Advancements in Technical Tradecraft for Online Intelligence Operations

Evolution of Training Methods and Skill Sets in Modern Intelligence Operations

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Aaryan Dhore

10/26/2023

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.

ADVISORS

MC Forelle, Department of Engineering and Society
Briana Morrison, Department of Computer Science

Introduction

The evolution of technology has not only rendered traditional methods of espionage obsolete but has also ushered in a new and complex array of threats on the international stage. Some of the most fundamental parts of intelligence are now rendered useless through these technological advancements. Previously iron-clad cover identities can now be cracked in a matter of seconds through facial recognition technology and digital footprint analysis. Agencies now have to deploy more sophisticated and expensive ways to maintain cover identities but at their best the identities are only good for a one time use (Lucas, 2020). Furthermore, the ease with which information can be shared, manipulated, and accessed globally has exposed vulnerabilities in traditional espionage strategies. Cyber espionage, misinformation campaigns, and electronic subversion have become potent tools in the hands of state-sponsored actors and rogue organizations. The interconnectedness of the digital world has enabled adversaries to exploit these tools, disrupting political processes, sowing discord, and compromising national security in unprecedented ways all within their own boundaries. For example, the Internet Research Agency, a Russia sponsored agency, created fake accounts mimicking Democratic candidates and official campaign committees during the 2020 elections. They used names and materials of legitimate domestic nonprofits and grassroots organizations and employed seemingly nonpolitical or commercial content to disguise their political activities (Kim, 2020). Traditional methods of espionage have no counters or defense to this type of foreign spying. This shifting landscape necessitates not only a reevaluation of traditional intelligence methods but also a proactive approach to understanding, countering, and adapting to the emerging challenges posed by these technological advancements on the international stage.

The integration of emerging technologies, particularly artificial intelligence (AI), within the realm of intelligence has ushered in a new era of efficiency and capability. These technological tools have significantly enhanced agencies' data processing and analysis capacities. AI, in its various forms, has become instrumental in geospatial, signals, human, and open-source intelligence, allowing for rapid analysis of vast datasets and identification of crucial patterns (Katz, 2020). However, amidst this technological surge, the human presence remains irreplaceable. As highlighted by former CIA officer Rober Grenier, the nuanced, context-driven interactions that humans comprehend are beyond the scope of technological methods alone (Human intelligence, n.d.). While AI can process immense volumes of data, human intelligence is essential to contextualize the information, assess its reliability, and discern subtle nuances. The collaboration between advanced AI systems and human expertise becomes imperative in navigating the complexities of modern intelligence challenges.

Moreover, the rapid development of AI and other emerging technologies has initiated a global 'space race' of sorts, with nations like China and Russia rapidly advancing their capabilities (Katz, 2020). This competitive environment underscores the urgency for intelligence agencies to train their operatives adeptly. Ensuring that agents possess not only a deep understanding of these technologies but also the ethical and strategic acumen to employ them responsibly is paramount. Intelligence professionals must be equipped not just to utilize these technologies but also to critically evaluate their outputs, recognizing potential biases and limitations. This training is crucial not only for maintaining a competitive edge on the global stage but also for safeguarding national security interests in an increasingly interconnected and technology-driven world. Balancing technological proficiency with human judgment is not merely a choice but a necessity in the evolving landscape of intelligence, emphasizing the critical

need for comprehensive and forward-thinking training programs for the intelligence operatives of the future.

The rapid advancements in internet and communication tools has made it easier for agencies to conduct remote surveillance, cyber espionage, and communication. These types of missions are more cost effective and efficient as agents can cover a broad range of targets over extended periods of time without worrying about the logistical or safety challenges of physically deploying agents (Dehlinger, 2020). Therefore, the final STS deliverable will explore how the evolving landscape of intelligence, marked by advancements in technology, impact the recruitment and training of intelligence officers. It will explore the specific skills, knowledge, and ethical considerations that are essential for intelligence operatives, and how training programs can be adapted to equip them effectively.

To remain on the competitive edge for foreign espionage and domestic security, new technologies must also be developed. The technical project will focus on the developments of such technologies during my internship.

