RAND

Research Report

DON SNYDER, CHAD HEITZENRATER

Enhancing Cybersecurity and Cyber Resiliency of Weapon Systems

Expanded Roles Across a System's Life Cycle

For more information on this publication, visit **www.rand.org/t/RRA1506-2**.

Published by the RAND Corporation, Santa Monica, Calif.

Cover: your123/Adobe Stock.

About This Report

The objective of this project was to provide tools to improve the rigor, reproducibility, and scalability of analytical tools to support cybersecurity assessment, nuclear surety, and nuclear safety certification. This report lays the foundation for managing cybersecurity and cyber resiliency of weapon systems throughout their life cycles. It is meant to outline the overall activities from research and development through disposal to ensure a weapon system meets all needs to operate in a cyber contested environment. The primary audience for the report is the acquisition community and program management offices, but it should also be of some interest to those working under the chief information officer in the execution of Risk Management Framework assessments and approvals.

The research reported here was commissioned by the U.S. Air Force Program Executive Officer for Strategic Systems and conducted within the Force Modernization and Employment Program of Project AIR FORCE as part of fiscal year 2022 under a project, "Algorithms to Support a Nuclear Unified Certification Strategy."

Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Resource Management; and Workforce, Development, and Health. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website:

http://www.rand.org/paf/

This report documents work originally shared with the DAF on March 25, 2022. The draft report, dated March 2022, was reviewed by formal peer reviewers and DAF subject-matter experts.

Acknowledgments

We thank Major General Anthony Genatempo for sponsoring the work. Colonel Jason Bartolomei and David Wright provided day-to-day support critical to the execution of the research. (Ranks are those at the time of this research.) We also deeply appreciate the collegial interactions with the entire Ground Based Strategic Deterrent (now Sentinel) Unified

Certification Strategy team, too numerous to cite individually. We thank Danny Holtzman for many conversations about the cybersecurity and cyber resiliency of weapon systems.

At RAND, we thank Bart Bennett, John Drew, Lieutenant General (retired) Robert J. Elder, Jr., Lance Menthe, and Jim Powers for discussions, support, and review of earlier drafts. Formal reviews by Teddy Parker and Mathew Sargent improved the report.

That we received help and insights from those acknowledged above should not be taken to imply that they concur with the views expressed in this report. We alone are responsible for the content, including any errors or oversights.

Summary

Issue

Weapon systems must be secure in a cyber contested environment, or they will not be able to carry out the missions that they are designed to support. How can engineering managed by program offices enhance the cybersecurity and cyber resiliency of weapon systems?

Approach

We surveyed current policy, relevant academic literature, and commercial practice and used our personal assessments of cybersecurity and cyber resiliency efforts in the Department of the Air Force (DAF) to identify gaps in the use of engineering for cybersecurity and cyber resiliency throughout the life cycle of weapon systems and to propose mitigations.

Key Findings

During the design phase, systems security engineering has recently become the policy within the Department of Defense (DoD) for cybersecurity and cyber resiliency of weapon systems, but it has not yet become the general practice in the DAF, and little policy or guidance directs specifically how to do it at the service level. An overreliance is still placed on the Risk Management Framework (RMF), which is largely carried out after systems engineering.

During the operations and sustainment phase, wing-level organizations perform much of the day-to-day security monitoring of weapon systems. However,

- They are not provided with authorized tools tailored to their weapon systems.
- The tools that they have cannot comprehensively monitor or defend their weapon systems.
- They are not provided with technical orders for what to do.
- Policy does not generally require feedback to the program offices of weapon system cyber status or cyber incidents.

Cybersecurity and cyber resiliency are not central parts of current sustaining engineering or life cycle sustainment plans.

Recommendations

Our principal message can be summarized as a recommendation to develop and maintain an integrated engineering-based plan for the cybersecurity and cyber resiliency of each weapon system throughout its life cycle. For the design phase, we advocate that systems security engineering be enhanced by placing into the program plan and contract language:

- standards for designing systems with adequate cyber separability
- methods that the DoD will use to assess cyber resiliency of designs.

These engineering and contract statements need to be specific and measurable with regard to the security outcomes. Before these can be issued, further development and refinement, based on experience, is needed for both the standards and methods.

For the operations and sustainment phase, we advocate for increased use of sustaining engineering and the life cycle sustainment plans for cybersecurity and cyber resiliency. We recommend that program offices do the following:

- Equip wing-level organizations with approved tools for any cyber monitoring of a weapon system that are
  - catered to the weapon system
  - rigorously designed, developed, and tested with a security mindset, so as not to introduce attack vectors into the system
  - comprehensive in their ability to access the weapon system.
- Provide wing-level organizations, such as mission defense teams, with technical orders for the cyber monitoring of weapon systems.
- Receive information regarding any non-nominal behavior within the system boundary or cyber incident.
- Direct and approve any configuration change within the system boundary.

We recommend that the DAF develop an ecosystem for cyber sustaining engineering that uses or mirrors the ecosystem for aircraft maintenance, including processes such as Form 22 notifications for discrepancies in the above-mentioned technical orders and 107 requests for additional, cyber-related technical assistance from program offices.

Life cycle management plans should explicitly outline how the cybersecurity and cyber resiliency of each weapon system will be assured during operations, sustainment, and disposal.

Security should not be considered an activity implemented by RMF but one created by sound engineering and continuous vigilance, rigorously and continuously assessed by RMF.

Contents

About This Report iii
Summary v
Chapter 1. Securing Weapon Systems in Contested Cyber Environments 1
The Goal of Security 1
The Nature of Security 3
Chapter 2. Systems Security Engineering 4
Engineering for Security 4
Findings 7
Recommendations 8
Chapter 3. Sustaining Engineering 10
Engineering for Security 10
Findings 11
Recommendations 12
Chapter 4. Closing Comments 13
Abbreviations 15
References 16

Chapter 1. Securing Weapon Systems in Contested Cyber Environments

> Because security requirements are generally stated as constraints on systems operation, security in the engineering workplace is increasingly considered an obstacle to operations rather than an enabler of mission assurance.
>
> —Jennifer L. Bayuk and Barry M. Horowitz[1]

The Goal of Security

Weapon systems must work under pertinent threat conditions, or they do not meet mission needs. One threat condition that has proven difficult to address is adversarial cyber operations. The negative effects of cyber operations can extend beyond mission failure if an adversary takes control of a system.

