Redefining Espionage: The Unseen War for Technological Dominance

By
Joshua Thibert

Published: March 24, 2026

The international system is undergoing a profound global power shift characterized by the resurgence of great power competition and a broad diffusion of technical capabilities. This environment is intensifying security competition across all domains. Concurrently, the proliferation of artificial intelligence (AI) and other disruptive technologies has fundamentally transformed espionage and defense. The traditional landscape of counterintelligence (CI) is obsolete and requires rapid, systemic overhaul to address the increasingly amplified, technologically enabled threats posed by state and non-state actors.

Specifically, the shift to great power technological competition has expanded CI's mandate from protecting military secrets to securing critical infrastructure, intellectual property (IP), and the integrity of the information domain. The dual-use nature of AI functions as both in support of automated espionage and a critical mechanism for preemptively anticipating and mitigating threats. The failure of the United States to strategically integrate AI into CI methodologies will result in the systemic erosion of national technological and economic advantage.

The Expanded Mandate of Modern Counterintelligence

CI functions to protect a nation’s secrets, personnel, and systems from foreign intelligence entities (FIEs). Yet today, CI must also confront a threat matrix dramatically enlarged in scope, sophistication, and velocity. The current geopolitical climate has necessitated a significant expansion of the traditional CI mission. In the context of great power competition, the most significant threat has shifted from the theft of classified military and diplomatic secrets to the large-scale acquisition of IP, trade secrets, and technological data, as highlighted in the recently released Annual Threat Assessment.

FIEs are aggressively targeting the private sector, academia, and research institutions, the very engines of national innovation through sophisticated economic espionage. Their strategic goal is not merely to obtain information, but to erode a nation's competitive advantage and accelerate the adversary's technological timetable, thereby shifting the global balance of power. CI must establish robust protective mechanisms that extend deep into the non-governmental technology and research ecosystem.

The dissolution of a clear distinction between peacetime competition and active conflict has resulted in a continuous state of confrontation known as the 'gray zone'. This strategic domain is characterized by persistent, non-lethal, yet tactically damaging activities designed to achieve political objectives without triggering traditional military responses. CI must now defend against a spectrum of subtle subversion, including large-scale cyber operations, persistent penetration of networks for reconnaissance and preparatory measures, and covert attempts to manipulate political discourse and decision-making.

The globalization of commerce and technology has created intricate, interconnected supply chains. These networks present significant CI risks, as adversaries seek to compromise the integrity, trustworthiness, and authenticity of products and services. By inserting "backdoors" or creating exploitable "choke points" at various nodes, adversaries establish capabilities for future exploitation. CI efforts are essential to conduct comprehensive due diligence and risk mitigation, securing these complex networks against both hardware and software compromise.

Artificial Intelligence: The Dual-Use Catalyst

AI and emerging technologies are not merely *targets* of modern espionage; they are simultaneously the most potent tools and the most necessary defenses in the counterintelligence battleground. This dual-use dynamic creates a challenging "AI vs. AI" scenario that demands immediate, radical adaptation. Adversaries are leveraging AI to dramatically enhance the speed, scale, and sophistication of their intelligence operations:

Automated Espionage and Big Data Analysis: AI-powered tools can automate and scale the processing, translation, and analysis of vast, heterogeneous datasets (Big Data), vastly increasing the volume and velocity of intelligence collection from both open-source intelligence and classified sources.

Adaptive Cyberattacks: Machine learning (ML) algorithms enable the development of more elusive and adaptive cyber threats. This includes automated exploitation of vulnerabilities, dynamic creation of polymorphic malware, and rapid penetration of defenses, operating at speeds that effectively outpace traditional, human-centric cybersecurity responses.

Generative AI for Influence: Generative AI can create highly realistic deepfakes (synthetic videos and audio) and synthetic narratives at scale. This facilitates sophisticated disinformation and propaganda campaigns to manipulate public opinion and conduct advanced social engineering, severely compromising the ability of institutions to discern truth from falsehood.

Three interconnected factors fundamentally redefine the scope of CI responsibility: target expansion, the blurring of conflict lines, and supply chain vulnerabilities. To effectively counter these technologically enabled threats, CI must aggressively embrace and integrate these same technologies, transforming them into proactive defensive tools:

Threat Anticipation and Predictive Analysis: AI can process and analyze massive amounts of threat data, identifying subtle, non-obvious patterns, trends, and anomalies. This capability allows CI to transition from merely reacting to threats toward predictive modeling, allowing one to forecast adversary actions before they materialize and enabling preemptive defense.

Enhanced Surveillance and Anomaly Detection: ML algorithms are crucial for the detection of subtle anomalies in network traffic, user behavior, and physical security systems that a human operator would miss. AI-driven monitoring provides real-time, large-scale pattern-of-life analysis that significantly exceeds human cognitive capacity.

Counter-Disinformation and Integrity Checks: CI requires AI-driven tools to effectively identify, analyze, and flag AI-generated propaganda, deepfakes, and synthetic media. Systems designed for content provenance and authenticity verification are essential to safeguard the integrity of the information domain and maintain public trust.

Insider Threat Mitigation: Defensively, AI can monitor internal networks to flag anomalous user behaviors such as unusual data access attempts, large data transfers, or deviations in an employee's digital pattern-of-life. As such they assist in identifying potential insider threats before significant compromise occurs.

The Strategic Imperative

The shift of global powers and the proliferation of disruptive technologies have thrust counterintelligence into an even more important aspect of national security. The stakes of this technological arms race transcend traditional security concerns, encompassing the integrity of a nation's innovative ecosystem, its economic competitiveness, and the resilience of its democratic institutions.

CI must rapidly evolve its strategies to prioritize the defense of economic and technological assets, and it must integrate AI as a foundational defensive technology to achieve predictive, scalable threat mitigation. Failure to aggressively master and deploy AI defenses against technologically augmented adversaries risks the systemic erosion of national advantage in a world where technological leadership is increasingly synonymous with global power. The future success of great power competition hinges directly on the adaptive capacity and technological sophistication of CI's function.

Joshua Thibert is a Senior Analyst at the National Institute for Deterrence Studies (NIDS) with over 30 years of comprehensive expertise. His background encompasses roles as a former counterintelligence special agent within the Department of Defense and as a practitioner in compliance, security, and insider risk management in the private sector. His extensive academic and practitioner experience spans strategic intelligence, multiple domains within defense and strategic studies, and critical infrastructure protection. The views of the author are his own.