife, familial discord, or financial turmoil may find themselves susceptible to exploitation, thereby becoming viable targets for recruitment. Burkett (2013) outlines a structured Agent Recruitment Cycle,

comprising six sequential stages. First, agencies engage in spotting, wherein they identify potential recruits based on predetermined criteria. Subsequently, these individuals undergo assessment to ascertain their possession of desired information and to evaluate their motivations, vulnerabilities, and suitability for espionage activities. Following this, agencies enter the development phase, where they establish rapport with potential recruits and delve deeper into the aforementioned factors. The recruitment process then proceeds to the formal recruitment stage, where agents are officially brought into the fold. Training ensues, involving briefings, task assignments, and debriefings to prepare agents for their roles. Finally, the cycle concludes with turnover or termination, wherein agents may be transferred to another case officer or the relationship may be terminated altogether.

During the recruitment process, it is imperative that case officers (recruiters) are able to establish contact with prospective spies to evaluate their motivations and trustworthiness. An internal study done by the CIA found that “personal meetings are required for agents assigned agent-organizational tasks, particularly the recruitment of new agents; these obviously cannot do their work without consultations” (Konovalov & Sokolov, 1996, p. 4). However, despite their necessity, such encounters pose inherent risks and logistical challenges. These meetings can take months or even years to plan and pose great logistical and safety issues. It could require exporting the prospective spy to the US or a neutral country endangering the prospect or the meeting might require the case officer to go to the spy. In both situations, either or both parties are at great risk. In the latter case, case officers often adopt a cover identity. These fabricated personas serve as a veil of protection, enabling officers to engage with potential recruits discreetly. These covers were easy to design and were designed to last across multiple missions (Lucas 2020). While personal meetings pose great risk, through the anonymity offered by cover

identities, such meetings were able to be accomplished enhancing the effectiveness of spy recruitment.

While spies were scouted by case officers and intelligence officers, the officers themselves were predominantly recruited through the military. Recruitment into intelligence officer positions within the US Army, for instance, often relied on individuals achieving high scores on the Armed Services Vocational Aptitude Battery (ASVAB) tests, as noted by Richard White, a former Counterintelligence officer ("How Are Intelligence Personnel Chosen or Recruited?" 2021). Additionally, specialized training programs such as the Intelligence Staff Officer Courses were primarily accessible to military personnel, effectively limiting opportunities for civilians to join intelligence ranks (*Intelligence Staff Officer Course*, 2004). This recruitment paradigm underscored the military's central role in shaping intelligence personnel, reflecting a historical emphasis on internal talent cultivation within military structures.

Intelligence agencies have exhibited a notable increase in financial investments towards research and development, particularly in the realms of cyber security and emerging technologies. Over the past two decades, the FBI has augmented its budgetary allocations towards cybersecurity initiatives, as evidenced by the Fiscal Year 2024 budget request which asks for a "\$63.4 million to enhance cyber information-sharing abilities and increase cyber tools and capacities ... and \$27.2 million to help protect internal FBI networks" (Federal Bureau of Investigation, 2023). Comparatively, in 2002 the FBI asked for "\$28,144,000 for providing specialized technical assistance to field investigators and for developing investigative tools for law enforcement to counter the use of digital technology" (Federal Bureau of Investigation, 2002). Similarly, the Department of Defense (DoD) has demonstrated a proactive stance towards

technological advancement, with a recommended spending increase on artificial intelligence (AI) for cybersecurity purposes (DiMolfetta, 2022). Key allocations comprise a \$75 million increase for DARPA, a \$50 million boost for AI applications within the US Cyber Command, and \$20 million in investments in quantum computing technologies. Such strategic financial outlays underscore the intelligence agencies investments towards adapting to an evolving threat landscape and capitalize on emerging technological frontiers to safeguard national security interests.

The advent of artificial intelligence (AI) has catalyzed a global race among governments to position their intelligence agencies at the forefront of technological progress. AI techniques, including machine learning and evolutionary algorithms, offer the promise of “more precise, faster, and scalable outcomes in big data analytics” (Rahmani et al. 2021, p. 1). Recognizing the transformative potential of AI, Richard, the CIA's chief cyber policy advisor, emphasized the imperative for agencies to integrate AI applications within their activities (Williams, 2023). To ensure fast development and adoption of such technologies, the Biden administration has passed an executive order to attract more AI talent internationally to the US government. It offers initiatives offering immigrant and non-immigrant pathways for foreign nationals to contribute their expertise to federal agencies (Nihill, 2023). This concerted effort to harness AI talent reflects a recognition of its strategic importance in maintaining competitive advantages in intelligence operations and underscores the urgency with which governments are embracing AI-driven approaches to meet evolving security challenges.

