The Role of Counterintelligence in Protecting Economic and Corporate Interests

By: Joshua Thibert
National Institute for Deterrence Studies

The traditional purview of counterintelligence has long been associated with protecting state secrets and military capabilities from foreign adversaries. While this function remains paramount, a profound shift in global power dynamics and technological proliferation has expanded the scope of counterintelligence to include the protection of a nation's economic and corporate interests. The rise of economic espionage as a primary instrument of statecraft has made corporate intellectual property and trade secrets as valuable, if not more so, than classified government documents. The challenge for modern counterintelligence is to adapt its strategies and forge new partnerships to combat these sophisticated threats, which endanger not only individual companies but also national economic security and competitiveness.

The methods of modern economic espionage are a complex mix of traditional human intelligence operations and cutting-edge cyber techniques. Foreign intelligence services, often with government support, actively seek to illicitly acquire sensitive information from key industries, including advanced computing, pharmaceutical, aerospace, and energy.
Traditional methods include recruiting corporate insiders who, through financial incentives, ideological persuasion, or blackmail, gain access to a company's most sensitive data. These operations may also involve physical infiltration of a company's facilities, such as placing an agent in a surreptitious role within the supply chain to obtain proprietary information. On the cyber front, the threat is even more pervasive. Adversaries employ sophisticated spear-phishing attacks to access corporate networks, deploy advanced malware to exfiltrate data covertly, and conduct supply-chain attacks that compromise software or hardware during manufacturing. This combination of physical and digital tradecraft allows foreign intelligence services to bypass traditional security measures and access vital research and development data, manufacturing processes, and business strategies at a fraction of the time and cost it would usually take to develop them organically.

In this context, the role of counterintelligence in managing and executing insider threat mitigation programs is a critical element of national security in the burgeoning era of global great-power competition. These programs move beyond simple security protocols to adopt a holistic, risk-based approach to deterring, detecting, and mitigating threats posed by a company's employees. Rather than focusing solely on a small number of spies, modern programs are designed to identify individuals on a "critical pathway" to becoming a threat by using both technical indicators (e.g., unusual data downloads, anomalous network activity) and non-technical, behavioral cues (e.g., unexplained affluence, foreign connections, or indicators of personal stress). The goal is to intervene early, assisting at-risk employees before a foreign

intelligence service can exploit their vulnerabilities. This proactive stance is essential because, in an environment where state-sponsored actors relentlessly target a nation's innovation base, the greatest risk often comes from within.
A robust insider threat program serves as the first line of defense against the human element of foreign espionage, thereby preserving a company's competitive edge and, by extension, a nation's technological superiority.

To counter this multifaceted threat effectively, a robust public–private partnership is no longer a luxury but a necessity. Government counterintelligence agencies possess unique authorities and global visibility that enable them to identify the motives, capabilities, and tactics of foreign intelligence services. Yet most sensitive intellectual property resides in the private sector, which lacks the legal mandate, resources, and authority to conduct proactive counterintelligence operations. This asymmetry creates a critical national vulnerability. An effective public–private partnership seeks to close this gap by enabling the secure, timely sharing of threat intelligence from government agencies to at-risk corporate firms. Collaborative successes have included joint task forces and intelligence-sharing portals that provide companies with actionable warnings about specific foreign threats.

Despite these actions, significant challenges remain. Legal and ethical constraints, particularly those related to privacy protections and the handling of classified information, often impede intelligence flows. Firms may also hesitate to report breaches due to concerns over reputational harm, investor confidence, and legal liability. Compounding these issues, the speed and scale of cyber-enabled espionage frequently outpace the bureaucratic processes governing efficient and practical cooperation. Addressing these gaps requires a unified national strategy that streamlines information-sharing mechanisms, clarifies legal authorities, and directly confronts insider threats and commercial espionage to mitigate their economic and national security consequences.

The protection of economic and corporate interests has become a core mission of modern counterintelligence. The convergence of traditional espionage and cyber operations has produced a complex threat environment that state security services cannot confront alone. As a result, the future of national security and economic prosperity hinges on resilient public–private collaboration, particularly through the implementation of robust insider-threat mitigation programs. By fostering trust, establishing clear and reliable communication channels, and adopting a unified national strategy, governments and industry together can build the defenses necessary to protect innovation, preserve strategic advantage, and sustain long-term economic competitiveness in an increasingly contested global environment.

Joshua Thibert is a Contributing 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. Views expressed in this article are the author's own.