Self-Reflection on

CAC 620 – Counter-Intelligence

by

Alejandro F. Sosa

This Unclassified paper was submitted to the faculty of the National Intelligence University in partial fulfillment of the requirements for the Master of Science and Technology Intelligence Portfolio.

October 2024

Introduction

I enjoyed CAC-620, Counterintelligence because it provided me a deeper understanding of the threats posed by foreign intelligence activities and how the United States responds to them strategically. Through the exploration of espionage, influence operations, economic espionage, and cyber intrusions, I gained a broader perspective on the significance of CI efforts in protecting national security and economic interests. The course's integration of theory, policy, and practical case studies has expanded my knowledge and strengthened my analytical skills. I really appreciated the nuance that the professor brought to this subject from his time as the OUSDI&S portfolio lead for counterintelligence. This reflection focuses on key takeaways, particularly the role of CI within the Intelligence Community (IC) and the strategies needed to address evolving threats. The artifact paired with this self-reflection is a midterm comprised of multiple short-answer questions about core CI topics.

Understanding Counterintelligence in the Context of the IC

One of the most valuable aspects of the course was understanding the role of counterintelligence within the broader IC framework. CI serves as both a defensive mechanism, preventing foreign actors from gaining unauthorized access to U.S. secrets, and a proactive tool, identifying and disrupting adversarial intelligence operations. The professor suggested that CI becomes clearer when mentally referring to it as “countering foreign intelligence,” and that is a mnemonic I still use today to remind me to focus on foreign intelligence service threats rather than broad intelligence threats.

The course also emphasized the importance of coordination between CI organizations and law enforcement agencies. Learning about the interactions between entities such as the FBI, CIA, the Air Force Office of Special Investigations, the Naval Criminal Investigation Service, and the

Army Criminal Investigation Division provided me with a clearer understanding of how these organizations share responsibilities in countering foreign threats. This understanding has been instrumental in showing me the challenges involved in ensuring smooth interagency cooperation, particularly when intelligence and law enforcement priorities may conflict. It has also helped in my role as a leader within the special operations community by providing me a clearer insight on CI threats to evaluate missions and opportunities for partnership.

Analyzing Foreign Intelligence Threats

The course provided in-depth coverage of various foreign intelligence threats, from traditional espionage to newer forms of economic espionage and cyber intrusions. What stood out to me most was the strategic nature of modern intelligence operations, where adversaries not only seek classified information but also aim to influence public opinion, disrupt political processes, and steal economic and technological secrets or merely build rapport with targets. Through case studies and class discussions, I was able to explore real-world scenarios involving insider threats and foreign influence campaigns. These examples illustrated the complexity of the threat landscape and how adversaries use a combination of traditional and unconventional methods to advance their agendas.

A key takeaway from these discussions was the growing threat of economic espionage, especially in a globalized economy where intellectual property and trade secrets are highly valuable. I now better understand how foreign governments and corporations engage in covert activities to gain competitive advantages, often targeting emerging technologies and critical industries.

Unfortunately, I took this class during the height of COVID in the summer of 2020 when classes were pushed online. I think this course would have been greatly enhanced by the ability

to have classified discussions about CI threats and capabilities. An increasing threat to intelligence operations is Ubiquitous Technical Surveillance, and I wonder if the course could have gone into more detail in this area if it had not been conducted via distance instruction.

Laws, Strategies, and the Importance of Adaptability

The course also introduced the legal frameworks and strategies governing counterintelligence activities. I found it valuable to learn about the various laws that shape the U.S. counterintelligence effort, such as the Foreign Intelligence Surveillance Act (FISA), and how they strike a balance between national security and civil liberties. Understanding these frameworks reinforced the importance of conducting CI operations in an ethical and lawful manner.

Another important aspect was the emphasis on adaptability. In an environment where threats are constantly evolving—especially in the cyber domain—CI strategies must remain flexible and forward-looking. This concept was reinforced through group discussions, where we debated how the U.S. could strengthen its CI posture against emerging challenges, including those posed by non-state actors and hybrid threats.

Conclusion

This course has greatly enhanced my understanding of the strategic importance of counterintelligence in safeguarding U.S. national security and economic interests. It has also provided me with practical insights into the complexities of managing CI efforts within the IC and the challenges posed by modern foreign intelligence operations. I now have a greater appreciation for the role of CI professionals in detecting and mitigating diverse threats, from traditional espionage to cyber intrusions.