Leszek. Cwojdziński
Dr hab. inż. pil.
Airbus Poland S.A.
samolot221@wp.pl

DOI: 10.35117/A_ENG_23_05_01

Cybersecurity of United States Air Force Weapons Systems – ensuring mission security

Abstract: This article presents assumptions about the threat to air force weapon systems which today are heavily dependent on complex software and a large number of interconnections to accomplish combat missions. Cyber capabilities enable many advanced functions (e.g., electronic attack, sensor interconnection and communications) that give combat aviation an advantage over potential adversaries. However, they also create potential opportunities and incentives for adversaries to counter the air force's superiority through cyberattacks. The author discusses how a sophisticated adversary may seek to discover and exploit vulnerabilities in aircraft software, support systems or the supply chain to gain intelligence or sabotage operations. The potential risk is not just limited to the newest and most advanced systems but also to systems that will be going out of service within the next decade or two. Older aircraft, which currently still make up the majority of US Air Force assets, are also vulnerable to attack from evolving cyber threats and must be protected. Cyber security audits show that current policies are better suited to simple, stable and predictable environments than to the complex, rapidly changing and unpredictable reality of today's cyber security environment. The model cybersecurity policy is intended to serve as a guide to help countries and their armed forces focus resources and activities to achieve a systemic approach to cyber security, including current and future combat systems being introduced. The author points out that the goal of developing new solutions is for states and stakeholders to be able to develop a systems-of-systems approach to protect against cyber threats and respond to and recover from cyber incidents in a timely manner, thereby increasing resilience to new threats without significant disruption to the use of combat systems.

Keywords: Cyber security; Security environment; System of systems; Security policy; Security culture; Air force; Combat aviation; Combat systems

Air Force weapon systems today are heavily reliant on complex software and numerous interconnections to carry out their missions. Cyber capabilities enable many advanced functions (e.g., electronic attack, sensor fusion, and intercommunication), which give the Air Force an advantage over potential adversaries. However, they also create opportunities and incentives for adversaries to counter the U.S. advantage through cyberattacks. One example is a sophisticated adversary seeking to identify and exploit vulnerabilities in aircraft software, supporting systems, or the supply chain to gather intelligence or sabotage operations. The potential risk is not limited to the newest and most advanced systems: older aircraft, which currently still constitute the majority of the U.S. Air Force inventory, are also exposed to evolving cyber threats and must remain vigilant.

To manage the cybersecurity of these systems, the U.S. Air Force and the U.S. Department of Defense (DoD) need appropriate policies that support system designs robust and resilient to cyberattacks, organizational structures optimally tailored to implement these policies, and monitoring and feedback mechanisms that capture the true state of cybersecurity (as opposed to mere compliance with existing policies) throughout the weapon system’s entire life cycle. The U.S. Department of Defense recommends the development of a model

cybersecurity policy that NATO member states and defense industry representatives could refer to when creating their own national or internal policies.