Technical Project

Specifically, in missions reliant on online communication with targets the agents must maintain two major things: anonymity and trust with the target. To maintain anonymity and an untraceable connection, the agent relies on existing technologies. There are many options that are used. One common option is using a TOR browser which hides sensitive information like IP addresses, a type of digital fingerprint, and browsing history by routing traffic through multiple nodes in the TOR network (Newman, 2019). Another method of communication used by agents is chat systems in video games which are often unmoderated. (Silva, 2021). Virtual private networks (VPNs) are also commonly used to hide browsing history, IP addresses, and true

location of officers (Rana et al., 2022). To establish trust with the target, the agent relies on their social engineering skills and cover identity to create rapport. The social engineering aspect lies fully on the agent and their training (Yadegari, 2023). However, technology can assist with creating cover identities. In the digital realm, the cover identity has two parts to it: legend and technical tradecraft. A legend is essentially a detailed, fictitious background story that an undercover agent adopts to establish a credible cover identity. A legend includes details about personal history, social connections, professional experience, hobbies, etc (Dorfman, 2019). Technical tradecraft refers to the methods to disguise technologies used (Intelligence Academy: Getting Professional Tradecraft Training, n.d.). For instance, consider an agent communicating with targets in Mexico while operating a computer set to Eastern Standard Time, devoid of any browser history. In such scenarios, the authenticity of the communication can rapidly deteriorate, jeopardizing the mission's success. Therefore, technical tradecraft has gained prominence, especially in missions reliant on online communication for evidence gathering or luring targets into traps. The ability to skillfully manipulate digital footprints, timestamps, and other technical aspects has become a fundamental skill for intelligence operatives, underscoring the critical role of technical tradecraft in maintaining the authenticity and effectiveness of modern espionage endeavors. In the technical portion of the paper, I will focus on what new technologies are being created for advancing technical tradecraft and my specific contributions.

To address this, I will draw on experience from my previous internship. The project was centered on maintaining technical tradecraft to make computer/network connections appear as genuine as possible to the target. Unlike other technologies, our solution allowed operatives to customize their setup to suit specific missions, selecting applications, browser history, keyboards, and more. Additionally, our solution could generate virtual machines (VMs) with

desired configurations instantly. This software-based approach saved agencies money and enhanced security, eliminating the need for frequent purchases of disposable "burner" laptops. In contrast, other technologies lacked this customizability, providing blank slates that required time-consuming setup tailored to the target/mission.

STS Project

The internet and artificial intelligence has significantly transformed the landscape of intelligence operations. Traditional, in-person missions that once characterized espionage are gradually diminishing, making way for a new era of remote intelligence gathering. This shift is primarily driven by the increasing reliance on digital communication, data analysis, and cyber capabilities. Intelligence agencies now harness the power of AI algorithms to process vast amounts of information, identify patterns, and extract valuable insights (Katz, 2020). Consequently, the nature of intelligence work has evolved, emphasizing skills in data analytics, cybersecurity, digital forensics, and machine learning, which were not as prominent in the past.

This evolution in intelligence methods necessitates a redefinition of skill sets required for modern intelligence officers. In the past, field operatives relied heavily on traditional espionage skills such as physical surveillance, disguise, and interrogation techniques. Now, these skills are complemented by expertise in cyber operations, coding, information security, and data analysis. Intelligence officers need to understand the intricacies of digital communication, recognize cyber threats, and adapt to rapidly changing technological landscapes.

Understanding the intricate ways in which technology impacts training and skill sets is of paramount importance for intelligence agencies' strategic resource allocation. By pinpointing the specific technical proficiencies required, agencies can strategically design training programs and allocate budgets accordingly, ensuring that operatives possess the essential skills vital for their

mission success. This strategic approach not only equips agents to navigate the complexities of modern intelligence but also allows agencies to swiftly adapt to emerging technologies, reducing the risk of obsolescence and bolstering their competitiveness within the intelligence landscape (Dalton, 2002). Moreover, the political dimension of assessing the influence of technical tradecraft on intelligence operations is vital for informed decision-making at the national level. Policymakers and politicians require deep insights into the evolving role of technology in intelligence to make judicious choices regarding national security priorities and resource allocation. Understanding the capabilities and constraints of technical tradecraft empowers governments to formulate comprehensive intelligence strategies aligned with national security objectives, ensuring a proactive and adaptive stance in the face of evolving technological challenges (Lebovic, 2010). The final STS deliverable focus on how the technological innovations in artificial intelligence, internet, and computational power impacts the recruitment and training methods of US intelligence officers.

