TECHNOLOGY AND PROGRAM PROTECTION

Shielding the Army's Technological Advantage

By Bernard Rhoades and Thomas Quigley

The early adoption of dual-use, disruptive technologies is increasingly pacing today's competition for global supremacy. The stakes have never been higher for program managers (PMs) and product support managers to anticipate how adversaries might subvert, compromise, or steal from our national technology and industrial base to diminish military advantage. The recent update of Army Regulation (AR) 70-77, Technology and Program Protection, and the maturation of the Army Protection Collection Management Board (PCMB) provide a framework for a more proactive, concerted, and adaptive technology and program protection effort. This framework aims to develop and maintain effective protection plans at all phases of the system development lifecycle to address the evolving threat landscape.

Program protection is a flexible, multi-disciplinary process used to maintain technological advantage for the warfighter from concept development to system disposal. It drives the implementation of system security engineering and supply chain security countermeasures focused on sensitive technical information, mission-critical components (e.g., software and microelectronics), and advanced technical know-how against cyber threats, espionage, sabotage, unauthorized technology transfer, and battlefield loss. Coupled with the integration of intelligence support, program protection informs risk management decisions.

AR 70-77 serves as the Army's capstone acquisition policy for technology and program protection. The updated regulation aligns program protection with War Department (DOW) acquisition reform, supply-chain risk management (SCRM) initiatives, and other new security policies issued since the original 2014 publication. These improvements involve initiating risk management as early as basic research, reinforcing protection through logistics and contracting, reprioritizing intelligence and security resources, establishing protection training standards, and continuously measuring and improving effectiveness.

The Army's Science and Technology Reinvention Laboratory (STRL) must now develop, maintain, and transfer approved science and technology protection plans (S&TPPs) before transitioning research to an Army PM. The S&TPP process starts when fundamental research yields technical information that warrants control or classification due to its maturity and application to military use. STRLs leverage the Army Research and Technology Protection Center to conduct assessments using standardized methods. The main goal of the S&TPP is to provide PMs with assurance that the prototype technology has already implemented adequate protection measures. This ensures the PM does not waste

resources protecting technology that is already compromised while jump-starting the protection process.

The updated AR 70-77 also mandates program executive offices to appoint trained program protection leads to manage program protection plans (PPPs) for their respective portfolios. This creates a network of Defense Acquisition University-credentialed experts, ensuring consistent implementation of program protection policies and best practices at the Acquisition Category II, III, and IV levels.

Previously, PPP updates and reviews only occurred during milestone decision events and annually for significant changes. Additionally, supply-chain risk assessments in the PPPs represented a snapshot in time without considering the lower tiers of suppliers from countries of special concern. Now, PPPs are reviewed every five years by the Deputy Assistant Secretary of the Army for Sustainment (DASA(S)), and PMs use SCRM illumination tools and software bills of material to ensure their relevance. As a result, the PPP provides system security engineers, logisticians, and supporting intelligence professionals with the ability to continuously adjust efforts based on evolving threats, modernization, and amorphous supply chains.

In recent years, the DOW has emphasized the need for enhanced intelligence in support of materiel and capability development activities. In response, the Department of the Army, led by the Assistant Deputy Chief of Staff for Intelligence (G-2) in partnership with the DASA(S), established the PCMB. This board meets quarterly to address intelligence and security issues related to Army modernization priorities and the DOW's critical programs and technologies (CP&T) list. The PCMB framework and partnerships facilitate a structured, collaborative approach to align strategy, plans, and actions; synchronize the delivery of current and estimative intelligence to Army senior leaders; and oversee and assess collection and protection activities based on acquisition community requirements.

The PCMB has already yielded valuable outcomes, including a process to measure the effectiveness of intelligence products in achieving desired acquisition or protection effects. The Counterintelligence Support Plan (CISP) and the Multi-Discipline Counterintelligence Threat Assessment (MDCITA) are essential for informing the development of PPPs that involve critical program information or technology elements on the DOW CP&T list. CISP development and implementation have improved significantly since the assignment of an Army Counterintelligence Command liaison embedded within the Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology. This ensures that PMs receive the CISP before initial PPP staffing for approval. The MDCITA is undergoing continuous transformation to streamline production and delivery processes.

In conclusion, the Army's multifaceted approach to technology and program protection, as outlined in AR 70-77 and facilitated by the PCMB, represents a significant step forward in safeguarding the Army's technological advantages. By integrating risk management early, emphasizing continuous improvement, and fostering collaboration between intelligence, acquisition, and sustainment communities, the Army is better positioned to maintain its competitive edge in an increasingly complex and contested global environment. This proactive and adaptive strategy is crucial for ensuring that warfighters have access to the most advanced and secure capabilities.

Mr. Bernard Rhoades is the program protection director for the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology. He previously served as the program protection policy lead and provided network and system security engineering contractor support for various War Department programs. He served four years as an Army signal officer. He is Life Cycle Logistics (Advanced) certified with a Master of Science degree in information technology security from Capella University.

Mr. Thomas Quigley serves as a Research, Development, and Acquisition program protection specialist for the Deputy Assistant Secretary of the Army for Sustainment in the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA[ALT]). He is a retired Army officer with numerous combat arms and staff positions throughout his career. He was an Army Acquisition Corps professional for a combined 16 years. His tenure at ASA(ALT) included serving two years on the Office of the Under Secretary of War Protecting Critical Technology Task Force, developing processes and procedures for enhanced protection. He has a Master of Business Administration from Troy University, a Master of Arts from the Naval War College, and is a graduate of the Eisenhower School of Strategic Studies.