Cybersecurity of Air Force Weapon Systems

Ensuring Cyber Mission Assurance Throughout a System's Life Cycle

Air Force weapon systems today are heavily reliant on complex software and high interconnectivity to perform their missions. Cyber capabilities enable many of the advanced features (e.g., electronic attack, sensor fusion, and communications) that give the Air Force its edge over potential adversaries. But they also create potential opportunities—and incentives—for adversaries to counter U.S. advantages through cyberattacks. For example, a sophisticated adversary may seek to discover and exploit vulnerabilities in an aircraft's software, supporting systems, or supply chain in order to gain intelligence or to sabotage operations. Nor are the potential risks limited to the newest and most advanced systems: Legacy aircraft, which make up the majority of Air Force inventory, are also exposed to attack from evolving cyber threats and must remain vigilant.

To manage cybersecurity for these systems, the Air Force and the U.S. Department of Defense (DoD) need appropriate policies to foster system designs that are robust and resilient to cyber attacks, organizational designs that are optimally shaped to implement these policies, and monitoring and feedback mechanisms that capture the true state of cybersecurity (as opposed to just compliance with policies) over a weapon system's entire life cycle.

The Air Force Life Cycle Management Center asked RAND Project AIR FORCE (PAF) to assess current laws, policies, organizations, and processes against best practices and sound principles of cybersecurity and to recommend steps for improvement. The research focused on national security systems for which the Air Force has some control over designs, architectures, protocols, and interfaces, as opposed to commercial, off-the-shelf (COTS) information technology and business systems.

Observations on Cybersecurity Management

Our premise is that the desired outcomes of cybersecurity management are to (1) limit how much critical information an adversary can obtain from a successful exfiltration and (2) maintain an acceptable level of operational functionality even when attacked. These outcomes must be achieved continuously throughout the life cycle of a military system, from research and development through disposal. All phases are important, but the development and sustainment stages

Key findings:

- Current policies are better suited to simple, stable, and predictable environments than to the complex, rapidly changing, and unpredictable reality of today's cybersecurity environment.

- Implementation of cybersecurity is not continuously vigilant throughout the life cycle of a military system.

- Control of and accountability for military system cybersecurity is spread over numerous organizations and is poorly integrated.

- Monitoring and feedback for cybersecurity is incomplete, uncoordinated, and insufficient for effective decision-making or accountability.

are particularly critical: the former because design decisions are made that can limit options in the future, and the latter because most systems reside in sustainment for the majority of their life cycle. Given these goals for cybersecurity, a review of the literature reveals two observations regarding organizational design and feedback for attaining these cybersecurity objectives:

- **Organizational design should be flexible and decentralized.** The cybersecurity environment is inherently dynamic and complex. The literature suggests that well-managed organizations cope with such environments by choosing organizational designs that favor solutions obtained through decentralized coordination and collaboration of workers over those prescribed by standardized and formalized controls.

- **Outcome-based feedback is more valuable than compliance-based feedback.** Organizations tend to focus on readily observable metrics, such as compliance with policies and directives, to indicate their level of cybersecurity. However, compliance does not, in itself, reflect the actual state of cybersecurity, especially in complex and rapidly changing threat environments. Organizations should instead focus on whether their policies

and practices are achieving the desired outcomes (e.g., mission assurance in the face of adaptive cyberattacks) and should be ready to adapt as needed.

Current Shortfalls and Their Implications

Comparing these management principles with a detailed review of the laws and policies governing Air Force cybersecurity reveals a number of gaps:

Current policies are better suited to simple, stable, and predictable environments than to the complex, rapidly changing, and unpredictable reality of today's cybersecurity environment. DoD has sought to standardize cybersecurity by applying the National Institute of Standards and Technology's (NIST's) security controls to all systems, including weapon systems. But these controls are designed to mitigate security issues in designs that the Air Force inherits, such as in COTS systems. Weapon systems, in contrast, present opportunities for designers to build systems that are more inherently secure. Sound system security engineering during the early design phase of a weapon system would be more effective than security controls that are applied as overlays to designs created without cybersecurity as an integral priority.

Implementation of cybersecurity is not continuously vigilant throughout the life cycle of a military system. Attention to cybersecurity is generally triggered by acquisition events, which mostly occur during procurement. As a result, policy does not cover the full range of cybersecurity issues that affect a system over its life cycle. This shortfall has several important consequences. First, programmatic triggers for cybersecurity come late in the design process and, therefore, have little leverage to influence critical design decisions that affect cybersecurity. Second, systems in programs beyond the procurement phase (i.e., in sustainment or disposal) receive less attention than those in procurement. As noted above, this underemphasizes the majority of Air Force systems, which are in sustainment. Third, this policy structure tends to favor vulnerability assessments (prevalent in the design phase) over mission impact and threat assessments (which affect the entire life cycle). Finally, management, oversight, and budgeting within DoD are strongly structured around programs, whereas cybersecurity vulnerabilities cross program boundaries. This creates a misalignment between cybersecurity challenges in specific systems and how they can be managed.