Research will primarily involve examining the historical aspect of this question, investigating how previous technological developments have driven the evolution of training within intelligence agencies. Historical context serves as a valuable predictor of future trends, offering insights into how agencies may adapt in response to changing technological landscapes since the 2000sFurthermore, I will employ the Actor-Network Theory framework to analyze specific case studies within intelligence agencies. ANT's focus on human and non-human actors will allow me to explore the intricate relationships and power dynamics shaping training and recruitment methods (Cressman, 2009). The human actors are the intelligence officers, and the non-human actors I will be focusing on will be the technologies they use. Specifically, I will focus on AI systems, internet communication tools, and cybersecurity technologies. On top of

understanding the interactions between these non-human actors and the intelligence officers, a technological evaluation will be conducted to understand the true capabilities of these tools and systems. By studying the current power and weaknesses of these systems, we can understand how these technologies may change in the future and make recommendations based on the predicted technological trends. By dissecting these socio-technical networks, I aim to identify key factors influencing intelligence officers' skill sets in response to emerging technologies and propose strategies for effective training programs.

Conclusion

In the evolving landscape of intelligence, where technology has both disrupted traditional methodologies and empowered agencies, a multifaceted approach is crucial. The technical project delves into the heart of modern espionage, where online communication demands both anonymity and trust. The technical project's contribution lies in advancing these techniques, enhancing agents' ability to operate effectively and securely in the digital sphere. Meanwhile, the STS project critically examines the changing skill sets required for intelligence officers. The digital era demands expertise in data analytics, cybersecurity, and AI interpretation, reshaping traditional espionage skills. Understanding this transformation is crucial for resource allocation within agencies, ensuring operatives are equipped to handle emerging challenges.

This symbiotic blend of technical prowess and strategic training stands as the cornerstone of contemporary intelligence operations. As the digital world and human ingenuity continue to intertwine, this synergy equips intelligence agencies to navigate the complexities of the digital age, fortifying nations against emerging threats. In this era of rapid technological advancement, these deliverables not only enhance the efficiency of intelligence gathering but also reinforce the essence of national security. As we move forward, this fusion of cutting-edge technology and

strategic expertise guarantees a future where nations are safeguarded, ensuring peace and stability in an ever-changing world.

References

Cressman, D. (2009). A Brief Overview of Actor-Network Theory: Punctualization, Heterogenous Engineering & Translation. https://summit.sfu.ca/item/13593

Dalton, W. H. (2002, Autumn). Intelligence: From Secrets to Policy. (Book Reviews). Naval War College Review, 55(4), 119+. https://link.gale.com/apps/doc/A95259487/AONE?u=anon~7d72387f&sid=googleScholar&xid=780bd4a1

Dehlinger, K. (2020). Espionage in the Digital Age: How Technology is Impacting the Recruitment and Handling of Spies [Plan II Honors Thesis, University of Texas at Austin]. https://doi.org/10.26153/tsw/11267

Dorfman, Z., & McLaughlin, J. (2019, December 30). 'Shattered': Inside the secret battle to save America's undercover spies in the digital age. *Yahoo News*. https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html?guccounter=1

Human intelligence. (2012, March 22). University of Delaware. Retrieved November 26, 2023, from https://www1.udel.edu/udaily/2012/mar/global-agenda-grenier-032212.html

Intelligence Academy: Getting professional tradecraft training. (n.d.). https://academy.ieis.eu/mod/page/view.php?id=168#:~:text=Generally%2C%20it%20simply%20refers%20to,used%20by%20human%20intelligence%20operators.

Katz, B. (2020, April 17). *The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence*. CSIS. https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence

Kim, M. (2020, March 5). *New Evidence Shows How Russia's Election Interference Has Gotten More Brazen*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more

Lebovic, J. H. (2010). [Review of Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War, by R. Jervis]. *Perspectives on Politics*, 8(4), 1167–1169. http://www.jstor.org/stable/40984296

Lucas, E. (2020, May 6). The Spycraft Revolution. *Foreign Policy*. https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/

Newman, L. H. (2019, May 7). The CIA Sets Up Shop on Tor, the Anonymous Internet. *WIRED*. https://www.wired.com/story/cia-sets-up-shop-on-tor/

Silva, B. C. M. a. S. (2021, September 22). Extremists using video-game chats to spread hate. *BBC News*. https://www.bbc.com/news/technology-58600181

Yadegari, S. (2023, July 6). A Warning From the FBI: How Bad Actors Use Social Engineering to Enable Hacking of Academia. *Chapman Blogs.* https://blogs.chapman.edu/information-systems/2023/07/06/a-warning-from-the-fbi-how-bad-actors-use-social-engineering-to-enable-hacking-of-academia/