SYM-AM-26-122

# Excerpt from the Proceedings

of the

# Twenty-Third Annual Acquisition Research Symposium and Innovation Summit

## Thursday, May 7, 2026 Sessions
## Volume II
## "Accelerating Warfighting Capabilities"

**Operationalizing Cyber Survivability Through Requirements Decomposition: A Marine Corps Case Study**

**Published: April 30, 2026**

The research presented in this report was supported by the Acquisition Research Program, Graduate School of Defense Management at the Naval Postgraduate School.

**To request defense acquisition research, please contact:**

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
E: arp@nps.edu
**www.acquisitionresearch.net**

Copies of Symposium Proceedings and Presentations; and Acquisition Sponsored Faculty and Student Research Reports and Posters may be printed from the **NPS Defense Acquisition & Innovation Repository** at **https://dair.nps.edu/**.


ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF ACQUISITION, FINANCE, AND MANPOWER
NAVAL POSTGRADUATE SCHOOL

# Operationalizing Cyber Survivability Through Requirements Decomposition: A Marine Corps Case Study

**Kathleen B. Coen—**is a Cyber Test Engineer at the Marine Corps Tactical Systems Support Activity, where she leads adversarial cyber assessments of USMC weapon systems to identify mission-impacting vulnerabilities prior to fielding. She holds a BS in Computer Science from Georgetown University and an ScM in Cybersecurity from Brown University. She is currently a PhD student in Information Sciences at the Naval Postgraduate School. Her work focuses on cyber survivability, test and evaluation, and the integration of cybersecurity policy into acquisition and operational decision-making. She holds the CISSP and DAWIA Engineering & Technical Management Practitioner certifications. [kathleen.coen@usmc.mil]

**Capt Andrew S. Benn, USMC—**is an active-duty Marine Corps officer. A 2023 graduate of the Naval Postgraduate School's Computer Science program and a 2017 graduate of the U.S. Naval Academy Cyber Operations Program, he is currently serving as the Cyber Branch Head at Marine Corps Tactical Systems Support Activity. In this role he supports Marine Corps acquisitions programs with Cyber Developmental Test and Evaluation and integration with Defensive Cyber tools. He served previously with Combat Logistics Regiment 35 and 3d Maintenance Battalion in Okinawa, Japan, as a communications officer and company commander. [andrew.benn@usmc.mil]

## Abstract

United States Marine Corps (USMC) warfighting systems must operate reliably in contested cyber environments to bring their capabilities to bear to a future fight. To ensure mission-critical and safety-critical functions and components remain operational, these systems must be equipped to prevent, mitigate, recover from, and adapt to adverse cyber events: a concept known as cyber survivability. Joint Staff J6 defines 10 Cyber Survivability Attributes (CSAs) and provides guidance for requirements and resource sponsors early in the acquisition lifecycle. However, as programs progress through the acquisition lifecycle, there exists no additional guidance on how to derive, validate, and verify standardized and measurable system-level cyber survivability requirements. This lack of traceability between policy, security controls, and system engineering artifacts results in inconsistent implementation, redundant testing, and reduced ability to evaluate survivability. The Marine Corps Tactical Systems Support Activity's (MCTSSA's) Cyber Branch worked with various USMC Program Offices and other stakeholders to decompose cyber survivability requirements into tailored performance specifications, verification processes, and acceptance criteria. Through iterative application to multiple USMC Programs of Record, this design science research led to the service's inaugural guidance on cyber survivability within the Warfighting Acquisition System: the USMC Cyber Survivability Requirements Guidebook.

**Keywords:** cyber survivability, cybersecurity, requirements decomposition, test and evaluation

## Introduction and Background

Warfighting systems must operate reliably in contested cyber environments to bring their capabilities to bear to a future fight, whether the conflict is with an asymmetric adversary or a pacing threat. To ensure mission-critical and safety-critical functions and components remain operational, systems must be equipped to prevent, mitigate, recover from, and adapt to adverse cyber events (DoW, 2026). This is a concept known as *cyber survivability*. Cyber survivability is critical to the success of modern warfighter systems, especially as adversaries increasingly target these systems through cyberattacks.