Control of and accountability for military system cybersecurity is spread over numerous organizations and is poorly integrated. This results in diminished accountability and unity of command and control for cybersecurity. These overlapping roles, and particularly the presence of a cybersecurity-focused authorizing official, create ambiguities in decision authority and accountability. For example, who can make the final decision regarding risk to a mission: the commander or the authorizing official? And should a cybersecurity incident occur, who is ultimately to be held accountable: the program manager, the authorizing official, or the operational commander?

Monitoring and feedback for cybersecurity is incomplete, uncoordinated, and insufficient for effective decisionmaking or accountability. Current feedback does not capture all systems, does not probe the consequences of cybersecurity shortfalls, and is not produced in a form that informs effective decisionmaking. The lack of comprehensive program- or system-oriented feedback on cybersecurity and the impact of cybersecurity on operational missions stands in contrast to the abundance of feedback on cost and schedule. This imbalance creates an incentive structure for program managers and program executive officers to favor cost and schedule over cybersecurity performance. These deficiencies in feedback on cybersecurity also further inhibit individual accountability.

Recommendations to Address Shortfalls

No simple solution will correct all of the above shortfalls, many of which are structurally embedded in DoD. Some result from well-intentioned statutory requirements and DoD policies that are not easily changed. However, within these bounds, there are steps the Air Force can take to strengthen cybersecurity for weapon systems:

1. Define cybersecurity goals for military systems within the Air Force around *desired outcomes* while remaining consistent with DoD issuances. As a working objective, *keep the impact of adversary cyber exploitation and offensive cyber operations to an acceptable level, as guided by a standardized process for assessing risk to mission assurance.*

2. Realign functional roles and responsibilities for cybersecurity risk assessment around a balance of system vulnerability, threat, and operational mission impact, and empower the authorizing official to integrate and adjudicate among stakeholders. For example, the life-cycle management community (specifically the program manager) would be responsible for program and system vulnerability assessments, the intelligence and counterintelligence communities would be responsible for threat assessments, and the mission owner (e.g., core function lead integrator, lead major command) would be responsible for operational mission assurance assessments. The authorizing official would integrate and balance these viewpoints based on an acceptable level of cybersecurity risk.

3. Assign each authorizing official a portfolio of systems and ensure that all systems explicitly fall under some authorizing official throughout their life cycles.

4. Encourage Air Force program offices to supplement the required DoD security controls (which focus on closing vulnerabilities) with more comprehensive cybersecurity measures, including sound system security engineering (which focuses on making the system robust and resilient in the face of successful attacks).

5. Foster innovation and adaptation in cybersecurity by decentralizing, in any new Air Force policy, how system security engineering is implemented within individual programs.

6. Explicitly assess the trade-offs between cybersecurity risks and functional benefits associated with interconnecting military systems in cyberspace. This would reverse the default culture of connecting systems whenever possible and would reduce the complexity of cybersecurity.

7. Create a group of experts in cybersecurity who can be matrixed as needed within the life-cycle community, making resources available to small programs and to programs in sustainment.

8. Establish an enterprise-directed prioritization for assessing and addressing cybersecurity issues in legacy systems.

9. Close feedback gaps and increase the visibility of cybersecurity by producing a regular, continuous assessment that summarizes the state of cybersecurity for every program in the Air Force. Hold program managers accountable for a response to issues.

10. Create cybersecurity red teams that are dedicated to acquisition/life-cycle management within the Air Force.

11. Hold individuals accountable for willful infractions of cybersecurity policies.

12. Develop mission threat data to support program managers and authorizing officials in assessing acceptable risks to missions caused by cybersecurity deficiencies in systems and programs.

We acknowledge that these recommendations, even if fully implemented, would not completely solve the challenges of cybersecurity. Further, some of these policies would necessarily require additional resources and a suitably skilled workforce to carry out the responsibilities—commitments that are difficult to make in a constrained fiscal environment. The fact is that there are no quick or easy fixes for achieving world-class cybersecurity. However, by adopting these recommendations, the Air Force would take a large step toward more effective cybersecurity of its military systems throughout their life cycles.

This brief describes work done in RAND Project AIR FORCE, documented in *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*, by Don Snyder, James D. Powers, Elizabeth Anne Bodine-Baron, Bernard Fox, Lauren Kendrick, and Michael H. Powell, RR-1007-AF, 2015 (available at www.rand.org/t/RR1007). To view this brief online, visit www.rand.org/t/RB9835. The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark. © RAND 2015

www.rand.org