Methods:

In this study, Actor Network Theory (ANT) serves as the primary theoretical framework, providing a lens through which to examine the intricate interactions between human and

non-human actors within the context of intelligence recruitment and operations. Central to ANT is the concept of "actorhood," which emphasizes that both humans and non-humans have agency and the capacity to act in ways that influence outcomes. This perspective challenges traditional views that prioritize human agency over the influence of non-human entities. Instead, ANT posits that agency emerges from the interactions and associations between actors, regardless of their material or social nature. Through ANT, the analysis delves into the dynamic interplay between various entities involved in intelligence endeavors, including human actors such as intelligence officers, spies, and policymakers, as well as non-human actors such as social media platforms, AI tools, the internet, and communicational technologies. (Latour, 1996).

The research methodology encompasses the collection and synthesis of recent secondary sources reporting on attacks, vulnerabilities, and intelligence practices from diverse nations, along with academic literature analyzing the relationships between intelligence agencies and private firms. This includes studies published within the past two decades to ensure the incorporation of the most up-to-date information reflecting the impact of innovations such as social media, AI technology, and mass data/internet on intelligence recruitment and operations. Additionally, publicly available documents from government agencies, particularly the CIA and FBI, will be used to examine restructuring efforts and past operational practices within this timeframe. By employing a multifaceted approach that combines qualitative analysis of recent secondary sources and examination of official documents, this study aims to provide a comprehensive understanding of the evolving landscape of intelligence recruitment and operations in the context of technological advancements over the past two decades.

Analysis

Due to the adoption of mass surveillance technologies, cover identities have been harder to create and maintain. Israeli companies have pioneered the deployment of facial recognition technologies, a trend that has proliferated globally, particularly in China and other nations (Lucas 2019). The facial recognition software, with its ability to match individuals' faces to known identities, poses a significant risk to individuals operating under cover identities, as even a fleeting encounter captured by surveillance cameras could potentially unveil their true identities and compromise their covert status. Simply, the risk of identification and exposure has increased exponentially. However, these facial recognition systems are relatively simplistic compared to systems that other countries have put in place. Singapore has created a database that tracks real-time data on traveler's movements including flight schedules, customs records, hotel bookings, and taxi journeys. If an individual takes a bit too long to get to their hotel, the system can trigger an alert at which point the authorities would monitor TVs and phones of the suspicious traveler (Dorfman & McLaughlin, 2019). With the ability to monitor travelers' movements and detect anomalies in their activities, intelligence agencies face increased challenges in maintaining the secrecy and authenticity of cover identities, potentially jeopardizing covert operations and compromising the safety of undercover agents. Given that cover identities were used to hold personal meetings with prospective spies, these meetings have become much harder to execute. They pose a much larger risk to both the case officer and the spy themselves.

While in-person meetings have become near impossible to execute safely, case officers are rapidly utilizing technology to circumvent these challenges. Officers can use social media, online chat rooms, and instant messaging to assess potential agents virtually. Nowadays, officers don't need to even resort to that. According to leaked internal CIA documents, agencies have

developed and used tools to hack into individual's phones, TVs, and cars to extract their private information (Timberg et al., 2017). This information could be used to judge potential spies' financial and emotional stability. A case officer can learn information about a potential agent in a matter of minutes, a process that may have taken many years to learn through face-to-face contacts. The active approach to use and create technologies have enabled case officers to make the recruitment process more efficient.

In the realm of intelligence recruitment, a person's digital footprint has become a pivotal factor in evaluating their suitability for covert roles. Intelligence agencies are disqualifying promising candidates due to compromising statements made on social media. Even after being hired by agencies like the CIA or FBI, they advise maintaining a visible presence on social media to avoid arousing suspicion (Pagliery, 2015). This necessity for caution extends beyond the recruitment process, emphasizing the ongoing need for discretion in all aspects of an operative's professional life. Former CIA Operations Officer Douglas London suggests that operatives can strategically leverage their existing online personas to enhance their cover. Thus, rather than viewing social media presence as inherently detrimental to covert operations, London's insights underscore the potential for operatives to adeptly navigate the digital landscape and utilize social media as a tool to reinforce their cover identities. Previously, agents were told to be untraceable, and initially there were mixed protocols from agencies regarding social media use (Hiskey, 2022). However, agencies now are wholefully accepting it and are evenly actively using it to assist in the maintenance of covers.