Adversarial cyber operations can be experienced in peacetime as well as wartime, at home station as well as deployed. Cyber operations come in many forms. Vulnerabilities in a weapon system can be exploited to exfiltrate information about the weapon system. An adversary can use such information to accelerate its weapon systems designs or to develop countermeasures to U.S. weapon systems. Successful cyber operations can also directly attack U.S. weapon systems, deleting critical data, altering data to a degree that a system cannot be used with confidence, denying communications, and taking control of a weapon system.

To counter adversarial cyber operations, a combination of defensive measures and resiliency efforts must be employed. Defensive measures include security controls, monitoring systems, and cyber-incident response planning. They are generally efforts done to keep adversaries out of systems and to protect systems—they defend boundaries. But defensive measures alone are insufficient.[2] Resiliency efforts are also needed, which strive to design and maintain system configurations that are robust to attack and limit the operational impact of adversarial actions. That is, they strive to ensure that systems are always able to absorb cyber operations such that any exfiltrated information or attack remains within an acceptable level of mission degradation.[3] Resiliency efforts focus on the sound architectural design of the system itself—they make the design of the system support successful functioning during and after an attack. Within the Department of Defense (DoD), the term *cybersecurity* tends to be associated with defensive

[1] Bayuk and Horowitz, "An Architectural Systems Engineering Methodology for Addressing Cyber Security," p. 296.

[2] Bayuk and Horowitz, "An Architectural Systems Engineering Methodology for Addressing Cyber Security."

[3] Cárdenas, Amin, and Sastry, "Secure Control."

measures. In this report, we stress a balance of defensive and resiliency measures, so we will refer to these balanced efforts as *cybersecurity and cyber resiliency*. For brevity, on occasion we will use the shorter term *security* for cybersecurity and cyber resiliency.

Ensuring cybersecurity and cyber resiliency requires integrated activities across the Department of the Air Force (DAF). Every organization within the DAF plays a role in this assurance.[4] In this report, we emphasize the role of the acquisition community in assuring cybersecurity and cyber resiliency of weapon systems, focusing on the role that program offices play in engineering throughout the life cycle of a weapon system. We therefore restrict our attention to the aspects of the problem that lie within the system boundary. We further emphasize the management of platform information technology (PIT) in weapon systems, which is defined as "[i]nformation technology (IT), both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems."[5]

PIT in weapon systems presents problems that differ from those of traditional information technology systems, such as business or administrative systems using Internet protocols and common consumer operating systems and software. PIT runs in real time, inseparably integrates with hardware, and often uses bespoke operating systems and software. Because of the installation on weapon systems, changes to PIT (including security measures) are often constrained by weight, heat dissipation, and latency. Solutions for cybersecurity and cyber resiliency for traditional information technology are often not appropriate for weapon systems. Although the DoD inherits any security flaws when it buys commercial products and attempts retroactively to mitigate those flaws by applying security controls, when procuring weapon systems, the DoD has control over design. Hence, the DoD has opportunities during design to proactively manage cybersecurity and cyber resiliency. Research has indicated that such coordinated approaches to cybersecurity and cyber resiliency are more efficient and have a better overall return on investment.[6]

The purpose of this report is to outline areas where the cybersecurity and cyber resiliency of weapon systems in the DAF can be improved throughout their life cycles. The focus is on what program offices can do and where acquisition policy can be improved. We do not attempt a comprehensive life cycle plan for the cybersecurity and cyber resiliency of weapon systems. Based on our review of current policy and practice, and what is known thus far from the engineering literature, we discuss critical areas where policy is lacking and that a proactive program office could pioneer better management of cybersecurity and cyber resiliency during selected phases of the life cycle of a weapon system.

---

[4] Snyder et al., *Managing for Mission Assurance in the Face of Advanced Cyber Threats*.

[5] Committee on National Security Systems, *Committee on National Security Systems (CNSS) Glossary*; Department of Defense Instruction 8500.01, *Cybersecurity*.

[6] Heitzenrater, *Software Security Investment Modelling for Decision-Support*.

The Nature of Security

Cybersecurity and cyber resiliency have much in common with other measures to meet the threat environment as well as some aspects that are unique. An integral element of security in the cyber domain is that it emerges from the sum of internal and external factors. Internal factors include design decisions, configuration control throughout the life cycle, and how operators interact with a weapon system. External factors include evolving technologies, discovery of vulnerabilities, and a changing threat environment. Security is, therefore, an emergent attribute of a weapon system.[7]

Because of its emergent nature, reasoning about security must be made within a specific context. Context refers here to the state of a weapon system relative to the threats it faces, its current posture, and the environment in which it operates. It is within this context that a system stakeholder makes trust decisions regarding the ability of a system to carry out a given mission.

The emergent and contextual nature of security means that security efforts are never complete. The nature of weapon-system security is such that it always carries with it unquantifiable uncertainties. Management of cybersecurity and cyber resiliency is, therefore, an exercise in risk management, not simply one of requirements definition or periodic application of security controls.[8]

Because of these attributes of cybersecurity and cyber resiliency, security (1) must be actively managed throughout the life cycle of a weapon system, from early research and development stages through disposal, and (2) must be managed in an integrated, deliberately coordinated effort. Security cannot simply be designed into a system and then forgotten, nor can security be achieved without being judiciously considered during early design stages. If left to later stages, risk mitigation becomes increasingly difficult and costly. In the remainder of this report, we select key phases in the life cycle of a weapon system and discuss where program offices can improve the security of weapon systems and where policy could change to drive better behavior, emphasizing the role that engineering plays throughout the life cycle of a weapon system.

---

[7] In the theory of complex systems, *emergence* is characteristic of a complex system in which the global properties of a system arise from the interactions of its elements, not as a sum of the properties of the elements. When hydrogen and oxygen combine to form a water molecule, the emergent property of water is not the sum of the properties of atomic hydrogen and oxygen.

[8] Snyder et al., *Measuring Cybersecurity and Cyber Resiliency*.