Since its introduction in 2015, cyber survivability has been included as a system requirement via the System Survivability Key Performance Parameter (SS KPP; Pitcher, 2023). The SS KPP is intended to promote the development of critical warfighter capabilities that can survive kinetic attacks and non-kinetic threats across domains and applicable environments. cyber survivability is one element of the SS KPP.

Striving for cyber survivability requires a balanced approach that integrates cybersecurity and cyber resilience. Cybersecurity is the process of protecting systems from unauthorized access and malicious attacks by ensuring the confidentiality, integrity, and availability of data and services. In contrast, cyber resilience assumes that security measures may eventually fail and emphasizes the system's ability to operate under duress, recover, and maintain operational capabilities (Swanson et al., 2010). Cybersecurity and cyber resilience form cyber survivability, ensuring systems can withstand and recover from a wide range of threats.

Cyber survivability is accomplished through a combination of Cyber Survivability Attributes (CSAs). The CSAs (Table 1) are a holistic set of cybersecurity and cyber resilience requirements. Each CSA corresponds to one of the four SS KPP pillars (prevent, mitigate, recover, adapt). By incorporating the concepts of cyber resilience, CSAs not only support but go beyond the coverage provided by the Risk Management Framework.

***Table 1. Cyber Survivability Attributes***

| SS KPP Pillars | Cyber Survivability Attributes (CSAs) |
|---|---|
| Prevent | CSA-01: Control Access |
| | CSA-02: Reduce Cyber Detectability |
| | CSA-03: Protect Data in Transit |
| | CSA-04: Protect Data at Rest |
| | CSA-05: Protect Critical Functions |
| | CSA-06: Minimize and Harden Attack Surfaces |
| Mitigate | CSA-07: Baseline and Monitor Systems to Detect Anomalies |
| | CSA-08: Enable Cyber Defense |
| Recover | CSA-09: Recover Capabilities |
| Adapt | CSA-10: Sustain an Operationally Relevant Cyber Survivability Risk Posture (CSRP) |

The CSAs are primarily intended for requirements and resource sponsors developing an Initial Capabilities Document (ICD), Capability Development Document (CDD), Information System ICD (IS-ICD), or Information System CDD (IS-CDD; Joint Staff, 2025).

As programs progress through the acquisition lifecycle, they transition from their service-level requirements process (replacing the Joint Capabilities Integration and Development System [JCIDS] process) to the Warfighting Acquisitions System (WAS). Within WAS, high-level requirements should be decomposed into performance specifications for engineering and testing purposes.

However, at the start of this research effort, there existed no additional guidance on how to derive, validate, and verify standardized and measurable system- and component-level cyber survivability requirements. This lack of traceability between policy, security controls, and system engineering artifacts resulted in inconsistent implementation, redundant testing, and reduced ability to evaluate survivability.

This gap has direct operational and acquisition consequences. As the Government Accountability Office (GAO) found, incorporating cybersecurity practices from the earliest stages of acquisition is typically easier, less costly, and more effective than attempting to add, or "bolt on," protections later in the development cycle or after a system is fielded. When cyber survivability requirements are not clearly defined and translated into measurable system-level

performance specifications, acquisition programs are limited in their ability to assess whether systems can continue to perform mission-critical functions under contested cyber conditions. This deficiency undermines risk-informed acquisition decisions, weakens the effectiveness of developmental and operational testing, and increases the likelihood that systems are fielded with unresolved vulnerabilities that could disrupt mission execution (GAO, 2021).

This research effort addresses this problem by providing analysis and guidance on cyber survivability requirements decomposition, leveraging a systems engineering process to translate high-level requirements into measurable and verifiable specifications. The central research question is:

> How can a structured requirements decomposition framework be used to operationalize CSAs into measurable and testable acquisition artifacts that improve test coverage and support risk-informed decision-making across the acquisition lifecycle?