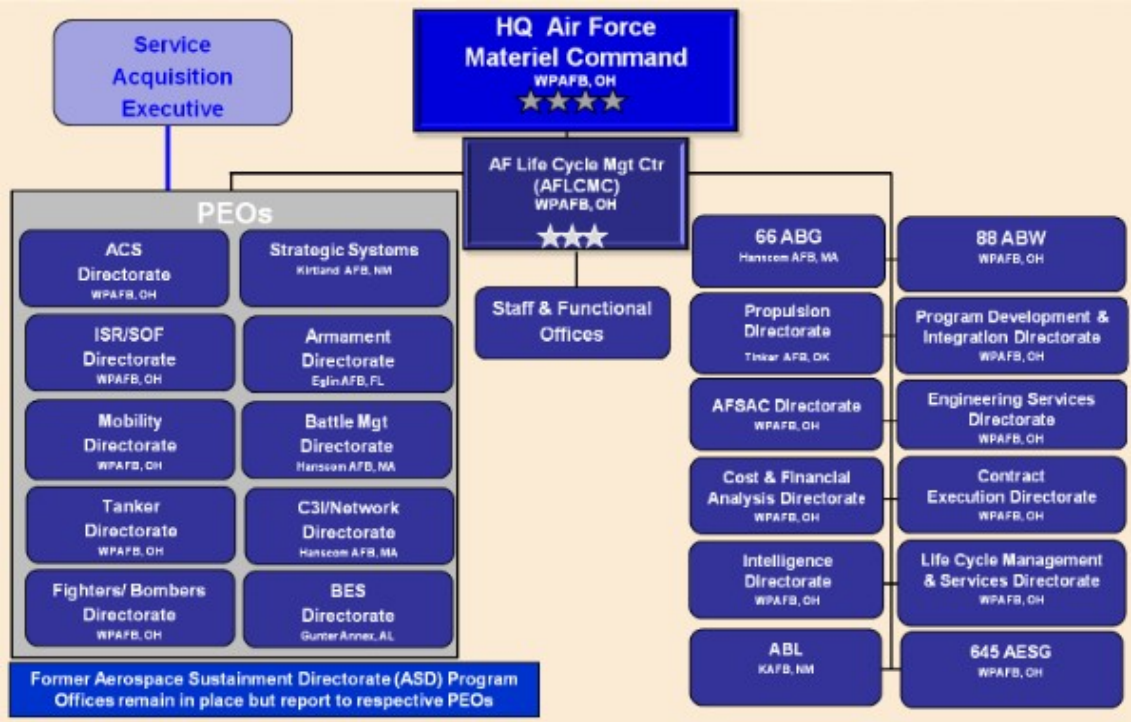
One of the key organizations established to support U.S. Air Force weapon systems throughout their full life cycle is the Air Force Life Cycle Management Center (AFLCMC), headquartered at Wright-Patterson AFB. It is one of six centers under Air Force Materiel Command responsible for managing the life cycle of U.S. Air Force weapon systems from inception to retirement. The mission of AFLCMC is to foster those weapon features that, through technical and technological superiority, will tip the balance of victory in armed conflicts in favor of the United States.

AFLCMC was designed to manage weapon systems throughout their entire life cycle, as well as to streamline and consolidate personnel functions and processes to reduce redundancy and increase efficiency. In addition, the operational structure of AFLCMC (Figure 1) provides a suitable framework for decision-making and process optimization across the entire weapon system life cycle. AFLCMC personnel work closely with their counterparts in other centers, overseeing: IT systems and networks; command, control, communications, intelligence, surveillance, and reconnaissance systems; armaments; strategic systems; aircraft platforms; and various specialized or support systems such as simulators and personal equipment. AFLCMC also executes the sale of aircraft and other defense-related equipment, while simultaneously building security assistance relationships with partner nations' air forces. These tasks are carried out by approximately twenty-six thousand AFLCMC Air Force specialists, civilian employees, and contractors at nine main locations and several dozen smaller sites.

The AFLCMC commander is responsible for organizing, training, and equipping the center, including life-cycle management processes. Each Program Office reports to one of ten Program Executive Officers (PEOs), who are accountable for actions within their respective areas of responsibility and report to the Air Force Service Acquisition Executive at the Pentagon (the Assistant Secretary of the Air Force for Acquisition). The Air Force Security Assistance and Cooperation Directorate oversees the execution of foreign military sales. The Propulsion Directorate oversees engine procurement and product support. AFLCMC support directorates provide direct program support, such as engineering, technical order management, development planning, contracting, and source selection assistance. The support directorates include: Program Execution; Technical Engineering Services; Financial Management Mission; Logistics Services; Contract Execution; Cyber & Analysis Programs; Program Development & Integration; and Intelligence.

The U.S. Air Force Life Cycle Management Center (AFLCMC) asked RAND Project AIR FORCE (PAF) to evaluate current regulations, policies, organizations, and processes with regard to best practices and sound cybersecurity principles, and to recommend steps for improvement. The research focused on national security systems over which the Air Force can exercise some control in terms of designs, architectures, protocols, and interfaces, as opposed to commercial, off-the-shelf (COTS) IT and business systems.

PAF's mission is to conduct an integrated program of objective analyses on issues of enduring interest to the Department of the Air Force. PAF addresses far-reaching and interrelated questions, such as: What role will air and space forces play in the future security environment? How should forces be modernized to meet changing operational needs? What should be the size and characteristics of the Department's personnel, and how can they best be recruited, trained, and retained? How should infrastructure maintenance and acquisitions be improved to control costs?