Chapter 2. Systems Security Engineering

> *Systems security engineering* is a specialty engineering discipline of systems engineering that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties and other contributing engineering specialties to provide a fully integrated, system-level perspective of system security.
>
> —Ron Ross, Michael McEvilley, and Janet Carrier Oren[9]

Engineering for Security

The more that vulnerabilities can be identified and mitigated early in the design phase, the cheaper and easier it is to resolve them.[10] Some issues, such as single points of failure if attacked, emerge from architectural characteristics of a system. Architectures are established early in design and are costly, if not impossible, to change at later stages. Evaluating a system's security after design with the goal of rectifying deficiencies through security controls goes against basic engineering principles.

The accepted mechanism for incorporating cybersecurity and cyber resiliency into design is through normal engineering processes, namely systems engineering. The purposeful inclusion of security concerns in systems engineering is called *systems security engineering*.[11] The original definition of systems security engineering, and the one most commonly used, is "[a]n element of system[s] engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats."[12] The goal of systems security engineering is *system security*, defined as "freedom from those conditions that can cause a loss of assets with unacceptable consequences."[13]

---

[9] Ross, McEvilley, and Oren, *Systems Security Engineering*, p. 9. Italics are in the original.

[10] See, for instance, Davison, Cameron, and Crawley, "Technology Portfolio Planning by Weighted Graph Analysis of System Architectures"; and Nourian and Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet."

[11] Anderson, *Security Engineering*; Bayuk, *Systems Security Engineering*; Ross, McEvilley, and Oren, *Systems Security Engineering*; Ross et al., *Developing Cyber-Resilient Systems*.

[12] DoD Handbook MIL-HDBK-1785, *System Security Engineering Program Management Requirements*, p. 5.

[13] Ross, McEvilley, and Oren, *Systems Security Engineering*, p. 18.

After a series of well-studied accidents—especially the losses of the Space Shuttles *Challenger* and *Columbia*—new concepts have emerged for safety and security of complex systems. Previous approaches—such as fault tree analysis and failure mode, effects, and criticality analysis—relied on enumerating all the possible failures of a system to design a sufficiently robust system using redundancy and other measures. New approaches recognize that the scale and complexity of many modern systems prevent enumerating all possible permutations that a system will realize. Instead, these new concepts emphasize the reverse—clearly defining the set of states that a system should remain within (which is less numerous than the possible undesirable states) and designing controls to prevent a system from departing from the set of desired states.[14]

A family of similar methodological approaches embrace this new way of thinking. Among those that are currently influencing acquisition programs in the DoD are the System Theoretical Accident Model and Process (STAMP), Systems-Theoretic Process Analysis (STPA), STPA for Security (STPA-Sec), Causal Analysis based on System Theory, Cyber Mission Thread Analysis, and methods derived from these, most notably Functional Mission Analysis-Cyber.[15]

The seminal methods in this space have their roots in the field of safety and were subsequently extended to apply to cybersecurity and cyber resiliency.[16] Several recent efforts have applied these methods to the cybersecurity of specific case studies with the aim of influencing system design.[17] One study focuses on the use of these cybersecurity concepts using the System Modeling Language (SysML), a modeling language commonly used in the DoD for digital engineering and model-based systems engineering.[18] Although specific use of SysML has been studied, it has also been argued that SysML has limitations for handling all relevant aspects of assessing the security of embedded systems.[19] The core concepts for safety and security have been recently extended by combining them with other methods to reduce the potential of

---

[14] For an early review of this change in thinking, see Hollnagel, Woods, and Leveson, *Resilience Engineering*.

[15] Leveson, *Engineering a Safer World*; Abdulkhaleq, Wagner, and Leveson, "A Comprehensive Safety Engineering Approach for Software Intensive Systems Based on STPA"; Bjerga, Aven, and Zio, "Uncertainty Treatment in Risk Analysis of Complex Systems"; Snyder et al., *Wing-Level Mission Assurance for a Cyber-Contested Environment*; Patriarca et al., "The Past and Present of System-Theoretic Accident Model and Processes (STAMP) and Its Associated Techniques"; Zhang et al., "Systems Theoretic Accident Model and Process (STAMP)"; Mayer et al., *Improving the Technical Requirements Development Process for Weapon Systems*.

[16] Young and Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory."

[17] Friedberg et al., "STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems"; Span et al., "Conceptual Systems Security Requirements Analysis"; Nourian and Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet"; Shin et al., "Application of STPA-SafeSec for a Cyber-Attack Impact Analysis of NPPs with a Condensate Water System Test-Bed." See also Carreras Guzman, Kozine, and Lundteigen, "An Integrated Safety and Security Analysis for Cyber-Physical Harm Scenarios."

[18] Carter et al., "Systems-Theoretic Security Requirements Modeling for Cyber-Physical Systems."

[19] Ali, "Formal Verification of SysML Diagram Using Case Studies of Real-Time System." See also Mili, Nguyen, and Chelouah, "Model-Driven Architecture Based Security Analysis." For a survey of SysML, see Delligatti, *SysML Distilled*.

overlooking important security aspects.[20] Some other recent research has simultaneously evaluated safety and cybersecurity in an integrated approach.[21]

Although there are similarities between safety and security that encourage integrated approaches, the mitigation techniques and derived technical requirements for safety and security can be different in important ways.[22] For both safety and security, one principal goal is to reduce the probability of correlated component failures that cause system failure. For safety, redundancy is a common mitigation technique. For example, using multiple hydraulic lines with independent pumps to manipulate a control surface on an aircraft provides a low probability of correlated failure if the lines run physically distinct paths. Yet redundancy alone renders little resiliency to cyber attack if each additional component of common design and configuration is similarly susceptible.

Another difference between safety and security is what constitutes an unacceptable hazard. For cybersecurity and cyber resiliency, unacceptable behavior can occur even when all components operate in a nominal state within the normal envelope of performance if an unauthorized actor is in control. This is a fundamental difference between safety and security—security involves not just the sum of the behavior of the components of a system but also the authorities related to system control.