## Methods

This study leveraged a design science research (DSR) approach. DSR is an established approach in information systems and engineering disciplines for developing and evaluating artifacts intended to solve identified organizational problems (Hevner et al., 2004). The primary contribution lies in both the artifact itself and the evidence demonstrating its utility. A design science approach was chosen because it places emphasis on clarifying the problem statement, goals, and underlying theoretical constructs to generate a new artifact (Gregor & Jones, 2007; McLaren et al., 2011; Moon & Ngai, 2010). DSR enables the development of structured, repeatable solutions that can be applied and evaluated within operational environments.

The DSR process follows an iterative cycle consisting of (1) problem identification, (2) definition of solution objectives, (3) artifact design and development, (4) demonstration in a relevant context, and (5) evaluation of artifact effectiveness (Peffers et al., 2007). This study adheres to that structure, using the iterative development and ultimate application of a requirements decomposition framework to operationalize cyber survivability.

### Problem Identification

The Marine Corps Tactical Systems Support Activity (MCTSSA) Cyber Branch provides cyber test and evaluation (T&E) support to Marine Corps Program Offices. During these engagements, system documentation, such as Capability Development Documents (CDDs), System Requirements Documents (SRDs), and Requirements Traceability Matrices (RTMs), is reviewed and analyzed to inform test activities.

Across multiple programs, a consistent pattern was observed. While CSAs were identified within the CDDs, there was limited evidence that they were decomposed into system- and component-level performance specifications. GAO (2021) found numerous examples of government-generated documentation omitting cyber-related performance specifications cybersecurity requirements. If included, they were often not measurable or directly verifiable through test activities.

This disconnect indicated a lack of standardized mechanisms for translating survivability constructs into actionable engineering and test artifacts, resulting in inconsistent implementation and reduced evaluability of cyber survivability.

### Definition of Solution Objectives

From September 2024 to April 2025, MCTSSA Cyber held a series of meetings with various stakeholders from several Program Offices from Marine Corps Systems Command and Program Executive Office–Land Systems, Systems Engineering and Acquisition Logistics (SE&AL), other USMC T&E Activities, and representatives from the Office of the Under

Secretary of War for Research and Engineering (OUSW[R&E]). Meetings with Program Offices included participation from Information Systems Security Managers (ISSMs), Information Systems Security Engineers (ISSEs), and Information Systems Security Officers (ISSOs) that are responsible for the implementation of CSAs. Meetings were either held virtually (via Microsoft Teams), in person at Marine Corps Base Camp Pendleton, CA, or in person at Marine Corps Base Quantico, VA, and typically lasted 1 hour.

Initial meetings were used to identify and explore the problem and understand stakeholders' perspectives. The MCTSSA Cyber Branch incorporated this feedback into initial drafts of the artifacts, which were then presented, discussed, and refined, in an iterative fashion, at future meetings.

The iterative development and application of the artifact yielded several emergent design principles for operationalizing cyber survivability within acquisition environments. First, survivability constructs must be decomposed into traceable, tailorable performance specifications that preserve alignment with policy-level intent while allowing system-specific refinement. Second, verification methods and plans must remain Tool, Technique, and Procedure (TTP)–agnostic but requirements-specific, enabling consistent test coverage without constraining T&E organizations' testing creativity. Third, artifact adoption depends on integration with existing acquisition workflows and taskings, rather than introducing new processes or burdens. These findings extend prior design science work by proposing a reusable set of principles for translating abstract cybersecurity constructs into actionable acquisition artifacts.

As a result, the MCTSSA Cyber Branch defined a set of objectives for a structured solution to support survivability operationalization within acquisition programs. The solution was required to

- facilitate the decomposition of CSAs into measurable, system-level performance specifications;
- align derived requirements with National Institute of Standards and Technology Special Publication (NIST SP) 800-53 controls, the backbone of the DoW's Risk Management Framework;
- provide associated verification methods and plans to support developmental and operational cyber T&E;
- support said evaluation of implementation effectiveness by providing defined metrics; and
- integrate with existing DoW acquisition and engineering processes without introducing additional procedural burden.