Social media has not only played a role in evaluating suitability, but also has been used by agencies themselves to find potential candidates themselves. Entities like the NSA are using social media platforms, primarily LinkedIn, to scoop up domestic tech talent that have been

displaced from companies (McGraw, 2023). Similarly, Chinese intelligence operatives have been observed utilizing LinkedIn to target potential foreign recruits discreetly. They specifically target “academics and people outside China who have just left their government jobs” (Lee, 2019). Recruiters are using social media platforms to recruit both local and foreign talent with great efficiency. As William R. Evanina, the director of the National Counterintelligence and Security Center stated, ““Instead of dispatching spies to the U.S. to recruit a single target, it’s more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles’”” (Schlosser, 2019). Simply, social media offers distinct advantages over traditional recruitment approaches, providing a safer and more discrete means for spotting potential recruits and facilitating rapid outreach.

The reluctance of intelligence agencies to actively develop internal talent and infrastructure, opting instead to rely heavily on private contractors for technological advancement, has resulted in significant recruitment challenges and an exodus of experienced personnel to private firms. As a result of the events of 9/11 and George W. Bush's Global War on Terror, significant funds were allocated towards the advancement of new technical systems, including imagery and signal intelligence satellites. At the time, the United States Intelligence Community (ICs) did not have the appropriate infrastructure or internal talent to develop such technologies. Therefore, instead of investing within themselves, ICs looked towards the private sector where firms were more specialized and fueled by competition boosting innovation. They hired thousands of contractors and gave private firms massive contracts to develop technologies. This behavior continued where a staggering 51% of the Defense Intelligence Agency's staff are now contractors, with private firm contracts constituting approximately 70% of intelligence agencies' budgets (Krishnan, 2011). While ICs were able to expedite the development process,

the transition came at a cost. Due to the lack of internal development, ICs have become reliant on private firms for their needs. These firms, in fierce competition with each other, are scooping up top talent through large salaries to boost their technological capabilities. These large salaries are nearly double as much as normal government employees (Rosenbach & Peritz, n.d). Fiscally motivated, employees from ICs have been migrating towards private firms. The exodus of experienced personnel from ICs to contracting firms poses retention challenges but also compounds the difficulty of attracting new talent. In the development of technology, agencies were more reluctant to take an active approach. The passive strategy they adopted ultimately diminished the diversity of skilled individuals within ICs and raised issues concerning the recruitment of fresh talent as well.

Intelligence agencies are only able to move forward in the recruitment of professionals by taking a more active role in the usage and development of technologies. In response to the IC's drain of technical experts, intelligence agencies have initiated innovative programs aimed at attracting skilled professionals back by offering specialized opportunities and more lucrative incentives. One such initiative is the implementation of public-private talent exchange programs. Intelligence officers undertake rotational assignments at private sector companies to develop deeper skills in specific technology and policy areas while private sector employees are sent to ICs (Justin, 2023). These assignments, lasting between 3 to 12 months, not only enable officers to acquire new expertise but also serve to expand awareness within the IC about job opportunities in the private sector. Additionally, the establishment of CIA Labs represents a proactive effort by intelligence agencies to foster innovation and retain talent. CIA Labs allows researchers to publicly file patents and collect a portion of the profits (Howell, 2020). By incentivizing researchers with the opportunity to profit from their inventions and contribute to

leading fields such as AI and biotechnology, the CIA aims to bolster its ability to attract and retain top talent, thereby enhancing its technological capabilities and maintaining its competitive edge in an evolving intelligence landscape.

While intelligence agencies should be proactive in adopting new technologies to overcome recruitment challenges, this effort should still be careful and deliberate to avoid unintentional consequences. As more development and research is dedicated to AI, certain models have been created for the assessment of potential applicants and recruits. There are some companies dedicated to using AI for talent acquisition: some focusing on scouting and others on screening applicants. Regardless, they advertise to streamline the hiring process and make it more cost-efficient. However, the active adoption of these technologies have the potential to hurt recruitment. Specifically, the inherent algorithmic bias within these systems can result in discriminatory hiring based on race, gender, ethnicity, personality traits, and religion (Chen 2023). Simply, blindly adopting technology without understanding their pitfalls can lead to more harm than good. While the active creation and adoption of technologies have undoubtedly transformed and enhanced recruitment processes within intelligence agencies, it is imperative to acknowledge the nuanced challenges and ethical considerations that accompany their implementation. As ICs embrace the potential of emerging technologies, they must remain vigilant of their unintended consequences that could exacerbate inequalities and hinder the fair and equitable evaluation of candidates. Striking a balance between technological innovation and ethical oversight will be essential to harnessing the full potential of these tools while mitigating their risks in recruitment practices moving forward.