The previously listed methods are good for identifying design deficiencies, especially those at the architectural level. They are new, powerful methods to supplement other efforts at the simpler component level, such as fault tree analysis and failure mode, effects, and criticality analysis. In addition to emphasizing architectural security during program planning, program managers require mechanisms to place language in contracts to prime contractors that drive secure designs. The *cyber separability* approach for mitigating discovered deficiencies takes its motivation from safety but is tailored as needed for the context of cybersecurity and cyber resiliency.[23]

The basic concept of cyber separability is to perform a system decomposition using one or more of the methods listed above. Decomposition reveals a subset of functions or components that are mission or safety critical. Loss of one of these leads to an unacceptable hazard to the mission. Security approaches for each of these critical functions or components levy a

---

[20] de Souza et al., "Extending STPA with STRIDE to Identify Cybersecurity Loss Scenarios"; Carreras Guzman et al., "A Comparative Study of STPA-Extension and the UFoI-E Method for Safety and Security Co-Analysis."

[21] Friedberg et al., "STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems"; Carreras Guzman et al., "Conceptualizing the Key Features of Cyber-Physical Systems in a Multi-Layered Representation for Safety and Security Analysis"; Carreras Guzman, Kozine, and Lundteigen, "An Integrated Safety and Security Analysis for Cyber-Physical Harm Scenarios"; Carreras Guzman et al., "A Comparative Study of STPA-Extension and the UFoI-E Method for Safety and Security Co-Analysis"; Shin et al., "Application of STPA-SafeSec for a Cyber-Attack Impact Analysis of NPPs with a Condensate Water System Test-Bed."

[22] Snyder et al., *Cyber Mission Thread Analysis*.

[23] Snyder et al., *Cyber Mission Thread Analysis*, pp. 26−28.

requirement that any cyber element supporting the function or component have at least one back-up so that no single cyber attack is likely to simultaneously affect both. Cyber-separable components are not *redundant*. Redundancy is when two or more identical components are available for a task. Cyber attacks can place identical components at risk simultaneously. Cyber-separable components are *diverse*. Diverse components are ones that differ in design or configuration to the extent that they are unlikely to be mutually susceptible to a common cyber attack. An architectural design for a weapon system that employs cyber separability in systems engineering is significantly more likely to have high cyber resiliency. The use of different processor types for critical control functions is an example of diversity.

Findings

Systems security engineering has recently been directed by policy within the DoD,[24] but the approach that we outline above has not yet become the general practice in the DAF, and little policy or guidance directs specifically how to do it at the service level. Instead, the dominant policy for security of weapon systems remains the Risk Management Framework (RMF).[25] Although the RMF contains sound practices, it has been interpreted and implemented within the DoD in unfortunate ways that emphasize defensive measures (e.g., security controls) over resiliency measures (e.g., sound security engineering design). It has created a culture in which cybersecurity is seen as the responsibility of RMF, and less so one of engineering. This result is natural, as the RMF created by the National Institute of Standards and Technology was designed for making *commercial* information technology systems as secure as possible. The government has no say in the design of these systems, and therefore must inherit any of their security deficiencies.

The implementation of RMF in DoD has also encouraged an atmosphere in which systems are first designed, and then after design, security controls are placed on the system by the RMF process in an attempt to improve security. Even the nomenclature used encourages this restrictive way of approaching security—the technical assessors advising authorizing officials in the RMF process are called *security control assessors* rather than *system security assessors*, or *system risk assessors*.[26] The implication is that their job is to apply security controls on an already designed,

---

[24] DoD Instruction 5000.83, *Technology and Program Protection to Maintain Technological Advantage*; Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*. See also Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*, Section 6.2.1; U.S. Air Force, *Systems Security Engineering (SSE) Acquisition Guidebook*; and U.S. Air Force, *Systems Security Engineering Cyber Guidebook*.

[25] DoD Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*; Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*.

[26] For a full discussion, see Snyder et al., *Managing for Mission Assurance in the Face of Advanced Cyber Threats*, pp. 29−35.

and potentially architecturally flawed, system. The statutory preference for acquiring commercial, off-the-shelf components for cost reasons rather than prioritizing designing for security amplifies this situation.[27] Both the overreliance on RMF for security, and the implementation of RMF with a focus on security controls limit the benefits for security that systems security engineering can bring.

Traditional systems engineering fails to incorporate security because its processes are built around meeting static technical requirements[28] because security is often equated with information assurance and therefore the responsibility of RMF.[29] Indeed, the implementation of RMF places the security of the system to adversarial cyber operations in the program protection plan and not in the systems engineering plan. However, as can be seen from the literature cited above, standard practices for systems security engineering continue to evolve and to be refined; they are relatively immature.

Recommendations

The principal recommendations are to place the following into the program plan and contract language:

- standards for designing systems with adequate cyber separability
- methods that the DoD will use to assess cyber resiliency of designs.

Employing systems security engineering is current DoD policy, although mechanisms for doing so and service-level details for how to do systems security engineering are still developing.[30] The goal of these recommendations is to establish mechanisms to drive security considerations early in the life cycle of a weapon system via designing for security and not relying on the application of RMF after system design. Applying RMF to a well-designed system that includes sound systems security engineering is a strong start to system cybersecurity and cyber resiliency.

As mentioned above, both the standards for cyber separability and methods to assess cyber resiliency of designs are areas of active research and are therefore evolving. Therefore, it is premature to write these standards and policies. A path is needed to get to the juncture when the following can be issued: (1) a military standard for cyber separability; (2) a DAF instruction for

---

[27] U.S. Code, Title 10, Section 3453. DAF policy directs: "The PM [program manager] utilizes . . . commercial standards and interfaces to the maximum extent practicable For Commercial-Off-the-Shelf systems and components being contemplated for use in the program, the PM evaluates the risks of using those items in the intended military use environment." Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*, Sections 5.1.1 and 5.4.5.

[28] Bayuk, *Systems Security Engineering*.

[29] Baldwin, "Systems Security Engineering: A Critical Discipline of Systems Engineering."

[30] DoD Instruction 5000.83, *Technology and Program Protection to Maintain Technological Advantage*.

systems security engineering; and (3) a DAF manual for implementing systems security engineering.

Further development and refinement, based on experience, is needed for both the standards and methods. Program offices and the Air Force Research Laboratory can play important roles. Regarding methods, STAMP, STPA-Sec, and similar approaches appear promising, but more refinement and proven track records are needed before they are enshrined. The DoD and DAF have more incentives to make security a central design element than commercial industry, who confront a different problem set and often do not suffer the consequences of security failures of their systems.