The solution was intended to serve both Program Offices, responsible for requirements development and system acquisition, and T&E activities, responsible for verification and validation of cyber survivability.

**Artifact Design and Development: The Marine Corps Cyber Survivability Requirements Guidebook**

The ultimate artifact from this research is the *United States Marine Corps Cyber Survivability Requirements Guidebook*. This guidebook offers a structured approach for defining and evaluating the 10 CSAs critical for maintaining Cyber survivability within USMC systems. Each CSA section is accompanied by a summary of the CSA and its specific objectives, followed by a comprehensive listing of requirements in support of the CSA. Each requirement includes exemplar language for the performance specification, measurable metrics, and verification methods to support system evaluations during both developmental and operational cyber testing phases. This format aims to provide Marine Corps acquisition activities and the

Test and Evaluation community with a clear, actionable framework for CSA refinement and evaluation.

### 1. CSA Summary

Each CSA section begins with a summary of the CSA describing the attribute's purpose and strategic significance. The summary highlights the primary objective of the CSA, key enablers that contribute to achieving it, and the anticipated mission impact of effective implementation. This provides a holistic understanding of how each CSA supports system resilience and mission continuity.

### 2. Performance Specifications

Each CSA section includes a listing of performance specifications in direct support of that CSA. Performance specifications provide subsystem- and component-level requirement statements that guide system implementation. As standard with performance specifications, functional requirements state the required results without specifically stating how the results are to be achieved; the guidebook does not present a preconceived solution to each requirement.

Performance specifications listed in the guidebook should be further tailored for each system. Provided statements do not include behavior considerations, such as constraints and restraints, to leave the trade-space open for program managers. An example of tailoring is shown in Table 2.

***Table 2. Example of Performance Specification Tailoring***

| Performance Specification Consideration | Guidebook's Tailorable Performance Specification | System-Specific Tailored Performance Specification |
|---|---|---|
| Cross Domain Solutions (CDSs) | The system shall integrate Department of Defense (DoD)-approved CDSs to enable data access between different security domains, per DoD Instruction (DoDI) 8540.01, May 8, 2015, Incorporating Change 1, August 28, 2017. | The system shall integrate DoD-approved CDSs, to including data labeling and auditing, per DoDI 8540.01, May 8, 2015, Incorporating Change 1, August 28, 2017, to enable data access from Coalition to Secret domains in the data standards or file formats of Extensible Markup Language (XML) and Internet Relay Chat (IRC). |
| Automated Shedding on Non-Mission and Non-Safety Critical Functions | The system shall provide capabilities to shed non-mission and non-safety critical functions, systems/subsystems, and interfaces. | The system shall provide automated capabilities to shed non-mission and non-safety critical functions, systems/subsystems, and interfaces within 5 seconds of detection of a critical system overload or a verified cyberattack. Non-mission and non-safety critical functions are defined in Table X. Shedding shall occur in the order specified in Table Y, minimizing impact to overall system performance as detailed in Table Z. Shed functions shall be automatically re-enabled when system load returns to normal operating parameters. |

Performance specifications should be selected during the Technology Maturation and Risk Reduction phase and finalized at the Critical Design Review that takes place during the Engineering and Manufacturing Development phase. Performance specifications should be included in the System Requirements Document or the System Performance Specification (SPS). The SPS is included in the Request for Proposal package provided to contractors and is closely aligned with the program's CDD and Capability Production Document, ensuring ultimate alignment with the cyber element of the SS KPP.

### 3. Verification Methods and Plans

For each performance specification, the guidebook provides a listing of verification methods and plans to test implementation effectiveness. The verification plans provide guidance on what should be tested but does not specify how they should be tested; verification plans were purposely left non-prescriptive. The T&E community should retain full autonomy over specific tools, techniques, and procedures used during testing. The ultimate objective is consistent and thorough assessments, ensuring test plans and cases have adequate coverage for each requirement.

