SENTINEL RESEARCH SOCIETY
Washington, DC

Policy Memorandum

Subject: The Growing Counterintelligence Deficit in U.S. National Security Strategy

To: Members of the House Permanent Select Committee on Intelligence (HPSCI), the Senate Select Committee on Intelligence (SSCI), and the House and Senate Committees on Armed Services

Date: 10 March 2025

Executive Summary

The United States faces an escalating national security crisis due to the diminishing resourcing of counterintelligence (CI) operations, despite an ever-growing requirement to defend against foreign intelligence threats. As adversaries such as China, Russia, North Korea, and Iran intensify espionage, malign influence, and cyber intrusions, the U.S. remains dangerously underprepared to counter these activities. A particularly alarming gap exists in the lack of dedicated counterintelligence resourcing within cleared defense contracting for major defense acquisitions. This results in the rapid exfiltration of cutting-edge U.S. defense technology by foreign intelligence services, nullifying strategic advantages and escalating costs to maintain military superiority.

Problem Statement

Current U.S. counterintelligence efforts are underfunded, outmatched, and misaligned with the threat landscape. Despite increasing instances of foreign espionage and the looming potential for armed conflict with China, counterintelligence budgets have stagnated or declined, even as the defense industrial base remains a primary target of hostile intelligence services.

When the Department of Defense (DoD) contracts with cleared defense contractors for major acquisitions, there is no statutory requirement to allocate additional counterintelligence resources to safeguard these investments. As a result, adversaries frequently acquire U.S. technology at nearly the same time as American forces, undermining operational security, eroding military advantage, and necessitating further costly research and development to counter the compromised systems. This cycle of vulnerability and reactive spending weakens U.S. strategic deterrence and imposes an undue financial burden on the defense budget. Adversarial technological surprise would set the conditions for a potential situation of strategic surprise that the United States might not be able to recover from in the near to mid-term.

Key Issues

1. **Exfiltration of Defense Technology** – Foreign intelligence services, particularly those of China and Russia, systematically target cleared defense contractors to acquire classified and sensitive defense technologies, often before these systems reach full operational capability.
2. **Lack of Counterintelligence Investment** – The U.S. has not made significant new investments in defense counterintelligence in over a decade, leading to insufficient personnel, technology, and investigative resources to address modern espionage threats.

3. **No Integrated CI Resourcing in Major Defense Acquisitions** – While billions are allocated for advanced defense systems, there is no proportional requirement to fund counterintelligence efforts to protect these investments from adversary intelligence exploitation.
4. **Budgetary Inefficiency** – The lack of CI investment results in adversaries compromising U.S. defense capabilities, forcing repeated reinvestments in new military technologies, driving up defense spending without achieving a sustained advantage.

Policy Recommendations

1. **Mandate Counterintelligence Resourcing in Defense Acquisitions** – Congress should legislate a requirement that any major defense acquisition program (MDAP) includes proportional counterintelligence funding to ensure effective security measures against foreign espionage.
2. **Expand Defense Counterintelligence Workforce and Capabilities** – Increase funding to the Defense Counterintelligence and Security Agency (DCSA), military service CI components, and other relevant agencies to enhance personnel, training, and technological capabilities.
3. **Enhance Public-Private Counterintelligence Collaboration** – Mandate formalized counterintelligence partnerships between DoD, the Intelligence Community (IC), and defense contractors, requiring active threat sharing and defensive operations against foreign intelligence threats.
4. **Develop a National Counterintelligence Strategy for Cleared Defense Contractors** – Implement a comprehensive strategy to secure the defense industrial base, with specific focus on supply chain security, insider threat programs, and enhanced cybersecurity measures.
5. **Increase Congressional Oversight on CI Effectiveness** – Establish a bipartisan committee to assess and report on the effectiveness of counterintelligence programs within the DoD and the defense industrial base, ensuring accountability and sustained investment in CI efforts.

Conclusion

The U.S. cannot afford to continue a cycle of unchecked adversary espionage that erodes national security, increases defense costs, and nullifies strategic advantages. Without decisive action, the U.S. risks losing its technological and military superiority at a time when global threats are rapidly escalating. Counterintelligence must be recognized as an essential element of national defense—one that requires immediate and sustained investment. Congress must act now to secure America's military advantage and ensure that our national security resources are effectively protected from foreign intelligence threats.