To support the principal recommendations above, the DAF should not wait for developments in these methodologies by academia or industry but instead should take the lead in further developing, testing, and refining these methods for military applications. Regarding standards for cyber separability, the path is similar. Efforts at developing standards for cyber separability will be stronger the more collaborative they are between the acquisition community and the RMF actors. Program offices can begin as pathfinders in these efforts. But for both methods and standards, some organization within the DAF will need to collect and disseminate lessons with the aim of informing the writing of standards and policy. In the interim, some guidelines would be useful for coordinating efforts.

Chapter 3. Sustaining Engineering

> How do we assure cyber resilience of the NC2 [nuclear command and control] system of the future? One important idea is to replace a culture of "tell me what I need to buy for cyber resilience so I can be done with it" with a culture of "this problem is 24/7 for the life of my system; I must assume the bad guys are already inside and my job is to confuse and deceive so that I can operate around them." This means continuous cyber surveillance of the system by really good people and tearing down the offense-defense stovepipes in establishing a permanent cyber offense "red team" to challenge defenders. — John Harvey[31]

Engineering for Security

Because of the characteristics of the cyber environment that we presented in Chapter 1, observation, monitoring, scanning, and occasional adjustments to configurations of systems during operations and sustainment are necessary for sustaining security. Security "requirements" are not static.[32] Even with strong and well-executed efforts in systems security engineering, the combination of changing technologies, an evolving threat environment, discoveries of susceptibilities, and new operational environments for a weapon system requires continuous vigilance for system security. Many dimensions of these activities lie within the system boundary and are highly technical. Exactly what to monitor, the tools that should be authorized to do such monitoring, and judgments regarding any configuration changes to the system for mitigating any issues discovered are engineering decisions.

Sustaining engineering is defined by the Defense Acquisition University to be "[t]echnical tasks (engineering and logistics investigations and analyses) to ensure continued operation and maintenance of a system with managed risk. This involves identification, review, assessment, and resolution of deficiencies throughout a system's life cycle."[33] The engineering component of sustaining the cybersecurity and cyber resiliency of a weapon system falls within this definition.

Weapon systems are in the possession of operators during the operations and sustainment phase of their life cycle, and therefore, operators play a key role in sustaining security. As of 2022, mission defense teams (MDTs) have been established at the wing level to monitor weapon systems and tactically defend them, at home station and deployed.[34] MDTs have largely been

---

[31] John Harvey, "Documentation," p. 245.

[32] See, for example, Mulokey, "Using the U.S. Department of Defense Architecture Framework to Build Security into the Lifecycle"; Snyder et al., *Measuring Cybersecurity and Cyber Resiliency*.

[33] Defense Acquisition University, *DAU Glossary of Defense Acquisition Acronyms and Terms*.

[34] For more on MDTs, see Air Combat Command, *Air Combat Command as Air Force Lead Command for Cyber Forces*; and Headquarters United States Air Force, *Implementation of Department of the Air Force Cyber Squadrons*.

devising their own approaches for monitoring and defending their weapon systems. The most common tool they use is the Cyberspace Vulnerability Assessment/Hunter (CVA/H) weapon system.[35] CVA/H was developed for monitoring and defending traditional information technology systems using Internet protocols rather than for specific PIT systems. CVA/H and similar tools are, therefore, not useful for many PIT applications, leaving parts of the weapon systems without suitable tools for monitoring or defending. Furthermore, MDTs have been the parties seeking authority to operate and authority to connect to their weapon systems for CVA/H and other tools rather than having approved tools provided to them.[36] This situation may inadvertently introduce risk by decentralizing the challenge of maintaining a toolset that is complete, is effective, and does not introduce vulnerabilities or act as an adversary vector into the PIT. Finally, when cyber-related issues arise with weapon systems, program offices are not indicated by policy as key stakeholders or as recipients of reported incidents.[37]

Findings

Wing-level organizations perform much of the day-to-day security monitoring of weapon systems. In contexts outside of cybersecurity and cyber resiliency, it is an unusual circumstance that wing-level organizations (1) determine how to perform technical monitoring within the system boundary, (2) obtain authorization to operate and/or connect for tools, or (3) determine what technical actions to take within a system when issues arise. In aircraft maintenance, for example, these responsibilities fall to program offices. Program offices provide tailored tools designed for the task at hand, such as support and test equipment, with authorization to operate or connect that equipment to a weapon system obtained before the wing receives the equipment. Program offices issue technical manuals detailing exact procedures to follow when using equipment and actions to take when changes need to be made. Wing-level personnel are expected to comply with these technical orders, not operate on their own judgment. Furthermore, when aircraft maintenance technical orders appear to be in error or fail to address a problem faced by wing-level personnel, formal procedures exist for redress. When wings believe technical data to be in error, they file a notice through the Form 22 process.[38] When technical data are insufficient to address a problem that they face, they file a "107 request," named after the governing technical order.[39] No similar ecosystem exists for managing the technical side of cybersecurity and cyber resiliency within a weapon system boundary.

---

[35] See Carter, "552nd Air Control Networks Squadron Creates First Qualification Training for Mission Defense Teams."

[36] Snyder et al., *Wing-Level Mission Assurance for a Cyber-Contested Environment*.

[37] Air Force Instruction 17-203, *Cyber Incident Handling*.

[38] Technical Manual TO 00-5-1, *AF Technical Order System*, Section 9.

[39] Technical Manual TO 00-25-107, *Maintenance Assistance*.

Although policy broadly directs continuous vigilance of security,[40] the emphasis leans on RMF over engineering, and the supporting ecosystem for program office support is lacking relative to functional areas, such as aircraft maintenance. In the *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, cybersecurity and cyber resiliency during operations and sustainment are barely mentioned, and no framework is provided for how a program is expected to exercise technical monitoring and coordinate with operational units.[41] One policy document related to sustainment and life cycle management declares that "[c]ybersecurity is implemented through the Risk Management Framework (RMF)."[42] This direction is in contrast to our findings, in which we would say that cybersecurity and cyber resiliency are implemented through sustaining engineering during operations and sustainment and assessed through the RMF process.