Each verification plan was tagged with its associated verification method. As stated in the *Systems Engineering Guidebook*, verification plans can be achieved through any combination of the following methods:

- **Inspection or Examination:** Visual inspection of equipment and evaluation of drawings and other pertinent design data and processes should be used to verify conformance with characteristics, such as physical, material, part, and product marking and workmanship.
- **Demonstration:** Demonstration is the performance of operations at the system or system element level where visual observations are the primary means of verification. Demonstration is used when quantitative assurance is not required for the verification of the requirements.
- **Analysis:** Analysis is the use of recognized analytic techniques (including computer models) to interpret or explain the behavior/performance of the system element. Analysis of test data or review and analysis of design data should be used as appropriate to verify requirements.
- **Test:** Test is an activity designed to provide data on functional features and equipment operation under fully controlled and traceable conditions. The data is subsequently used to evaluate quantitative characteristics.

In accordance with *the Guide for Performance Specifications*, each performance specification can, and typically does, utilize more than one method for proper verification.

The verification methods and plans should be used as a starting point for the development of test plans and cases. Cyber test activities must begin as soon as the program is established and continue throughout the acquisition lifecycle. USMC cyber T&E activities and teams should be involved as soon as possible in the early system assessments based on available program documentation, hands-on testing of individual components/subcomponents during system development, and cyber survivability testing of complete systems and the entire platform in test and operationally representative environments.

### 4. Metrics

Each performance specification is accompanied by a listing of related metrics used to determine the successful implementation of the requirement. These metrics can be used to determine if the system's specific threshold survivability requirements are being met and to

quickly gauge a system's potential performance under contested cyber conditions. These acceptable threshold requirements are not numeric in the guidebook, as they are highly system- and mission-dependent and should be determined by the PM.

Through this structure, the guidebook provides a repeatable mechanism for transforming abstract survivability constructs into actionable engineering and acquisition artifacts. In doing so, it addresses the core problem identified in this research: the lack of standardized methods for operationalizing cyber survivability within the acquisition lifecycle.

## Results: Demonstration in a Relevant Context

Consistent with design science methodology, the artifact was not evaluated in isolation but via application within an operational context.

A draft version of the guidebook was used by a Marine Corps Program of Record within a Middle Tier Acquisition pathway, where it was used to develop and refine cyber survivability requirements and associated verification methods.

During the requirements phase, the platform was assigned a Cyber Survivability Risk Category (CSRC) value of 3. The CSRC identifies the appropriate degree of cyber survivability required for a system. It is a function of the system's Mission Type, the Adversary Threat Tier expected to be facing the system, the Cyber Dependence Level of the system, and the Impact Level of system compromise or loss; the final CSRC is a numeric value ranging from 0 to 5. The CSRC value determines how many CSAs should be selected; a CSRC 3 system does not require all 10 CSAs. This platform selected seven CSAs total.

### Evaluation of Artifact Effectiveness

In the end, based on the seven CSAs, the platform was assigned a robust set of cyber-related performance specifications. 90% of the performance specifications were taken and tailored from the guidebook. The program averaged eight verification methods per performance specification. 82% of the verification methods were taken and tailored from the guidebook. The guidebook is meant to provide initial considerations that should be built on and further tailored for each system.

Feedback from Program Offices indicated increased confidence in cyber requirements alignment, reduced ambiguity in CSA interpretation, and improved communication between the dedicated professionals involved in requirements development, management, implementation, and evaluation of cyber survivability in the USMC.

The artifact of this DSR, the *USMC Cyber Survivability Requirements Guidebook*, is expected to be published June 2026.

## Discussion

The results of this work provide empirical support for the central research question that guidance for a structured requirements decomposition process improves the operationalization of cyber survivability within acquisition programs. By translating high-level CSAs into measurable and testable performance specifications, the artifact addresses and minimizes the critical gap between strategy intent and engineering execution.

Cyber survivability, as it is defined in high-level guidance, lacks measurability. Without further decomposition, the CSAs remain a conceptual objective rather than an engineering requirement. The artifact effectively transforms CSAs into a set of verifiable system design consideration, enabling engineers to design against concrete criteria and testers to evaluate performance in a structured manner.