1. Organizational Structure of AFLCMC
Source: https://www.hanscom.af.mil/Portals/57/documents/AFD-120716-005.pdf?ver=2016-07-11-082154-383

PAF was originally known as the RAND Project—the name RAND being derived from Research ANd Development—and was established in 1946 by General H. H. "Hap" Arnold as a means of preserving the significant benefits of civilian scientific thought demonstrated during World War II. Since its inception, PAF has remained the only Federally Funded Research and Development Center (FFRDC) funded by the Department of the Air Force that is devoted exclusively to research and analysis, rather than to systems engineering or scientific laboratory work. This special FFRDC status facilitates stable, long-term support to the Department of the Air Force and ensures that research personnel have access to relevant Department information and leadership. The Department's need for PAF's analytical support led to the establishment of four research programs that represent its core capabilities:

- **STRATEGY AND DOCTRINE** seeks to increase knowledge and understanding of geopolitical and other challenges in national security environments that affect Department of the Air Force operations. PAF provides expertise in grand strategy; evolving security challenges; power projection; expeditionary operations; and the changing roles of air, space, and cyber forces in current and future operations.
- **MODERNIZATION AND DEVELOPMENT OF FORCES** identifies and evaluates ways in which technological advances and new operational concepts can enhance the Department of the Air Force's ability to meet a range of future operational requirements. This research includes assessing the feasibility, performance, cost, and risk of technologies. PAF evaluates key components of future air, space, and cyber forces, as well as the systems and infrastructure that support them. Areas of specialization include intelligence, surveillance, reconnaissance, mobility, long-range strike, combat air forces, command and control, space, cyber, and nuclear.
- **RESOURCE MANAGEMENT** examines policies and practices within three main areas: (1) resilience of Department of the Air Force (DAF) installations, assets, and information; (2) effective and efficient resource allocation; and (3) the health of the

defense industrial and technological base. The goal of this program's research is to maximize operational effectiveness and efficiency in a resource-constrained environment.

- **WORKFORCE, DEVELOPMENT, AND HEALTH** (formerly Manpower, Personnel, and Training) examines the size and composition of the personnel of the Air Force Department and is concerned with the best ways to define, sustain, renew, deliver, and coordinate critical work capabilities. PAF also considers personnel development, such as training, employment opportunities, and career advancement, as well as analyzes the physical and mental health of employees. PAF's research encompasses the entire workforce: active duty, guard, reserve, civilian, and executive personnel. PAF also conducts extensive research on topics that pertain to all four programs and regularly responds to requests from the Air Force for assistance in solving urgent problems.

Insights on Cybersecurity Management

PAF experts have posited that the desired outcomes of cybersecurity management are (1) limiting the amount of critical information that an adversary can obtain through successful exfiltration and (2) maintaining an acceptable level of operational functionality even in the event of an attack. These outcomes must be continuously achieved throughout the entire lifecycle of a military system, from research and development to disposal. All stages are important, but the development and maintenance stages are particularly critical: the former arises from making design decisions that may limit capabilities in the future, and the latter because most systems remain in maintenance for the majority of their lifecycle. Considering these cybersecurity objectives, the literature review reveals two observations regarding organizational design and feedback to achieve these cybersecurity goals.

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 employee collaboration over solutions recommended by standard and formalized controls. Outcome-based feedback is more valuable than compliance-based feedback. Organizations tend to focus on easily observable indicators, such as compliance with policies and directives, to indicate their level of cybersecurity. However, compliance alone does not reflect the actual state of cybersecurity, especially in complex and rapidly changing threat environments. Instead, organizations should focus on whether their policies and practices are achieving the desired outcomes (e.g., ensuring mission success in the face of adaptive cyberattacks) and should be prepared to adapt as necessary.

Current Gaps and Their Implications

Comparing these management principles with a detailed review of regulations and policies governing cybersecurity in the US Air Force 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 the cybersecurity environment. The US Department of Defense strives to standardize cybersecurity by applying the National Institute of Standards and Technology (NIST) security controls to all systems, including weapon systems. These controls aim to mitigate security issues in systems inherited by the Air Force, such as COTS (Commercial Off-The-Shelf) systems. In contrast, weapon systems give designers the ability to build systems that are inherently more secure. Robust security engineering of the system at the early design stage of a weapon system would be more effective than security controls applied as overlays to designs created without cybersecurity as an integral priority.