Recommendations

We recommend that program offices do the following:

- Equip wing-level organizations with approved tools for any cyber monitoring of a weapon system that are
  - catered to the weapon system
  - rigorously designed, developed, and tested with a security mindset, so as not to introduce attack vectors into the system
  - comprehensive in their ability to access the weapon system.
- Provide wing-level organizations, such as MDTs, with technical orders for the cyber monitoring of weapon systems.
- Receive information regarding any non-nominal behavior within the system boundary or cyber incident.
- Direct and approve any configuration change within the system boundary.

We recommend that the DAF develop an ecosystem for cyber sustaining engineering that uses or mirrors the ecosystem for aircraft maintenance, including processes such as Form 22 notifications for discrepancies in the above-mentioned technical orders and 107 requests for additional, cyber-related technical assistance from program offices.

Life cycle management plans should explicitly outline how the cybersecurity and cyber resiliency of each weapon system will be assured during operations, sustainment, and disposal.

---

[40] Air Force Instruction 17-130, *Cybersecurity Program Management*.

[41] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, pp. 42−43.

[42] DAF Pamphlet 63-128, *Integrated Life Cycle Management*, Section 15.12.7.

Chapter 4. Closing Comments

> The DOD's relentless expansion of internet protocol (IP) networks has greatly improved our peacetime ability to communicate. But it has often been accomplished with little regard for cybersecurity, and has created an ever-growing network boundary that the DOD has limited ability to defend.
>
> — Robert F. Behler[43]

Our principal message can be summarized as a recommendation to develop and maintain an integrated engineering-based plan for the cybersecurity and cyber resiliency of each weapon system throughout its life cycle. By *integrated*, we mean that the activities of maintaining an integrated effort for the cybersecurity and cyber resiliency of a weapon system throughout its life cycle should not be partitioned from the other acquisition (life cycle management) activities. Instead, security should be part of systems engineering and sustaining engineering and be a major component of the life cycle sustainment plan. Rather than create a new administrative burden in the form of an approved and periodically updated life cycle plan for cybersecurity and cyber resiliency, we propose a more formal introduction of elements of such a plan into the systems engineering and life cycle sustainment plans. Security should not be considered an activity implemented by RMF but one created by sound engineering and continuous vigilance, rigorously and continuously assessed by RMF.

Although current policy now incorporates systems security engineering into policy, it places the associated plan as an appendix to the program protection plan emphasizing defensive measures of information assurance for approval by the relevant authorizing officials rather than as an integral part of the systems engineering and life cycle sustainment plans. Therefore, current policy understates the importance of the role of systems security engineering and sustaining engineering in security, emphasizing instead the role of RMF.

Providing an ecosystem for cyber-related engineering support to security modeled after the mature ecosystem for aircraft maintenance will accelerate and institutionalize the engineering component of cybersecurity and cyber resiliency within the system boundary of weapon systems. However, enhancing the role of engineering through the program offices and larger acquisition community will require changes to workforce and culture. Personnel in program offices will need to understand that they are key actors in weapon system cybersecurity and cyber resiliency and exactly what their roles are. They must not see security as a function assigned to a specialized group but one in which everyone has equities. This need also means that systems

[43] Behler, *Director, Operational Test and Evaluation*, p. 227.

engineers, sustaining engineers, and product support managers will need to be more versed in cyber operations and mitigation methods.[44]

The changes that we recommend will require more funding, and funding in appropriately dedicated budget lines. They will also require an adequate number of positions and a workforce with the necessary skills. The funding and changes to the workforce allocation should not be considered *costs* but should be viewed as the *investments* needed for mission assurance. This is the view for such areas as flight worthiness and flight safety of an aircraft. The associated costs can be appreciable but are accepted relative to the costs of the consequences of not having adequate flight worthiness and safety. Without these changes, the DAF will accept risk in a cyber contested environment, and its readiness will be jeopardized.

[44] For recommendations on changing the culture with regard to cybersecurity, see Snyder et al., *Managing for Mission Assurance in the Face of Advanced Cyber Threats*, pp. 39−48.

Abbreviations

CVA/H	Cyberspace Vulnerability Assessment/Hunter
DAF	Department of the Air Force
DoD	Department of Defense
MDT	mission defense team
PIT	platform information technology
RMF	Risk Management Framework
STAMP	System Theoretical Accident Model and Process
STPA	Systems-Theoretic Process Analysis
STPA-Sec	Systems-Theoretic Process Analysis for Security
SysML	System Modeling Language

References

Abdulkhaleq, Asim, Stefan Wagner, and Nancy Leveson, "A Comprehensive Safety Engineering Approach for Software Intensive Systems Based on STPA," *Procedia Engineering*, Vol. 128, 2015, pp. 2−11.

Air Combat Command, *Air Combat Command as Air Force Lead Command for Cyber Forces: Air Force Mission Defense Team (MDT) Operating Concept*, January 2020, Not available to the general public.

Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, Secretary of the Air Force, February 6, 2020.

Air Force Instruction 17-130, *Cybersecurity Program Management*, Secretary of the Air Force, February 13, 2020.

Air Force Instruction 17-203, *Cyber Incident Handling*, Secretary of the Air Force, March 16, 2017.

Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*, Secretary of the Air Force, June 30, 2020, Incorporating Change 1, November 23, 2021.

Ali, Sajjad, "Formal Verification of SysML Diagram Using Case Studies of Real-Time System," *Innovations in Systems and Software Engineering*, Vol. 14, No. 4, 2018, pp. 245–262.

Anderson, Ross, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., Wiley, 2008.

Baldwin, Kristen, "Systems Security Engineering: A Critical Discipline of Systems Engineering," *INCOSE Insight*, Vol. 12, No. 2, July 2009, pp. 11−13.

Bayuk, Jennifer, *Systems Security Engineering*, Systems Engineering Research Center, Report No. SERC-2010-TR-005, August 22, 2010.

Bayuk, Jennifer L., and Barry M. Horowitz, "An Architectural Systems Engineering Methodology for Addressing Cyber Security," *Systems Engineering*, Vol. 14, No. 3, 2011, pp. 294−304.

Behler, Robert F., *Director, Operational Test and Evaluation: FY 2019 Annual Report*, Department of Defense, December 20, 2019.

Bjerga, Torbjørn, Terje Aven, and Enrico Zio, "Uncertainty Treatment in Risk Analysis of Complex Systems: The Cases of STAMP and FRAM," *Reliability Engineering & System Safety*, Vol. 156, December 2016, pp. 203–209.