The study also highlights the role of decomposition in improving traceability across the acquisition lifecycle. By establishing explicit linkages between CSAs, NIST SP 800-53 controls, Zero Trust Activities, and system-level requirements, the framework created a continuous thread for those in the Systems Security Engineering community to focus on. In the absence of such linkages, acquisition programs risk redundant engineering and cyber assessments.

From an acquisition standpoint, the implications are equally significant. The introduction of structured, decomposed requirements improved alignment across stakeholders, including Program Offices, system engineers, vendors, and test organizations. Reduced ambiguity in requirement interpretation will facilitate more consistent implementation, ease of understanding, and efficient communication. This is particularly important in complex acquisition environments, where misalignment between stakeholders, particularly between the government and its vendors, can lead to costly rework, delayed testing, and incomplete risk assessments.

However, the results also underscore that decomposition is not a purely technical solution. Its effectiveness depends on adoption, correct application, and integration within existing acquisition processes. The guidebook provides a structured starting point, but it requires tailoring to system-specific contexts and active engagement from stakeholders. As such, the value of decomposition lies not only in the artifact itself, but in how it is leveraged and applied by the broader engineering and acquisition community.

By bridging the gap between policy and implementation, the approach improves traceability, enhances test coverage, and supports more informed acquisition decisions. These findings contribute to ongoing efforts to integrate cybersecurity and resilience considerations into systems engineering and acquisition practices and provide a foundation for scaling survivability-focused approaches across the DoW.

## Future Research

This study is subject to several limitations that inform both the interpretation of findings and the direction of future research. First, while several Program Offices and stakeholders provided feedback in the iterative cycle of artifact development, the evaluation of the artifact was limited to a single-case application within a Marine Corps platform. While the selected case provides a realistic and operationally relevant test environment, it limits the generalizability of findings across different acquisition pathways, system types, services, and organizational contexts. Programs with varying levels of cyber maturity, system complexity, or stakeholder expertise may experience different outcomes when applying a requirements decomposition framework. Additionally, the platform selected is still early in the acquisitions lifecycle. The long-term impact of requirements decomposition on ultimate system survivability and lifecycle cost has not yet been observed.

Finally, this research opens an opportunity to extend the decomposition approach beyond cyber survivability to other elements of the SS KPP or other high-level requirements. Each of these domains faces similar challenges in translating high-level constructs into actionable engineering requirements. A unified decomposition methodology may therefore provide broader value across the WAS.

## References

DoW. (2026). *Cyber developmental test and evaluation* (DoW Manual 5000.103). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/5000103m.pdf

GAO. (2021). *Weapon systems cybersecurity: Guidance would help DOD programs better communicate requirements to contractors* (GAO-21-179). https://www.gao.gov/assets/gao-21-179.pdf

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, 8(5), 312–335. https://doi.org/10.17705/1jais.00129

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1). https://doi.org/10.2307/25148625

Joint Staff J6 Command, Control, Communications, and Computers/Cyber. (2025). *Cyber survivability endorsement implementation guide*.

McLaren, T. S., Head, M., Yuan, Y., & Chan, Y. (2011). A multi-level model for measuring fit between a firm's competitive strategies and information systems capabilities. *MIS Quarterly*, *35*(4). https://doi.org/10.2307/41409966

Moon, K. L., & Ngai, E. (2010). R&D framework for an intelligent fabric sample management system: A design science approach. *International Journal of Operations Production Management*, *30*(7). https://doi.org/10.1108/01443571011057317

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3). https://doi.org/10.2753/MIS0742-1222240302

Pitcher, S. (2023). Improving cyber survivability for weapon system mission assurance. *Cybersecurity and Information Systems Information Analysis Center*. https://csiac.dtic.mil/webinars/improving-cyber-survivability-for-weapon-systems-mission-assurance/

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication No. 800-34). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1




Acquisition Research Program
Department of Acquisition, Finance, and Manpower
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net