Cybersecurity relies on intelligence data, threats, and risk management, which are an integral part of the entire system lifecycle. All data and systems must have an assigned owner at all times. Functions, systems, and critical infrastructure are identified within risk management processes. A "security by design" approach combined with "Defence in depth" principles is used to protect critical systems. Redundancy of critical systems is treated as a factor that increases system security. Data and information are protected during storage and transmission, according to their sensitivities. Managing the entire software/hardware supply chain is part of aviation cybersecurity management. Software and hardware used in critical aviation functions must meet cybersecurity requirements throughout the lifecycle of combat aviation systems.

Physical Protection (including personnel protection) is part of aviation cybersecurity management. The task of physical protection is to secure people, infrastructure, facilities, equipment, materials, and documents from unlawful interference and to protect critical aviation systems from unauthorized physical access. Physical protection contributes to risk management by identifying entities that pose a threat and/or the likelihood of attacks on military aviation critical infrastructure.

Information, Communication, and Technology (ICT) Protection is part of aviation cybersecurity management, defines and implements logical security measures, and contributes to managing cyber incidents, data recovery, and business continuity in cyber incident management processes, data recovery, and business continuity. Teleinformatics security contributes to risk management by identifying vulnerabilities, areas, and directions of attack, and by monitoring changes in the cybersecurity threat landscape. Incident management and critical function continuity are key factors in incident management processes. An integral process is the testing of crisis management and data recovery plans, which is an integral part of incident management.

Implementing Cybersecurity is Not Continuously Active Throughout the Military System Lifecycle

Attention to cybersecurity is typically triggered by events related to weapon acquisition, which most often occur during procurement processes. As a result, policy does not cover the full range of cybersecurity issues that impact the system throughout its entire lifecycle. This lack has several significant consequences.

Firstly, programmatic triggers for cybersecurity emerge at a late stage of the design process and therefore have little influence on key design decisions that affect cybersecurity. Secondly, systems in programs outside the procurement phase (i.e., in the maintenance or disposal phase) receive less attention than systems in the procurement phase. As mentioned above, this leads to the underestimation of most US Air Force systems that are in the maintenance phase. Thirdly, this policy structure tends to favor vulnerability assessments (predominant in the design phase) over mission impact and threat assessments (which affect the entire lifecycle). Finally, management, oversight, and budgeting within the United States Department of Defense are highly structured around programs, while cybersecurity vulnerabilities transcend program boundaries. This creates a discrepancy between cybersecurity challenges in individual systems and the way they are managed.

Monitoring and Feedback on Cybersecurity are Incomplete, Uncoordinated, and Insufficient for Effective Decision-Making or Accountability**.** Current feedback does not encompass all systems, does not examine the consequences of cybersecurity shortcomings, and is not conveyed in a manner that enables effective decision-making. The lack of comprehensive, program- or system-oriented cybersecurity feedback and the impact of cybersecurity on operational missions contrasts with the abundance of feedback on costs and schedules. This imbalance creates a motivational structure for program managers and program

executive officers who prioritize costs and schedules over cybersecurity outcomes. These gaps in cybersecurity feedback further limit individual accountability.

Recommendations to Address the Shortcomings

No simple solution will correct all of the above deficiencies, many of which are structurally rooted in the US Department of Defense. Some result from well-intentioned statutory requirements and Department of Defense policies that are not easily changed. However, within these constraints, the Air Force can take steps to strengthen the cybersecurity of weapon systems:

- Define Cybersecurity Goals for Military Systems in the Air Force Around Desired Outcomes While Remaining Compliant with Department of Defense Guidelines. The working goal is to maintain the impact of an adversary's cyber exploitation and offensive cyber operations at an acceptable level, in accordance with the standard risk assessment process to ensure mission success.
- Redefine Functional Roles and Responsibilities in Cybersecurity Risk Assessment Based on a Balance Between System Vulnerability, Threat, and Mission Impact, and Grant the Approving Official Authority to Integrate and Resolve Stakeholder Interests. For example, the lifecycle management community (particularly 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., the chief integrator of core functions, main command) would be responsible for mission assurance assessments. The approving official integrates and balances these viewpoints based on an acceptable level of cybersecurity risk.
- Assign Each Approving Official a Portfolio of Systems and Ensure That All Systems Are Clearly Under the Oversight of an Approving Official Throughout Their Lifecycle.
- Encourage US Air Force Program Offices to Complement Required DoD Security Controls (which Focus on Mitigating Weaknesses) with More Comprehensive Cybersecurity Measures, Including Robust System Security Engineering (which Focuses on Ensuring System Robustness and Resilience in the Face of Successful Attacks).
- Support Innovation and Adaptation in Cybersecurity Through Decentralization, Within Each New Air Force Policy, of How System Security Engineering is Implemented Within Individual Programs.
- Assess the Trade-offs Between Cybersecurity Risk and Functional Benefits Associated with Connecting Military Systems in Cyberspace. The goal is to reverse the default culture of connecting systems whenever possible, which would reduce cybersecurity complexity.
- Create a Group of Cybersecurity Experts Who Can Be Mobilized as Needed Within the Lifecycle Community, Providing Resources to Small Programs and Programs in the Maintenance Phase.
- Establish Priorities for Enterprises in Assessing and Addressing Cybersecurity Issues in Older Systems.
- Eliminate Feedback Gaps and Increase Cybersecurity Visibility by Producing Regular, Ongoing Assessments Summarizing the Cybersecurity Posture for Each Program in the US Air Force. Hold program managers accountable for responding to issues.
- Create Cybersecurity Red Teams Dedicated to Acquisition/Lifecycle Management in the US Air Force.
- Hold Individuals Accountable for Deliberate Violations of Cybersecurity Policies.

- Develop Mission Threat Data to Support Program Managers and Approving Officials in Assessing Acceptable Risk for Missions Caused by Cybersecurity Shortcomings in Systems and Programs.

It should be recognized that these recommendations, even if fully implemented, will not entirely resolve cybersecurity issues. Moreover, some of these policies would require additional resources and appropriately skilled personnel to fulfill duties—commitments that are challenging to undertake in a constrained fiscal environment. The fact remains that there are no quick or easy solutions to achieve world-class cybersecurity. However, by adopting these recommendations, the Air Force would make significant strides toward more effectively securing the cybersecurity of its military systems throughout their entire lifecycle.

Cybersecurity Culture is a Crucial Element of Security Policy. A developed plan for implementing education, awareness, training, and exercises is an integral part of managing the cybersecurity of Air Force weapon systems. The cybersecurity culture is fully coordinated with existing security and protection cultures, supported by robust internal and, where possible, external information-sharing practices.

Key Conclusions

Cybersecurity audits indicate that current policies are better adapted to simple, stable, and predictable environments than to the complex, rapidly changing, and unpredictable reality of the cybersecurity landscape.

- Cybersecurity Implementation is Not Consistently Maintained Throughout the Military System Lifecycle.
- Control and Responsibility for Cybersecurity of Military Systems are Distributed Across Multiple Organizations and Poorly Integrated.
- Monitoring and Feedback on Cybersecurity are Incomplete, Uncoordinated, and Insufficient for Effective Decision-Making or Accountability of Structures and Functional Personnel.

A model cybersecurity policy is intended to serve as a guide to help nations and their armed forces focus resources and actions aimed at achieving a systemic approach to cybersecurity in the US Air Force, including both current and legacy systems. The ultimate goal is for nations and stakeholders to be able to develop a system-of-systems approach that enables protection against cyber threats, as well as the ability to respond to and mitigate cyber incidents in a timely manner, thereby ensuring resilience against new threats without significant disruptions.

Main Outcomes Expected from the Implementation of the Cybersecurity Policy.The primary outcomes anticipated from the implementation of the cybersecurity policy include establishing a framework for the further development and deployment of cybersecurity within the Air Force. This will be achieved through:

- Publishing and Disseminating the Cybersecurity Policy among relevant stakeholders and structures.
- Conducting Periodic Reviews of the policy to ensure its effectiveness and relevance.

These steps aim to create a robust foundation for enhancing cybersecurity measures, ensuring that they evolve in line with emerging threats and technological advancements.

Source materials

[1] https://hii.com/wp-content/uploads/2023/03/HII-Game-Changer-9.1.22.pd
[2] https://nap.nationalacademies.org/read/25393/chapter/1
[3] https://www.aflcmc.af.mil/WELCOME/Organizations/
[4] https://www.afsbirsttr.af.mil/About/Cybersecurity-and-the-Blue-Cyber-Education-Series/

[5] https://www.hanscom.af.mil/Portals/57/documents/AFD-120716-005.pdf?ver=2016-07-11-082154-383
[6] https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf
[7] official websites use .mil ., An official website of the United States government
[8] website belongs to an official U.S. Department of Defense organization in the United States.