Conclusion:

In an era characterized by rapid technological advancement, the emergence of new technologies has fundamentally reshaped the landscape of intelligence recruitment and operations. These agencies have faced significant shifts in their operational tactics, exemplified by the increasing difficulty in maintaining cover identities amidst the pervasive scrutiny of facial recognition systems and real-time tracking databases. However, the active adoption of technology also enables them to circumvent issues. Case officers can use social media to spot and assess potential spies, greatly speeding the recruitment cycle. Similarly, agencies have used these platforms to identify and engage with displaced technical talent, but when intelligence agencies fail to actively engage in the creation and development of technologies, it results in recruitment challenges, hindering their ability to attract and retain top talent in an increasingly competitive landscape. Therefore, the establishment of specialized labs and research opportunities is not only essential for maintaining a technological edge but also serves as a critical component in bolstering recruitment efforts. While I urge agencies to maintain an active approach with technology for recruitment, it is important that technologies are not blindly accepted. They must be scrutinized and understood to ensure we minimize and mitigate potential consequences.

As intelligence agencies navigate the evolving landscape of recruitment technology, it is necessary to strike a balance between innovation and ethical responsibility, ensuring that the potential benefits of technology are realized while safeguarding against its unintended consequences. Moving forward, agencies must view technology as a tool to enhance recruitment efforts, but with a critical eye towards understanding and mitigating potential consequences. This work calls for a balanced approach that prioritizes innovation while remaining ethically

responsible, ensuring that technological advancements serve to improve recruitment practices while safeguarding against unintended negative impacts.

References

- Burkett, R. (2013, March). An Alternative Framework for Agent Recruitment: From MICE to RASCLS. *Studies in Intelligence*, 57(1).
<https://www.cia.gov/resources/csi/static/9ccc45dc156271d11769e5205ec49c29/Alt-Framework-Agent-Recruitment-1.pdf>
- Chen, Z. Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications* 10, 567 (2023).
<https://doi.org/10.1057/s41599-023-02079-x>
- DiMolfetta, D. (2022, December 22). *2023 defense bill supports DOD adoption of more AI for cybersecurity*. S&P Global. Retrieved February 17, 2024, from
<https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/2023-defense-bill-supports-dod-adoption-of-more-ai-for-cybersecurity-73477388>
- Dorfman, Z., & McLaughlin, J. (2019, December 30). *'Shattered': Inside the secret battle to save America's undercover spies in the digital age*. Yahoo News. Retrieved March 1, 2024, from
https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAE-yC6mSBOzxWIKH1YtECSJCqLCemKHvNxLc70QqpTsOwYUxt
- Federal Bureau of Investigation. (2002). *FY 2002 Budget Request*. FBI Archives. Retrieved February 17, 2024, from
<https://archives.fbi.gov/archives/news/testimony/fy-2002-budget-request>

Federal Bureau of Investigation. (2023, April 27). *Federal Bureau of Investigation Budget Request For Fiscal Year 2024*. FBI. Retrieved February 17, 2024, from <https://www.fbi.gov/news/testimony/federal-bureau-of-investigation-budget-request-for-fiscal-year-2024>

Grigorij Serscikov (2024) 'Tell him that he is different': how U.S. intelligence tried to recruit the Soviets in Iran, *Journal of Intelligence History*, 23:1, 20-39, DOI: 10.1080/16161262.2022.2129824

Hiskey, D. (2022, December 1). *How Do Spy Agencies Actually Recruit Spies in Real Life?* Today I Found Out. Retrieved March 1, 2024, from <https://www.todayifoundout.com/index.php/2022/12/how-do-spy-agencies-actually-recruit-spies-in-real-life/>

How are intelligence personnel chosen or recruited? (2021, September 5). Quora. Retrieved February 17, 2024, from <https://www.quora.com/How-are-intelligence-personnel-chosen-or-recruited>