Cárdenas, Alvaro A., Saurabh Amin, and Shankar Sastry, "Secure Control: Towards Survivable Cyber-Physical Systems," *Proceedings of the 28th International Conference on Distributed Computing Systems Workshop*, 2008.

Carreras Guzman, Nelson H., Morten Wied, Igor Kozine, and Mary Ann Lundteigen, "Conceptualizing the Key Features of Cyber-Physical Systems in a Multi-Layered Representation for Safety and Security Analysis," *Systems Engineering*, Vol. 23, No. 2, 2020, pp. 189–210.

Carreras Guzman, Nelson H., Igor Kozine, and Mary Ann Lundteigen, "An Integrated Safety and Security Analysis for Cyber-Physical Harm Scenarios," *Safety Science*, Vol. 144, December 2021.

Carreras Guzman, Nelson H., Jin Zhang, Jing Xie, and Jon Arne Glomsrud, "A Comparative Study of STPA-Extension and the UFoI-E Method for Safety and Security Co-Analysis," *Reliability Engineering & System Safety*, Vol. 211, July 2021.

Carter, Bryan T., Georgios Bakirtzis, Carl R. Elks, and Cody H. Fleming, "Systems-Theoretic Security Requirements Modeling for Cyber-Physical Systems," *Systems Engineering*, Vol. 22, No. 5, 2019, pp. 411–421.

Carter, Joshua, "552nd Air Control Networks Squadron Creates First Qualification Training for Mission Defense Teams," 552nd Air Control Wing, November 12, 2019.

Committee on National Security Systems, *Committee on National Security Systems (CNSS) Glossary*, CNSSI No. 4009, April 6, 2015.

DAF—See Department of the Air Force.

Davison, Peter, Bruce Cameron, and Edward F. Crawley, "Technology Portfolio Planning by Weighted Graph Analysis of System Architectures," *Systems Engineering*, Vol. 18, No. 1, 2015, pp. 45−58.

Defense Acquisition University, *DAU Glossary of Defense Acquisition Acronyms and Terms*, July 21, 2020.

Delligatti, Lenny, *SysML Distilled: A Brief Guide to the Systems Modeling Language*, Addison-Wesley, 2014.

Department of the Air Force Pamphlet 63-128, *Integrated Life Cycle Management*, Secretary of the Air Force, February 3, 2021.

Department of Defense Handbook MIL-HDBK-1785, *System Security Engineering Program Management Requirements*, Department of Defense, August 1, 1995 (rescinded).

Department of Defense Instruction 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, Office of the Under Secretary of Defense for Research and Engineering, Change 1, May 21, 2021.

Department of Defense Instruction 8500.01, *Cybersecurity*, March 14, 2014, Incorporating Change 1, October 7, 2019.

Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 12, 2014, Incorporating Change 3, December 29, 2020.

de Souza, Nivio Paula, Cecília de Azevedo Castro César, Juliana de Melo Bezerra, and Celso Massaki Hirata, "Extending STPA with STRIDE to Identify Cybersecurity Loss Scenarios," *Journal of Information Security and Applications*, Vol. 55, December 2020.

DoD—*See* Department of Defense.

Friedberg, Ivo, Kieran McLaughlin, Paul Smith, David Laverty, and Sakir Sezer, "STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems," *Journal of Information Security and Applications*, Vol. 34, June 2017, pp. 183−196.

Harvey, John, "Documentation," *Comparative Strategy*, Vol. 38, No. 3, 2019, pp. 234−251.

Headquarters United States Air Force (HQ USAF), *Implementation of Department of the Air Force Cyber Squadrons*, Department of the Air Force, Program Action Directive (PAD) D15-03, May 12, 2020, Not available to the general public.

Heitzenrater, Chad, *Software Security Investment Modelling for Decision-Support*, thesis, University of Oxford, 2017.

Hollnagel, Erik, David D. Woods, and Nancy Leveson, eds., *Resilience Engineering: Concepts and Precepts*, Ashgate, 2006.

Leveson, Nancy G., *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, 2011.

Mayer, Lauren A., William Shelton, Christian Johnson, Daniel Adducchio, Raza Khan, Suzanne Genc, Danielle C. Tarraf, and Nahom Beyene, *Improving the Technical Requirements Development Process for Weapon Systems: A Systems-Based Approach for Managers*, RAND Corporation, RR-A997-1, 2022. As of December 4, 2023: https://www.rand.org/pubs/research_reports/RRA997-1.html

Mili, Saoussen, Nga Nguyen, and Rachid Chelouah, "Model-Driven Architecture Based Security Analysis," *Systems Engineering*, Vol. 24, No. 5, 2021, pp. 307–321.

Mulokey, William P., "Using the U.S. Department of Defense Architecture Framework to Build Security into the Lifecycle," *INCOSE Insight*, Vol. 12, No. 2, 2009, pp. 27−29.

Nourian, Arash, and Stuart Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet," *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 1, January/February 2018, pp. 2–13.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, Version 1.0, May 26, 2015.

Patriarca, Riccardo, Mikela Chatzimichailidou, Nektarios Karanikas, and Giulio Di Gravio, "The Past and Present of System-Theoretic Accident Model and Processes (STAMP) and Its Associated Techniques: A Scoping Review," *Safety Science*, Vol. 146, February 2022.

Ross, Ron, Michael McEvilley, and Janet Carrier Oren, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, U.S. Department of Commerce, NIST Special Publication 800-160, Vol. 1, November 2016.

Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, U.S. Department of Commerce, NIST Special Publication 800-160 Vol. 2, Revision 1, December 2021.

Shin, Jinsoo, Jong-Gyun Choi, Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Jun-Young Son, "Application of STPA-SafeSec for a Cyber-Attack Impact Analysis of NPPs with a Condensate Water System Test-Bed," *Nuclear Engineering and Technology*, Vol. 53, No. 10, 2021, pp. 3319−3326.

Snyder, Don, Elizabeth Bodine-Baron, Dahlia Anne Goldfeld, Bernard Fox, Myron Hura, Mahyar A. Amouzegar, and Lauren Kendrick, *Cyber Mission Thread Analysis: A Prototype Framework for Assessing Impact to Missions from Cyber Attacks to Weapon Systems*, RAND Corporation, RR-3188/1-AF, 2022. As of December 4, 2023: https://www.rand.org/pubs/research_reports/RR3188z1.html

Snyder, Don, Lauren A. Mayer, Guy Weichenberg, Danielle C. Tarraf, Bernard Fox, Myron Hura, Suzanne Genc, and Jonathan William Welburn, *Measuring Cybersecurity and Cyber Resiliency*, RAND Corporation, RR-2703-AF, 2020. As of December 4, 2023: https://www.rand.org/pubs/research_reports/RR2703.html

Snyder, Don, Lauren A. Mayer, Jonathan Lee Brosmer, Elizabeth Bodine-Baron, Quentin Hodgson, Myron Hura, Jonathan Fujiwara, and Thomas Hamilton, *Wing-Level Mission Assurance for a Cyber-Contested Environment*, RAND Corporation, RR-A580-1, 2021. As of December 4, 2023: https://www.rand.org/pubs/research_reports/RRA580-1.html

Snyder, Don, Lauren A. Mayer, Myron Hura, Suzanne Genc, Colby Peyton Steiner, Laura Werber, Kathryn O'Connor, Keith Gierlack, Paul Dreyer, and Bernard Fox, *Managing for Mission Assurance in the Face of Advanced Cyber Threats*, RAND Corporation, RR-4198-AF, 2021. As of December 4, 2023: https://www.rand.org/pubs/research_reports/RR4198.html

Span, Martin, III, Logan O. Mailloux, Robert F. Mills, and William Young, Jr., "Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study," *IEEE Access*, Vol. 6, 2018.

Technical Manual TO 00-5-1, *AF Technical Order System*, Secretary of the Air Force, January 25, 2021.

Technical Manual TO 00-25-107, *Maintenance Assistance*, Secretary of the Air Force, October 1, 2015.

U.S. Air Force, *Systems Security Engineering (SSE) Acquisition Guidebook*, Version 1.4, October 9, 2018, Not available to the general public.

U.S. Air Force, *Systems Security Engineering Cyber Guidebook*, Version 3.0.1, Cyber Resiliency Office for Weapon Systems, January 29, 2021, Not available to the general public.

U.S. Code, Title 10, Section 3453, Preference for Commercial Products and Commercial Services.

Young, William, and Nancy G. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," *Communications of the ACM*, Vol. 57, No. 2, February 2014, pp. 31–35.

Zhang, Yingyu, Chuntong Dong, Weiqun Guo, Jiabao Dai, and Ziming Zhao, "Systems Theoretic Accident Model and Process (STAMP): A Literature Review," *Safety Science*, Vol. 152, August 2022.

RESEARCH SUMMARY

Enhancing Cybersecurity and Cyber Resiliency of Weapon Systems

Expanded Roles Across a System's Life Cycle

DON SNYDER, CHAD HEITZENRATER

To access the full report, visit www.rand.org/t/rrA1506-2

ISSUE

Weapon systems must be secure in a cyber contested environment, or they will not be able to carry out the missions that they are designed to support. How can engineering managed by program offices enhance the cybersecurity and cyber resiliency of weapon systems?

APPROACH

We surveyed current policy, relevant academic literature, and commercial practice and used our personal assessments of cybersecurity and cyber resiliency efforts in the Department of the Air Force (DAF) to identify gaps in the use of engineering for cybersecurity and cyber resiliency throughout the life cycle of weapon systems and to propose mitigations.

KEY FINDINGS

During the design phase, systems security engineering has recently become the policy within the Department of Defense (DoD) for cybersecurity and cyber resiliency of weapon systems, but it has not yet become the general practice in the DAF, and little policy or guidance directs specifically how to do it at the service level. An overreliance is still placed on the Risk Management Framework (RMF), which is largely carried out after systems engineering.

During the operations and sustainment phase, wing-level organizations perform much of the day-to-day security monitoring of weapon systems. However,

- They are not provided with authorized tools tailored to their weapon systems.
- The tools that they have cannot comprehensively monitor or defend their weapon systems.
- They are not provided with technical orders for what to do.
- Policy does not generally require feedback to the program offices of weapon system cyber status or cyber incidents.

continued

Cybersecurity and cyber resiliency are not central parts of current sustaining engineering or life cycle sustainment plans.

RECOMMENDATIONS

Our principal message can be summarized as a recommendation to develop and maintain an integrated engineering-based plan for the cybersecurity and cyber resiliency of each weapon system throughout its life cycle. For the design phase, we advocate that systems security engineering be enhanced by placing into the program plan and contract language:

- standards for designing systems with adequate cyber separability
- methods that the DoD will use to assess cyber resiliency of designs.

These engineering and contract statements need to be specific and measurable with regard to the security outcomes. Before these can be issued, further development and refinement, based on experience, is needed for both the standards and methods.

For the operations and sustainment phase, we advocate for increased use of sustaining engineering and the life cycle sustainment plans for cybersecurity and cyber resiliency. We recommend that program offices do the following:

- Equip wing-level organizations with approved tools for any cyber monitoring of a weapon system that are
  - catered to the weapon system
  - rigorously designed, developed, and tested with a security mindset, so as not to introduce attack vectors into the system
  - comprehensive in their ability to access the weapon system.
- Provide wing-level organizations, such as mission defense teams, with technical orders for the cyber monitoring of weapon systems.
- Receive information regarding any non-nominal behavior within the system boundary or cyber incident.
- Direct and approve any configuration change within the system boundary.

We recommend that the DAF develop an ecosystem for cyber sustaining engineering that uses or mirrors the ecosystem for aircraft maintenance, including processes such as Form 22 notifications for discrepancies in the above-mentioned technical orders and 107 requests for additional, cyber-related technical assistance from program offices.

Life cycle management plans should explicitly outline how the cybersecurity and cyber resiliency of each weapon system will be assured during operations, sustainment, and disposal.

Security should not be considered an activity implemented by RMF but one created by sound engineering and continuous vigilance, rigorously and continuously assessed by RMF.

RAND PROJECT AIR FORCE

RAND Project AIR FORCE (PAF), a division of RAND, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. For more information, visit PAF's website at www.rand.org/paf.