Howell, P. (2020, September 21). CIA's new tech recruiting pitch: More patents, more profits. *MIT Technology Review*. Retrieved March 1, 2024, from <https://www.technologyreview.com/2020/09/21/1008654/cias-new-tech-recruiting-pitch-more-patents-more-profits/>

Intelligence Staff Officer Course [Website]. (2004, 5 5). CIA Reading Room. Retrieved 2 16, 2024, from <https://www.cia.gov/readingroom/docs/CIA-RDP55-00110A000100080003-4.pdf>

jj838. (2023, July 19). *Intelligence agencies are trying to poach tech talent. You can do better than them*. ClearanceJobs Blog. Retrieved February 17, 2024, from

<https://discuss.clearancejobsblog.com/t/intelligence-agencies-are-trying-to-poach-tech-talent-you-can-do-better-than-them/16819>

- Justin, D. (2023, December 4). *Intel agencies look to build skills through public-private talent exchange*. Federal News Network. Retrieved March 1, 2024, from <https://federalnewsnetwork.com/inside-ic/2023/12/intel-agencies-look-to-build-skills-through-public-private-talent-exchange/>
- Konovalov, A. A., & Sokolov, V. S. (1996, 7 2). Meeting with Agents. *CIA Historical Review Program*. <https://www.cia.gov/static/Meeting-with-Agents.pdf>
- Krishnan, A. (2011). The Future of U.S. Intelligence Outsourcing. *The Brown Journal of World Affairs*, 18(1), 195–211. <http://www.jstor.org/stable/24590792>
- Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, 47(4), 369–381. <http://www.jstor.org/stable/40878163>
- Lee, Y. N. (2019, August 28). China is reportedly using LinkedIn to recruit spies overseas. *CNBC*. Retrieved March 1, 2024, from <https://www.cNBC.com/2019/08/28/china-is-reportedly-using-linkedin-to-recruit-spies-overseas.html>
- Lucas, E. (2019, April 27). *The Spycraft Revolution*. Foreign Policy. Retrieved Feb 15, 2024, from <https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/>
- McGraw, M. (2023, February 13). *NSA Set to Snap Up Displaced Tech Talent*. PSHRA. Retrieved March 1, 2024, from <https://pshra.org/nsa-set-to-snap-up-displaced-tech-talent/>
- Nihill, C. (2023, December 21). *AI talent wanted: The federal government is searching far and wide to fill new cutting-edge positions*. FedScoop. Retrieved February 17, 2024, from <https://fedscoop.com/ai-talent-wanted/>

- Pagliery, J. (2015, March 13). Want to be a CIA spy? Be careful on Facebook. *CNN Business*. Retrieved March 1, 2024, from <https://money.cnn.com/2015/03/13/technology/security/cia-facebook-rules/>
- Rahmani AM, Azhir E, Ali S, Mohammadi M, Ahmed OH, Yassin Ghafour M, Hasan Ahmed S, Hosseinzadeh M. Artificial intelligence approaches and mechanisms for big data analytics: a systematic study. *PeerJ Computer Science*. 2021 Apr 14;7:e488. doi: 10.7717/peerj-cs.488.
- Rosenbach, E., & Peritz, A. J. (n.d.). The role of Private Corporations In The Intelligence Community. *Harvard Kennedy School*. <https://www.belfercenter.org/sites/default/files/legacy/files/private-corporations.pdf>
- Schlosser, K. (2019, August 27). *New York Times report calls out LinkedIn as an 'ideal' vehicle for China to recruit spies*. GeekWire. Retrieved March 1, 2024, from <https://www.geekwire.com/2019/new-york-times-report-calls-linkedin-ideal-vehicle-china-recruit-spies/>
- Timberg, C., Dwozkin, E., & Nakashima, E. (2017, March 7). WikiLeaks: The CIA is using popular TVs, smartphones and cars to spy on their owners. *The Washington Post*. Retrieved March 29, 2024, from <https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-our-tvs-smartphones-and-cars-for-spying/>
- Wilder, U. M. (2017, June). The Psychology of Espionage. *Intelligence Studies*, 61(2). <https://www.cia.gov/static/9ccc45dc156271d11769e5205ec49c29/Alt-Framework-Agent-Recruitment-1.pdf>

Williams, L. C. (2023, October 5). *The CIA's data-challenged AI imperative*. Defense One.

Retrieved February 17, 2024, from

<https://www.defenseone.com/defense-systems/2023/10/cias-data-challenged-ai-imperative/390994/>